



SteelCentral™ AppResponse 11 User's Guide

Version 11.17.0

September 2023



© 2023 Riverbed Technology. All rights reserved.

Riverbed®, SteelConnect™, SteelCentral™, SteelHead™, and SteelFusion™ are all trademarks or registered trademarks of Riverbed Technology, Inc. (Riverbed) in the United States and other countries. Riverbed and any Riverbed product or service name or logo used herein are trademarks of Riverbed. All other trademarks used herein belong to their respective owners. The trademarks and logos displayed herein cannot be used without the prior written consent of Riverbed or their respective owners.

This document is furnished "AS IS" and is subject to change without notice and should not be construed as a commitment by Riverbed. Riverbed does not provide any warranties for any information contained herein and specifically disclaims any liability for damages, including without limitation direct, indirect, consequential, and special damages in connection with this document. This document may not be copied, modified or distributed without the express authorization of Riverbed and may be used only in connection with Riverbed products and services. Use, duplication, reproduction, release, modification, disclosure or transfer of this document is restricted in accordance with the Federal Acquisition Regulations as applied to civilian agencies and the Defense Federal Acquisition Regulation Supplement as applied to military agencies. This document qualifies as "commercial computer software documentation" and any use by the government shall be governed solely by these terms. All other use is prohibited. Riverbed assumes no responsibility or liability for any errors or inaccuracies that may appear herein.



Riverbed Technology
680 Folsom Street
San Francisco, CA 94107
www.riverbed.com

Part Number
712-00302-23

About This Guide	xi
Audience	xi
Document Conventions	xi
Documentation and Release Notes.....	xii
Contacting Riverbed	xii
1 - Overview	1
AppResponse 11 Web User Interface	1
Global Search	2
Search.....	2
Insight on	5
Groups.....	7
Applications	7
Monitoring Interfaces	8
Using Packet Brokers	8
Interface Speed and Duplex Settings	9
Editing a Monitoring Interface	10
Metrics in AppResponse 11	11
Metrics for TCP Clients and TCP Servers	12
Other Metric Revisions in AppResponse 11	12
Metrics for Web Transaction Analysis (WTA).....	12
TCP Connection	13
How AppResponse 11 Selects and Stores Top Elements	14
General Notes	14
Selecting Top Elements	14
Common Workflows in AppResponse 11	15
Investigating a Web Application	15
Interpreting TCP Performance Metrics	16
Troubleshooting Host Groups and Applications	18
2 - Configuration	21
Licensing.....	22
Licensing Overview.....	22
Licensing Toolbar	24
Adding a License	24
Deactivating a License	24
Deleting a Feature Key	25
Restoring a Feature Key	25
- Administration - Authentication	26
User Administration and Account Policy	26
Local Users tab	26
Password Policy tab	27

Roles and Permissions	27
Roles	28
Permissions	28
Default User Preferences	32
Default Metric Colors	32
Remote Authentication.....	34
Remote Authentication	34
General Tab	35
RADIUS Authentication	37
TACACS+ Authentication	38
Setting Up Remote Authentication	39
SAML 2.0 Authentication	41
Virtual Interface Groups (VIFGs)	43
Virtual Interface Groups Tab	43
The Default VIFG: other_vifg	44
VIFG Modes	45
VIFG Usage Considerations	47
Creating or Editing a VIFG.....	47
Deleting a Virtual Interface Group	48
Managing Virtual Interface Group Members	48
Importing and Exporting VIFG Definitions.....	48
Flow Export	50
Configuring Flow Export	50
Checking Flow Export Status.....	51
Capture Jobs	52
Adding a New Capture Job.....	52
Downloading Packets From a Capture Job.....	55
Analyzing Traffic with Packet Analyzer Plus.....	56
Analyzing Traffic with Transaction Analyzer	56
Restricting User Access to Packets	57
Packet Format.....	58
Supported Parameters	58
Configuring Packet Dissection.....	58
Web Server Settings	60
Secure Vault For Encrypted Security Files	60
Configuring HTTPS Settings	61
Configuring HTTP Access.....	61
Viewing the SSL Certificate	62
Replacing the SSL Certificate.....	62
FIPS Mode	63
Supported AppResponse Platforms	63
General Considerations When Using FIPS Mode	64
Traffic Handling.....	64
Enabling FIPS Mode	64
Feature Support	64
SSL Decryption.....	68

Installed Keys Tab	68
Certificates With Installed Keys Tab	68
Certificates With Missing Keys Tab	69
Ignored Keys Tab	69
PFS Tab	69
SSL Ciphers Supported For Decryption.....	69
NetProfiler Integration	74
Viewing the NetProfiler Export Certificate	74
Replacing the NetProfiler Export SSL Certificate.....	75
Viewing the Trusted NetProfiler Certificates	76
Adding a Trusted NetProfiler Certificate	76
Deleting a Trusted NetProfiler Certificate	77
Flow Export Settings tab	77
Flow Export Traffic Selection tab	77
Flow Export Status tab.....	77
Server Response Time Analysis	78
Configuring the Mode	78
Configuring Port Whitelist Mode.....	78
Configuring All Ports Mode	79
Editing Table Entries	80
Deleting a Table Entry.....	80
3 - General Settings	82
Management Interfaces	82
Default Gateway	82
Configuring Management Interfaces	83
Managing Routes	83
Time	85
Time zone.....	85
Configuring PTP.....	85
Configuring NTP	86
Manually Setting Date and Time	87
Hostname/DNS	89
Hostname and DNS Servers	89
Static Name Resolution.....	89
Editing a Static Hostname.....	89
Deleting a Static Hostname	90
Exporting and Importing Static Hostnames	90
SNMP	91
Considerations For Using SNMP In FIPS Mode	91
Integration Links	93
4 - Administration - Other	94
User Preferences	94
Language and Time	94
Appearance	95

Data Units	95
Default Insight	95
Search Settings.....	96
Built-In Policy Preferences.....	96
Email Server	96
Specifying an email server	97
Recipients	98
Defining Recipients	98
Encrypted Syslog Support.....	99
ServiceNow Support.....	101
Business Hour Profiles	102
5 - System Operations.....	103
Configuring and managing storage units	104
AppResponse 11 CLI Storage and Service commands	104
Initializing storage units.....	105
Changing the Storage RAID level	105
System Dumps	106
Creating a System Dump	106
Managing System Dumps.....	106
Downloading a System Dump	107
System Health.....	109
Storage Status and Usage	113
Hardware Status	113
Storage Usage	114
Storage Configuration	114
Software Update	118
Updating AppResponse 11 Software	118
Update Information	119
Update Source	119
Reboot/Shutdown	120
Rebooting AppResponse 11.....	120
Shutting Down AppResponse 11.....	120
Backup and Restore	121
Backup/Restore Workflow Overview	121
Backup/Restore Page and Operations	122
Define a Backup Server	122
Back Up on Demand	123
Schedule A Backup For Another Time	123
Restore Previously Backed Up Data.....	124
Transferring Licenses For RMA Situations	126
6 - Definitions	127
Host Group Configuration	127

Recommended Practices When Using Host Groups	127
Defining Host Groups	128
Importing Business Groups from an Upgraded AppResponse 9.6.x Appliance	129
Editing a Host Group	129
Exporting and Importing Host Groups	130
Application Configuration.....	132
Importing Applications from an Upgraded AppResponse 9.6.x Appliance	132
Traffic Matching Mode.....	133
General	134
URL	136
Web.....	136
Auto-recognized.....	141
Importing and Exporting Application Definitions	141
Preferred IPs	144
Specifying Preferred IP Addresses	144
Exporting Preferred IP Addresses.....	145
Importing Preferred IP Addresses.....	145
Port Alias Configuration.....	146
Configuring a Port Alias	146
Editing a Port Alias.....	147
Deleting a Port Alias.....	147
Policies	148
Static Policies and Adaptive Policies	148
Defining a Policy.....	149
General Properties	149
Alert On & Filtering Properties.....	150
Trigger Properties.....	151
Notification Properties.....	153
Editing and Deleting Policies	156
Built-In Policies.....	156
Importing and Exporting Policies.....	157
Traffic Analysis Filters	159
Example Use Cases	159
Editing Protocol Filters.....	159
Adding a Definition to a Filter	160
Synchronizing Changes with Packet Analyzer Plus	161
Discovered Service Names	163
7 - Insights.....	164
Opening Insights	164
Specifying IP Addresses and Ports	165
Supported Insights.....	165
Summary Insights	166
Individual Insights	167
Interactive Insights	167
Viewing Insights	168

Drill Downs	168
Launching and Managing Insights	169
Editing an Insight's Properties	170
Using the Layout Editor to Modify a Custom Insight's Content.....	170
Deleting an Insight	171
Importing Custom Insights	171
Schedules	171
Viewing Saved Reports	173
Alerts	173
Viewing Alert Events.....	173
Viewing Alert Event Details.....	175
Insight PDF Downloads.....	178
Downloads	180
Traffic Diagnostics Insight	182
General	182
Flow Export	182
ASA Module.....	182
WTA Module	183
DBA Module	183
UCA Module.....	183
CXA Module	183
SSL/TLS Insights	185
DNS Insights	187
8 - Navigator	189
Navigating Groups and Selecting Favorites	189
Viewing a Group in Navigator	190
The Navigator Top Table	190
The Top Table Toolbar.....	191
The Navigator Workspace	192
The Workspace Toolbar.....	192
Controlling Chart and Table Updates	193
Adding Top Table Rows to a New or Existing Chart or Table	193
Using Settings to Select Chart Data and Appearance	194
Favorites	196
Creating a Favorite	196
Adding or Deleting Groups in a Favorite	196
Deleting a Favorite	197
Using Right-Click Menu Options in Tables and Charts.....	197
Drill-downs.....	198
Right-click Options	199
GeoMap Chart	200
ASA Drilldown Changes Introduced in Version 11.7.0.....	201

Transaction Searches	205
9 - Web Transaction Analysis.....	206
Page Analysis Configuration	206
Data Collection Options.....	206
Advanced Options	207
Installing a WTA Configuration from an Upgraded AppResponse 9.6.x Appliance	208
Page Analysis Rules: Customize How WTA Constructs Page Views	210
Custom Page Analysis Rule Settings	210
Page Family Rules: Customize How WTA Constructs Page Families	211
Custom WTA Metrics/Columns	216
Page Match Criteria.....	216
Information Privacy	217
User Session Tracking	221
Important Notes.....	222
Use the Session Tag for User Name if User Name Not Found	222
Discover User Tracking Information from a Packet Trace File	223
Define User Session Tracking for a Web Application	225
10 - Database Analysis.....	228
Configuring DB Analysis	229
Configuring Database Analysis Filters	229
Using Insights to View and Analyze Database Metrics	230
Using Inputs to select or specify Insight contents	230
Using Navigator to Explore and Create Insights	230
11 - UC Analysis	231
12 - CXA Module.....	232
A - Command-Line Interface	233
Command-Line Interface Operation	233
B - Supported CODECS	235
Audio	235
Video	235
Voice	236
C - AppResponse 11 Metric Descriptions	241
Common Concepts In Metrics.....	241
Application Stream Analysis (ASA) Metrics.....	242

Citrix Analysis (CXA) Metrics.....	248
Database Analysis (DBA) Metrics.....	252
Unified Communications Analysis (UCA) Metrics	256
Web Transaction Analysis (WTA) Metrics	258
Round Trip Time.....	263
D - Security Mechanisms for General Access	265
Method 1: Browser/Web UI access.....	265
Method 2: REST API	265
Method 3: CLI	265
Security Mechanisms for Captured/Stored Packets	265
Security Mechanisms for SSL/TLS Keys	267

Welcome

About This Guide

Welcome to the *SteelCentral™ AppResponse 11 User's Guide*. This guide describes how to use AppResponse 11 to capture packets and use network and application performance metrics to monitor, troubleshoot, and resolve network and end-user issues.

Audience

This guide is written for network and application operators and managers:

- who operate, manage, and troubleshoot corporate networks and applications.
- are familiar existing and emerging networking technologies such as TCP/IP and Layer 3 through Layer 7 Protocols.

Document Conventions

This guide uses the following standard set of typographical conventions.

Convention	Meaning
<i>italics</i>	Within text, new terms and emphasized words appear in <i>italic</i> typeface.
boldface	Within text, CLI commands, CLI parameters, and REST API properties appear in bold typeface.
Courier	Code examples appear in Courier font: <pre>amnesiac > enable amnesiac # configure terminal</pre>
< >	Values that you specify appear in angle brackets: interface <ip-address>
[]	Optional keywords or variables appear in brackets: ntp peer <ip-address> [version <number>]
{ }	Elements that are part of a required choice appear in braces: {<interface-name> ascii <string> hex <string>}
	The pipe symbol separates alternative, mutually exclusive elements of a choice. The pipe symbol is used in conjunction with braces or brackets; the braces or brackets group the choices and identify them as required or optional: { delete <filename> upload <filename>}

Documentation and Release Notes

The most current version of all Riverbed documentation can be found on the Riverbed Support site at <https://support.riverbed.com>.

See the Riverbed Knowledge Base for any known issues, how-to documents, system requirements, and common error messages. You can browse titles or search for keywords and strings. To access the Riverbed Knowledge Base, log in to the Riverbed Support site at <https://support.riverbed.com>.

Each software release includes release notes. The release notes list new features, known issues, and fixed problems. To obtain the most current version of the release notes, go to the Software and Documentation section of the Riverbed Support site at <https://support.riverbed.com>.

Examine the release notes before you begin the installation and configuration process.

Contacting Riverbed

This section describes how to contact departments within Riverbed.

- **Technical support** - Problems installing, using, or replacing Riverbed products? Contact Riverbed Support or your channel partner who provides support. To contact Riverbed Support, open a trouble ticket by calling 1-888-RVBD-TAC (1-888-782-3822) in the United States and Canada or +1 415-247-7381 outside the United States. You can also go to <https://support.riverbed.com>.
- **Professional services** - Need help with planning a migration or implementing a custom design solution? Contact Riverbed Professional Services. Email proserve@riverbed.com or go to <http://www.riverbed.com/services/index.html>.
- **Documentation** - Have suggestions about Riverbed's online documentation or printed materials? Send comments to techpubs@riverbed.com.

Overview

AppResponse 11 Web User Interface

The Home page opens when you sign-in to SteelCentral AppResponse. A Virtual Interface Group (VifG), `other_vifg`, containing all visible interfaces is automatically configured. A capture job, `default_job`, using all available VifGs (`other_vifg`, by default) also has been configured to capture and monitor network traffic. By default, the All Traffic Insight is displayed, showing current network and application metrics for all your network traffic.

This page can be customized in the following ways:

- Under Administration > Other: User Preferences:
 - Selecting another Insight to be displayed when this page is opened.
 - Selecting not to display any Insight when this page is opened.
- Changing the time interval displayed using the current time selections choices or click the edit icon to specify your own time interval.
- Selecting Auto-Update to update the Insight, every minute by default. Click the expand icon to specify a different update interval.
- You also can create your own Insight in Navigator to display the groups and charts of most interest to you when you sign in to AppResponse 11. Go to Administration > Other: User Preferences and select your Insight to display automatically.

Want to immediately view other Insights?

1. Double click the collapsed column on the left side of the window.
2. A list of all Insights is displayed.
3. At the top of the list is a filter bar to assist you in finding an Insight. Multiple filters can be applied to the list of Insights. A green background indicates an applied filter in the filter bar. Click the funnel icon to select the type of filter and choose its values:
 - By owner displays a list of owners for selection.
 - By tag displays a list of all current tags for selection.
 - By name matches the text specified with Insight names.
 - Tags is a shortcut to selection by tag, used when applying multiple filters.
 - All Shared is a shortcut to by owner, used when applying multiple filters.

- Click **Apply** to use the revised filter.

4. Click the Insight in the left column to view it.

Global Search

Use the Search field at the right end of the AppResponse 11 menu bar to enter search terms for items of interest, for example, URLs, IP addresses, named ports, or applications. Your search strings can include CIDR masks and wildcard characters. You also can choose the type of search performed. Just left and adjacent to the search field, click on the drop-down list icon. You can choose from these search types:

- **Search** — returns information related to your search term, organized by source. This is the default. Note that a DNS name typed as a search term will be resolved and shown in the search results as the corresponding IP address.
- **Insight on** — returns an insight of the type selected, providing detailed status and performance information on your search term. The search box describes the expected input, based on the search type selected, for example, IP address.

Search

If you choose Search, a list of possible choices is displayed as you begin typing your search term. The more characters you enter, the closer the possible matches that are shown. Click a suggested match from the list or enter the complete search term and press Enter.

Supported Search String Formats

IP address search strings are supported in these formats:

- Fully qualified IPv4 address, such as: 10.91.126.84
- Fully qualified IPv6 address, such as: 2A03:2A03:2880:F000:F000:F000:0000
- IPv4 wildcard, such as:
 - 10.91.*
 - 10.91.**
 - 10.91.126.*

Note that these formats are not allowed: 10.*.1.1; 10*

- IPv6 wildcard, such as:
 - 2A03:2A03:2A03:2880:F000:F000:*.*
 - 2A03:2A03:2A03:2880:F000:F000:F000:*

Note that a wildcard in the middle is not allowed.

- IPv4 CIDR, such as:
 - 10.0.0.0/8
 - 192.168.1.0/32

- Short form of IPv4 CIDR: 10/8
- IPv6 CIDR, such as: 2001:db8::/32
- Partial IPv4 address, such as:
 - 10.
 - 10.91.
- Partial IPv6 address, such as:
 - AAAA:
 - AAAA:BBBB:

Note: Multiple IP addresses in the form of "10.0.0.1, 10.0.0.2" are not supported. Only one IP address or CIDR/wildcard is supported at a time.

URL search strings are supported in these formats:

- URL:, such as: http://www.riverbed.com?abc=55
- URL with wildcard, such as:
 - https://www.riverbed*
 - https://www.riverbed*.com
 - http*://www.riverbed.com

Wildcards are supported everywhere in the URL.

Search Result Tabs

Search results will be organized into one or more of the following tabs, as appropriate for the results:

- DNS Lookups
- IP Addresses
- Web Page URLs
- Host Groups
- General Apps
- URL Apps
- Web Apps
- Auto-Recognized Apps
- Page Families
- Reports
- Insights
- Favorites
- Port Aliases (TCP)
- Port Aliases (UDP)
- Policies

- DB Types
- DB Instances
- DB Process Names
- DB Server Users
- DB Client Users
- DB Query Commands
- DB Query Statements
- DB Return Codes

For example, while looking at an Insight chart listing the busiest applications, you see an application named Epmmap. Unsure of what this, exactly? Execute a search to investigate it by clicking the expand icon to the left of the search field and choosing Search from the drop-down list. As you start entering the name, a list of possible matches is displayed. Click a suggested match from the list or enter the complete string and press Enter. If your user input is a valid host name, resolved IP addresses are shown as click-on options in the suggested matches. The results for this search are shown below.

Search Results ?

All	Auto-RecognizedApps	NamedTCPPort	NamedUDPPort
-----	---------------------	--------------	--------------

Epmmap - Auto-RecognizedApps
Microsoft EPMAP (End Point Mapper), also known as DCE/RPC Locator service, is used to remotely manage services.
[Summary](#) [New Favorites](#) [Definition](#)

epmap - NamedUDPPort
[Summary](#) [New Favorites](#) [Definition](#)

epmap - NamedTCPPort
[Summary](#) [New Favorites](#) [Definition](#)

http-rpc-epmap - NamedUDPPort
[Summary](#) [New Favorites](#) [Definition](#)

http-rpc-epmap - NamedTCPPort
[Summary](#) [New Favorites](#) [Definition](#)

pxc-epmap - NamedTCPPort
[Summary](#) [New Favorites](#) [Definition](#)

pxc-epmap - NamedUDPPort
[Summary](#) [New Favorites](#) [Definition](#)

solera-epmap - NamedUDPPort
[Summary](#) [New Favorites](#) [Definition](#)

solera-epmap - NamedTCPPort
[Summary](#) [New Favorites](#) [Definition](#)

The list in the heading displays available information types, for example, Auto-RecognizedApps, or NamedTCPPort. By default All, the first choice, is used and displays all results. All resolved IP addresses are grouped into a single search result with links that start separate IP data searches on each of the resolved addresses.

Under each result, you can select the information that is of interest to you. For example, if you investigate the first result, “Epmmap- Auto-RecognizedApps” the following details are available:

- **Summary**—This opens an Individual: AP Insight for detailed application traffic and performance metrics.
 - Use the time interval in the top right corner to see the application metrics for a different time interval.
- **New Favorites**—Allows you to save Epmap as a new Favorite or add it to an existing Favorite.
- **Definition**—Opens the list of Auto-Recognized Applications where you find that Epmap is a “Microsoft EPMAP (End Point Mapper), also known as DCE/RPC Locator service, is used to remotely manage services.”

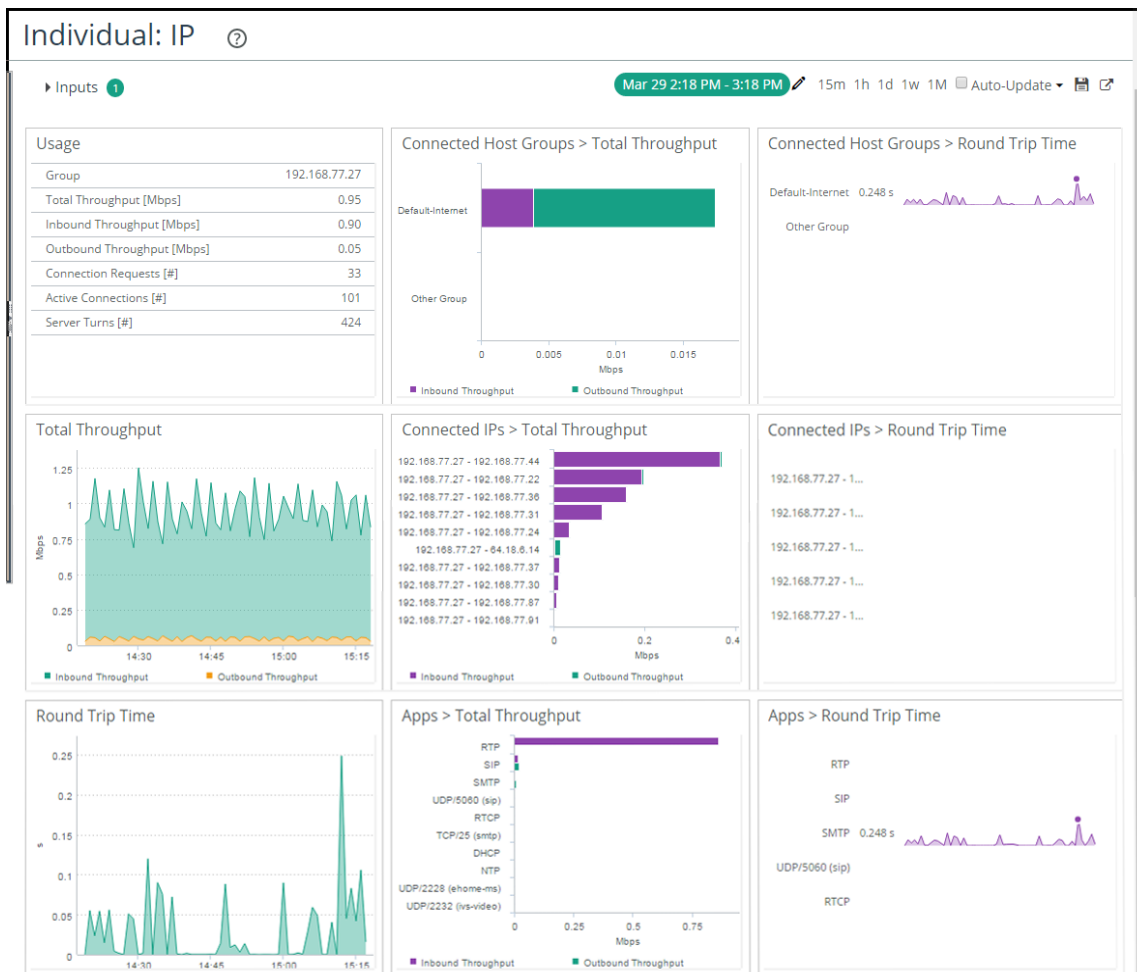
You can investigate the other search results tabs to find the TCP port or UDP port assigned to the Epmap application.

Insight on

You can choose to display an insight on your search term by choosing from the supported subjects listed in the drop-down menu:

- IP Address
- General/URL App
- Host Group
- Web App
- Web User Group
- DB Server IP
- DB Client IP

For example, in Navigator you see that the IP address 192.168.77.27 has the highest Total Throughput for the current time interval. To have a quick look at this IP you do an Insight on search for this IP address. The search results appear below.



The Individual IP insight shows you what the activity is on this IP address and its performance using timelines, bar charts, and sparkline charts.

Clicking on the Inputs drop-down icon in the top left corner shows the input used was 192.168.77.27:

Inputs 1

IP *

Launch * - required

To view the IP address with the second highest total throughput, replace 192.168.77.27 with that IP address and click **Launch**.

The Inputs drop-down list contains all of the available inputs that you can specify for the insight. You can create a custom insight and save it by clicking the disk icon in the top right corner of the insight. You can choose to enable Public (read-only), Shared or Private access to the saved insight.

Groups

AppResponse 11 automatically collects and aggregates data, in the form of metrics, into groups. These groups represent the aggregate for all elements within the groups. AppResponse 11 provides a set of built-in groups that are supported out of the box with no configuration required.

In addition, users can defined their own groups in the form of Host Groups and Applications. Host Groups provide the custom aggregation necessary to understand the relevance of data exchanges to your business. They can be defined to represent any set of relevant network users, such as customers, business units, application servers and remote offices.

AppResponse not only lets managers examine the performance and utilization of Groups in isolation, they can also be used to understand and troubleshoot traffic exchanges between Groups. This detailed information about the connectivity and interaction between Groups is crucial in understanding how your valuable network resources are used and how they are performing.

Applications

Applications can be defined against standard protocols and protocol/port combinations and further specified again a server or set of servers and, if desired, a URL or set of URLs. In addition, over 1,300 popular business and recreational applications are automatically recognized through deep packet inspection.

Monitoring Interfaces

AppResponse 11 monitors network traffic on its physical or virtual interfaces. Each interface is known as a monitoring interface. Use the Monitoring Interfaces tab on the Capture Jobs/Interfaces page to configure and manage each interface.

AppResponse 11 provides three built-in monitoring interfaces:

- **mon0** – The default monitoring interface, enabled by default, used if no others are configured.
- **primary-gre** – Disabled by default, this provides packets received by the management port within a GRE, ERSPAN2 or ERSPAN3 tunnel.
- **primary vxlan** – Disabled by default, this provides packets received by the management port within a VXLAN tunnel.

All three are shown on the Monitoring Interfaces page and the Traffic Diagnostics Insight.

All detected interfaces and their status are listed under Monitoring Interfaces. A monitoring interface can be edited (see [“Editing a Monitoring Interface” on page 10](#)):

- to change the interface description.
- to set the interface speed and duplex using auto-negotiation (default) or by specifying, when available, the interface speed and duplex.

A *virtual interface group* (VIFG) is a logical grouping of one or more monitoring interfaces. AppResponse treats all physical or virtual interfaces in the same VIFG as one interface. To see what interfaces are used by a Virtual Interface Group, look at the Virtual Interface Groups tab. For more information, see [“Virtual Interface Groups \(VIFGs\)”](#).

Important: Capture jobs are configured using VIFGs as traffic sources, not monitoring interfaces.

This section discusses the following:

- [“Using Packet Brokers” on page 8](#)
- [“Interface Speed and Duplex Settings” on page 9](#)
- [“Editing a Monitoring Interface” on page 10](#)

Using Packet Brokers

AppResponse 11 appliances can select from a set of supported packet brokers. The following Gigamon packet brokers are supported:

- Gigamon Header (available on GigaSmart blades), slicing supported
- Gigamon Trailer (available on GigaSmart blades), slicing supported
- Gigamon X12 (available on Gigamon H-series)
- cPacket TS only
- cPacket TS and Slice, slicing supported

- Anue, slicing supported
- Arista (three modes of operation, automatically detected)

Note: AppResponse 11 virtual edition only supports the selection of the Gigamon Header packet broker.

Important: The use of a packet broker is a global option across all interfaces and affects all monitored traffic.

When a packet broker is enabled or modified, the new setting is propagated automatically, with no restart needed.

When using a packet broker, an unexpected number of dropped packets may indicate a problem with the packet broker configuration.

Using a packet broker requires the following:

- The correct packet broker is selected in the web UI. If the wrong packet broker is selected, timestamps may not be processed successfully, causing packets to be dropped. If a packet broker is selected but no packet broker is in use, timestamp processing also can result in dropped packets.
- Timestamps are configured correctly in the packet broker. AppResponse 11 automatically drops packets that are out of range (too early or too late) when checked against the system clock or previous packets.

Observe these additional considerations:

- Make sure the packet broker clock is not off relative to AppResponse 11's clock; AppResponse 11 tolerates an error of up to five minutes.
- Make sure you are not sending line rate traffic to the packet broker. That will cause packets to be dropped between the broker and AppResponse 11.

To use a packet broker

1. Go to Administration > General Traffic Settings: Capture Jobs/Interfaces, and click the Monitoring Interfaces tab.
2. Under Packet Broker Settings, select one of the supported packet brokers from the drop-down list in the Packet Broker field. By default, NONE is selected.

Note: The AppResponse 11 virtual edition only supports the Gigamon Header packet broker.

Interface Speed and Duplex Settings

The speed and duplex settings available are listed by interface type below:

- 1 G Copper Interface
 - **AUTONEG**
Autonegotiates 10 Mbps and 100 Mbps at half-duplex or full-duplex.
Autonegotiates 1000 Mbps at full-duplex.

- **AUTONEG_10**
Autonegotiates 10 Mbps at half-duplex or full-duplex.
- **AUTONEG_100**
Autonegotiates 100 Mbps at half-duplex or full-duplex.
- **AUTONEG_1000**
Autonegotiates 1000 Mbps at full-duplex.
- **10_FD, 10_HD, 100_FD, 100_HD, 1000_FD**
Sets link speed and duplex at these specified values with no autonegotiation.
- 1 G Fiber Interface
 - **1000_FD**
Sets 1000 Mbps at full-duplex with no autonegotiation.
- 10 G Fiber and Virtual
 - **10000_FD**
Sets 10000 Mbps at full-duplex with no autonegotiation.

Editing a Monitoring Interface

A monitoring interface can be edited but it cannot be deleted.

1. Go to Administration > General Traffic Settings: Capture Jobs/Interfaces, and click the Monitoring Interfaces tab.
2. With the mouse, hover over the interface to be edited and click the pencil icon on the right-end of the row.
3. In the Edit Monitoring Interfaces window, Link information shows the current status and settings of the interface.
4. Clear the check box to disable the interface; click the check box to enable the interface.
5. Revise the description.
6. Depending on the interface, select the speed and duplex from the dropdown list.
7. If you are using a packet broker, choose one from the dropdown menu.
8. Optionally, click to enable UDP deduplication or TCP deduplication. Note that TCP deduplication applies to TCP packets with their IP identification field set to 0.
9. Click **Apply** to make and save the edits. Click **Revert** to discard the edits.

Metrics in AppResponse 11

For TCP client and server metrics, AppResponse 11 collects a single set of metrics and employs three groupings:

- **Host Groups**—Aggregations of network IP addresses representing stores, plants, sales offices, business functions, or network tiers. Host group IP addresses can be clients or servers, depending on their role in a TCP connection. Host groups can contain member host groups, allowing the definition of a hierarchies in host groups.
- **TCP Clients**—IP addresses that open a connection, that is, it sends a SYN.
- **TCP Servers**—IP addresses that respond to A TCP Client SYN.

For example, data transfer time is a single metric that appears in three groupings:

- Total Data Transfer Time [sec]
- Request Data Transfer Time [sec]
- Response Data Transfer Time [sec]

These three groupings also make it easier to interpret the data presented in Navigator tables as the direction of the traffic reported (request or response) is determined by the type of table row (Client or Server), not the type of table column metric.

AppResponse 11 metrics also allow you to monitor traffic to and from Host Groups (external) as well as traffic between Host Group members and peers (internal). TCP Clients and TCP Servers

A Host Group can include both Clients and Servers. When you see a group that reads “*Group (c)*” the group refers to all IP addresses in the group that sent TCP data requests within the current time interval.

Figure 1-1. Client Groups

TCP Client Groups > Server Resets	
Group	Server TCP Resets [#] ↕
Default-10.x.x.x (c)	137
Default-192.168.x.x (c)	9
Default-Internet (c)	1
Default-172.x.x.x (c)	0

When you see a group that reads “*Group (s)*” the group refers to all IP addresses in the group that received and processed TCP data requests within the current time interval.

Figure 1-2. Server Groups

Bandwidth Usage		
Group	Total Throughput [Mbps]	Inbound Throughput [Mbps]
Default-Internet (s)	4.80	1.08
Other Group (s)	1.44	0.10
Default-192.168.x.x (s)	1.39	0.40
Default-10.x.x.x (s)	0.09	0.03
Default-172.x.x.x (s)	< 0.01	< 0.01

When you see an IP address that reads “IP address (c)” or “IP address (s)” it refers to an individual IP address acting as a client or as a server.

Figure 1-3. Web Client and Web Server IP Addresses

Top TCP Connections	
Group	
sfo1-ntap-prd-t3.nbtttech... (s)	10.33.24.62:954 (c)
74.125.157.85:80 (s)	-jh...-w7.nbtttech.com:51752 (c)
64.18.6.14:25 (s)	-192.168.77.27:46364 (c)
8.254.28.126:80 (s)	-aba...-w7.nbtttech.com:59986 (c)

Metrics for TCP Clients and TCP Servers

Metrics are measured from both the client request side and the sever response side. The client and server metrics are combined for a total of the metric. For example, the Payload Transfer Time Metric appears in these groupings:

- Request Payload Transfer Time
- Response Payload Transfer Time
- Total Payload Transfer Time

Other Metric Revisions in AppResponse 11

The following metrics are also available:

- **Throughput for Host Groups**— includes:
 - Internal traffic within the Host Group (member IP < - > member IP)
 - External traffic (member IP < - > connected IP)
- **Round Trip Time**—is a single metric in AppResponse 11. In legacy versions of AppResponse, it was split into two metrics, Inbound and Outbound.
- **Retransmission Delay**—is a sum of all packets lost in both directions (Client - > Server and Server - > Client). The Request Retrans Delay and Response Retrans Delay metrics identify retransmission delays by source.
- **Server Response Time**—measures only request processing time at the server tier.

Metrics for Web Transaction Analysis (WTA)

These metrics are available for AppResponse 11 WTA:

- Individual metrics for HTTP Response Codes of interest:
 - HTTP 100s
 - HTTP 200s
 - HTTP 300s misc, HTTP 304
 - HTTP 400, HTTP 400s misc, HTTP 401, HTTP 402, HTTP 403, HTTP 404, HTTP 407

- HTTP 500, HTTP 500s misc, HTTP 501, HTTP 503
- Five custom metrics can be configured to display web payload data, for example, SOAP values.
“See “Custom WTA Metrics/Columns” for more information.

User Response Time

User Response Time is a sum of the averages of the following four metrics:

“Connection Setup Time [msec]” + “Server Response Time [msec]” + “Total Payload Transfer Time [msec]” + “Total Retrans Delay [msec]”.

User Response Time estimates the average time for an application to process a TCP data request, and thus is a good measure of end-user response time.

Total Retrans Delay composition can be viewed as Request Retrans Delay [msec] and Response Retrans Delay [msec] to isolate the source of the delay.

Server Response Time

AppResponse 11 measures only request processing time at the server tier.

TCP Connection

A TCP connection observed by AppResponse 11. All Application Performance metrics labeled "(c)" and "(s)" are based on TCP Connections and the role of these IP addresses in these connections:

How AppResponse 11 Selects and Stores Top Elements

The disk space available for traffic data is finite on each appliance. This section describes the criteria used to select and store the most useful data for each time window.

General Notes

When selecting the top elements for a specific time window, AppResponse 11 considers criteria such as:

- Bidirectional throughput (top talkers)
- Preferred IPs
- IP addresses that triggered alerts
- Host Group membership (to ensure that all Host Groups are included)

Selecting Top Elements

AppResponse 11 retains detailed metrics for top elements based on throughput. It also calculates and retains aggregated total traffic, throughput, and utilization metrics for ALL traffic seen. To give priority to some IP addresses over others “preferred” IPs are used. For example, if an IP address has low traffic throughput and therefore may not be in the top elements, but you always want to store that IP no matter its traffic, then you can add it to the preferred IP list and priority will be given in the selection of top elements. To avoid selecting only preferred IP addresses, the top elements are split between preferred IP addresses and highest throughput IP addresses. See [“Preferred IPs” on page 144](#) for more information.

Common Workflows in AppResponse 11

AppResponse 11 workflows use the new web UI to monitor and troubleshoot your applications and network. In this section common workflows used in AppResponse 9.6.x are reviewed and then presented using the AppResponse 11 web UI.

Investigating a Web Application

I need to investigate my web applications, identify a potential problem, and drill down all the way to the packets for a poorly performing web page. How do I do that in AppResponse 11.1?

Investigating in AppResponse 9.6.x

In AppResponse 9.6.x this is typically done using a combination of the Web Application Performance and Individual Page Views insights.

1. You use the Web Application Performance Insight to get a summary of the important web applications, a list of web applications that have been filtered down by a *keyword* in their description fields.
2. You can identify specific key web apps that have a lot of slow pages, then select a web app and view the top page families for that web app.
3. You can then select a page family that also has a lot of slow pages and then right-click on it to launch the Individual Page Views Insight.
4. Now you can view the individual page views for that selected page family.
5. From here, you can select an individual page view and right-click to view its waterfall chart or download the packets associated with that page view to ATX, PA or Wireshark.

Investigating in AppResponse 11

In AppResponse 11, this is done using the Summary: Web Apps and Summary: Page Views insights. These two insights support the same investigatory workflows with the following differences:

- Unique Users and a breakdown of Page Time by Client/Network/Server Busy Time is supported for web apps and all its drill-downs (not limited to web apps-only and individual page views, respectively).
- The 95th Percentile Page Time metric is supported.
- The Summary: Page Views Insight contains:
 - a TruePlot scatter chart of actual page time measurements for each individual page view.
 - a waterfall chart (now called a Timeline) within the Insight. There is no need to launch a separate waterfall window via a right-click - simply select a different page view.
- There is no support for filtering the Navigator top table by keywords or tags in AppResponse 11 11.1.0. You can customize the Summary: Web Apps insight by doing the following:
 - Go to Insights > Actions: Launch/Manage.

- Open the Summary: Web Apps insight, then save the insight with a new name.
- For each chart or table in your insight, click the gear icon in the top right corner and change the data used from Top Groups to Specific Groups (click the radio button).
- Add all the important Web Apps that you want this insight to summarize.
- Click Save to keep the new web apps you added to the-insight.
- The Slow Page metrics are currently not supported.
- To view or download packets for an individual page:
 - Open the Summary: Page Views insight.
 - Right-click a Page View of interest and select Show TCP Connections.
 - Right-click a TCP conversation to download the packets or launch Steel Central Packet Analyzer Plus. From Packet Analyzer Plus the packets can be sent to ATX or Wireshark.

Interpreting TCP Performance Metrics

How do I interpret the TCP performance metrics that are shown in tables and charts?

Interpreting TCP Performance Metrics in AppResponse 9.6.x

The Application Stream Analysis (ASA) data groupings in AppResponse 9.6.x are IP-based only. As a consequence, all TCP performance metrics were duplicated, one calculated from when the group included TCP servers and the other calculated when the group included TCP clients. So, for example, the server response time metric has 2 variants: server response time (servers) and server response time (clients).

In addition, the reference is always the first group in a drill-down path. So, for example, if you are looking at the drill-down NY Branch Office BG > Connected IPs > 10.10.10.1, then all the metrics are reported from NY Branch Office BG. The server response time (servers) metric for this path would be from IPs within NY Branch Office BG that were identified as servers.

Some of the benefits to this approach:

- You can show both (servers) and (clients) metrics side-by-side to quickly see if a Business Group included IPs identified as TCP servers and/or TCP clients.
- When you drilled down from a group to its children, the traffic for a given metric always added up for a given direction or role: servers or clients

Some of the disadvantages to this approach:

Interpreting the metrics can be particularly challenging, especially when viewing a metric in the context of various drill downs. For example, server response time (clients) of NY Branch Office BG > Connected IPs > 10.10.10.1, is NOT the server response time of servers in NY Branch Office BG. It's actually the server response of the server 10.10.10.1.

Interpreting TCP Performance Metrics in AppResponse 11

The Application Stream Analysis (ASA) data groupings in AppResponse 11 are IP-based only, TCP servers and TCP clients. As a consequence, there are no variants of any TCP performance metrics. These groupings clarify how the TCP performance metrics are calculated:

- IP-based only TCP performance metrics are calculated by being agnostic as to whether the IPs have been identified as TCP servers or TCP clients. The metrics are averaged over measurements of both TCP servers and TCP clients. The measurements are IP-based only.
- TCP servers TCP performance metrics are calculated only for traffic identified as to or from TCP servers.
- TCP clients TCP performance metrics are calculated only for traffic identified as to or from TCP clients.

As an example, host groups are presented in three groupings: host groups, server groups and client groups. The NY Branch Office BG in AppResponse 9.6.x would be presented in AppResponse 11 as:

- NY Branch Office HG
- NY Branch Office HG (s)
- NY Branch Office HG (c)

There is only one version of each TCP performance metric (for example, server response time (SRT)).

SRT for NY Branch Office HG is averaged over all servers in the NY Branch Office and all clients in the NY Branch Office connecting to various servers. SRT for NY Branch Office HG (s) is averaged over all TCP servers in the NY Branch Office. SRT for NY Branch Office HG (c) is averaged over all TCP clients in the NY Branch Office connected to various servers.

In AppResponse 11, the reference is always the last group in a drill-down path. For example, if you are looking at the drill-down NY Branch Office HG > Connected IPs > 10.10.10.1, all the metrics are reported from 10.10.10.1. The server response time (servers) metric for this path would be for 10.10.10.1 when it was identified as a TCP server.

Some of the benefits to this approach:

- Interpreting the metrics is simplified, especially when viewing a metric in the context of various drill-downs. All the information needed to interpret the metric is included in the last group in a drill-down path. For example, the server response time of NY Branch Office HG (c) > Connected IPs > 10.10.10.1 (s), is the server response of the server 10.10.10.1.

Some of the disadvantages to this approach:

- You can no longer show both (servers) and (clients) metrics side-by-side to quickly see if a Host Group includes IPs identified as TCP servers and/or TCP clients. To support this discovery workflow, you need to add the Server Group and Client Group to a Navigator Favorites. From there you can see the relative amounts of server and client traffic by comparing adjacent rows instead of adjacent columns.
- When you drilled down from a group to its children, the traffic for a given metric may not add up for direction metrics. For example, consider Inbound and Outbound metrics. The Throughput (Inbound) for NY Branch Office HG is reported as Throughput (Outbound) for NY Branch Office HG > Connected IPs.

Troubleshooting Host Groups and Applications

When troubleshooting investigations, I always begin with the same fixed set of Business Groups (AppResponse 11 Host Groups) and Applications. I typically want to drill down into these groups and view their performance in time series charts. How do I use AppResponse 11 to support these key workflows?

Troubleshooting Business Groups and Applications with AppResponse 9.6.x

Favorites Tables and Projects are the two key features in the Java Console that are used to support these common troubleshooting workflows. Troubleshooting typically starts with a top table to find key Business Groups or Applications or both. You then add them to a Favorites Table, either by drag-and-drop or using the Add To > Favorites right-click link. You can also add the groups directly by clicking on the Add button in the Favorites Table toolbar.

Once you have your key groups in a Favorites Table you have a single starting place to start your investigations. You can add relevant metrics to the Favorites Table, drill down into a group to get various supported breakdowns, or double-click on a cell to get a time series chart of that group and metrics that the cell represents.

The Group Chooser behaves a little differently in AppResponse 9.6. It is split into a 2-step process. You first select the type of group or drill-down from the Select Group dialog. The labels are displayed in plural rather than singular form (e.g. Apps, instead of App). Once you've selected the type of drill-down, click OK, and that group/drill-down is added to the Select Filter/Group dialog. You can then select specific groups for each group type in your drill-down by clicking on the pencil edit icons.

To make that Favorites Table with all the groups and metrics I've added available to me every time I run the Java Console, I save my current Favorites Table in a Project, and then configure the Java Console to automatically load this project every time I launch the Java Console.

Troubleshooting Business Groups and Applications with AppResponse 11

Navigator is the feature used in troubleshooting workflows. In AppResponse 11 you define and configure groups and applications in the web UI (Business Groups are called Host Groups in AppResponse 11). The Navigator top table enables you to select and view related groups of aggregated application and network traffic data, along with selectable metrics. Launch Navigator by selecting a group type of interest from the Navigator drop-down list in the main menu, or select More to review all group types in the navigation panel before making a selection.

Expanding a row in a group displays associated subgroups and their data for each metric (column). Symmetrical groups provide multiple paths to the same data, for example, you can start with an application and drill down to related TCP Server Groups or you can start with a TCP Server Group and drill down to the applications.

You also can create custom groups, known as Favorites, containing groups you typically use when troubleshooting. A Favorite can be saved and updated as you explore in Navigator, selecting groups in top table rows or workspace charts and tables. If you have selected multiple groups, click on the Add to Favorites button (the star icon) in the Navigator toolbar. If you have a single group selected, you can either click on the Add to Favorites button, or right-click on the group and select Add to Favorites in the list of options. In AppResponse 11, the right-click menu applies only to the row you've currently selected, unlike in AppResponse 9.6 where the right-click menu can apply to a multi-row selection. Also, the ability to add one of the groups in your selected drill-down path is not supported in AppResponse 11.

The Add to Favorites dialog window gives you the option to either add the group to a new Favorite (default) or add it to an existing Favorite. When you create a new Favorite, the top table and workspace are automatically saved. *Subsequent changes, for example, adding more charts or tables in the workspace) are only saved if you click on the disk icon (Save button) in the top-right corner of the Navigator toolbar.*

An AppResponse 11 Favorites table behaves much like an AR 9.6 Favorites table. You can drill down into any group you've added to the top table and access any of its supported drill-downs. You can add or remove groups with the Add or Delete buttons in the Navigator toolbar. You also can modify what table columns (metrics) are displayed and their order (click the Open Column Chooser icon in the Navigator toolbar).

The Navigator Favorites is really a hybrid combination of these AR 9.6.x features:

- Favorites Table
- Insight
- Project

In AppResponse 11 the workspace below the Favorites Table displays a time series chart by default. Every time you select one or more groups in the Favorites Table, it's automatically added to the time chart. You can add additional charts and tables (widgets): for example, RTC, multi-metric time chart, pie or bar chart. All of the widgets you add to the workspace behave in the same manner when you select one or more rows in the Favorites Table. The selected groups are automatically added to those widgets. You not only want to add the important groups to your Favorite top table, you also want to add all the key charts and tables that you use when investigating trouble; configure them with the appropriate metrics and formats through the chart's settings. To bring up a chart's settings, hover your mouse over a chart area, and click on the gear icon in the upper right corner.

Important: Be sure to save your Navigator Favorites once you are done with your changes (just like an AR 9 Project). Click on the disk icon (Save button) in the top-right corner of the Navigator toolbar.

To launch a Navigator Favorite, open Navigator and select the Favorites from the left Navigation Pane under the Favorites section. You can launch the Navigator with just the Favorites section expanded to list your Navigator Favorites by selecting List under the FAVORITES section of the Navigator drop-down list from the main menu bar.

Unlike Projects which are stored locally on a client's system, Navigator Favorites are stored on AppResponse 11 itself. You can allow other users access to your Navigator Favorites by enabling the Public or Shared option under Access when saving your Favorites. The Public option lets other users use your Navigator Favorites, but they cannot save and overwrite your Navigator Favorites with changes they make to the Favorites table or the workspace. They can save their changes to a new Navigator Favorites. The Shared option however, does give other users the option to save and overwrite your Navigator Favorites with any changes they have made.

Configuration

The options in this section affect system-wide settings. Some options, for example, Base Interfaces, are configured in the installation process. Changes can be made to those settings here. Other options, such as SSL Decryption, need to be configured before data decryption can be used in WTA. Changes to these settings can only be made by a user with read/write system configuration permissions.

Licensing

AppResponse 11 requires a license to operate. The installed license includes Feature Keys that determine the software options and capabilities available in AppResponse 11. The header line at the top of each web UI page shows the AppResponse 11 system model and license. If no license is installed “UNLICENSED” follows the model. Instructions for installing a license on AppResponse 11, either appliance or virtual edition, are contained in the installation guide for each product.

When installed, if AppResponse 11 is connected to the Internet, licenses are automatically added when a connection is made to the Riverbed Licensing site at <https://licensing.riverbed.com>. A license can be manually installed if AppResponse 11 is not connected to the Internet.

This section covers AppResponse 11 licensing:

- “Licensing Overview” on page 22
- “Licensing Toolbar” on page 24
- “Adding a License” on page 24
- “Deactivating a License” on page 24
- “Deleting a Feature Key” on page 25
- “Restoring a Feature Key” on page 25

Licensing Overview

With a license, Feature Keys are installed automatically if AppResponse 11 is connected to the Internet, or manually if it is not. Feature Keys enable AppResponse 11 Shark Packet Analysis (SPA) to operate. They also may include optional modules such as Application Stream Analysis (ASA) and Web Transaction Analysis (WTA) that expand the product’s capabilities.

AppResponse 11 uses two different types of licenses, one type for appliances and one for virtual editions:

- When AppResponse 11 is installed on an appliance, the license is for that appliance serial number and can only be used on that appliance. It cannot be moved to another appliance.
- When AppResponse 11 virtual edition is installed on a virtual system, the license is for the product key specified by the customer. This license can be activated or deactivated for use with any AppResponse 11 virtual edition.

While each license type installs Feature Keys that enable AppResponse 11 to operate, their components are not the same.

Appliance Licenses and Terminology

An appliance license is tied to the appliance’s serial number. When a new appliance is connected to the Internet, the license is installed automatically from the Riverbed Licensing site. Appliances without an Internet connection must install a license manually. The terms below provide specific information about an appliance license;

- **Appliance Serial Number**—The serial number assigned by Riverbed to the appliance. This can be used to retrieve the license from the Riverbed Licensing site.

- **License Status**—Current operating state of the license.
- **Activation Status**—The following status information is displayed:
 - **Activating.** The supplied Product Key is being processed by the License Manager.
 - **Disconnected.** The Feature Keys were successfully added manually.
 - **Failed to Contact Provider.** The Feature Keys must be added manually. The status changes to Disconnected when the Feature Keys are successfully added.
 - **License Already Assigned.** The license is already in use. This license must be deactivated and deleted before a new license can be added.
 - **License Not Found.** A license cannot be found for the Product Key entered. This license must be deactivated and deleted before a new license can be added.
 - **Successful.** The Feature keys have been automatically added by the provider.
- **Last synced**—Last contact with the Riverbed Licensing site over the Internet.
- **Feature Keys**—License-specific keys to activate software and product capabilities.

Virtual Edition License Terminology

AppResponse 11 virtual edition requires a virtual edition license, not an appliance license. While a virtual edition license can only be used on one AppResponse 11 virtual edition at a time, the license can be activated and deactivated, allowing the same Product Key to be used again to license a different or the same AppResponse 11 virtual edition. The terms below provide specific information about a virtual license;

- **License Manager**—The name of the license source, also known as the provider.
- **Product Key**—A Riverbed supplied key used to retrieve a license from the Riverbed Licensing site on the Internet.
- **License Status**—Current operating state of the license.
- **Last synced**—Last contact with the Riverbed Licensing site over the Internet.
- **Email**—Email address of the customer installing the Product Key.
- **Activation Code**—A code provided by the Riverbed Licensing site that identifies the active license.
- **Deactivation Code**—A code identifying a deactivated license. If connected to the Internet at deactivation, the same product key can now be used again to license an AppResponse 11 virtual edition. If not connected to the Internet, the Deactivation Code can be entered on the Riverbed Licensing site or provided to Support to enable the same product key to be used again.
- **Activation Status**—The following status information is displayed:
 - **Activating.** The supplied Product Key is being processed by the License Manager.
 - **Disconnected.** The Feature Keys were successfully added manually.
 - **Failed to Contact Provider.** The Feature keys must be added manually. The status changes to Disconnected when the Feature Keys are successfully added.
 - **License Already Assigned.** The license is already in use. This license must be deactivated and deleted before a new license can be added.

- License Not Found. A license cannot be found for the Product Key entered. This license must be deactivated and deleted before a new license can be installed.
- Successful. The Feature keys have been automatically added by the provider.
- Feature Keys—License-specific keys to activate software and product capabilities.

Licensing Toolbar

The toolbar, located just above the table, contains the following tools:

- **Sync**—Click to contact the Riverbed Licensing site to synchronize a license. Click **Sync** to activate an appliance license when connected to the Internet if the license has not yet been activated.
- **Import**—Click to install Feature Keys.
- **Export**—Click to create a text file containing the installed Feature Keys.
- **Deactivate**—Click to deactivate an active license (virtual edition licenses only). Only licenses with an active license status can be deactivated. If connected to the Internet, deactivating a virtual edition license takes effect immediately. The same Product Key can now be used to license an AppResponse 11 virtual edition.

If not connected to the Internet, the Deactivation Code can be entered on the Riverbed Licensing site or provided to Support to enable the same Product Key to be used again to install a license on an AppResponse 11 virtual edition.

Note: A license must be deleted after it is deactivated.

Adding a License

See the Installation Guide for your AppResponse 11 appliance or virtual edition for these instructions.

Deactivating a License

To deactivate a virtual edition license do the following:

1. Check that the current license has the following:
 - A Product Key. This ensures the license can be deactivated and the Product Key used again. Appliance licenses are tied to the appliance serial number and can only be used on that appliance
 - The license status is active. Only active licenses can be deactivated.
2. Click **Deactivate** in the toolbar.
3. A pop-up window appears explaining the impact of deactivating a license. Click **OK** to continue or **Cancel** to retain the license.
4. In the new window you must click **Delete License** to generate a Deactivation Key and to allow a new license to be installed. If connected to the Internet, deactivating a virtual edition license takes

effect immediately. The same Product Key can now be used to license an AppResponse 11 virtual edition.

If not connected to the Internet, the license deactivation takes place immediately. The Deactivation Code can be entered on the Riverbed Licensing site or provided to Support to enable the same Product Key to be used again to install a license on an AppResponse 11 virtual edition.

Deleting a Feature Key

Important: Feature Keys are associated with a specific license and cannot be transferred from one AppResponse 11 to another. A virtual edition license can be used on another AppResponse 11 virtual edition, but it can only be used on one AppResponse 11 virtual edition at a time.

A deleted Feature Key is effective immediately.

To delete a Feature Key:

1. Go to Administration > Other: Licensing in the web UI.
2. Hover over the left end of the row that contains the Feature Key to be deleted.
3. Click the 'x' that appears.
4. Click **Delete** to remove the Feature Key or **Cancel** to discard any change.

Restoring a Feature Key

A Feature Key can be restored only on the licensed AppResponse 11 it was removed from. Feature Keys cannot be moved to an AppResponse 11 with a different license.

To restore a deleted Feature Key

- For AppResponse 11 appliances or virtual editions connected to the Internet
 - A periodic sync with the Riverbed Licensing site restores a deleted Feature Key after a period of time.
 - Clicking **Sync** on the toolbar.
- For AppResponse 11 appliances or virtual editions *not* connected to the Internet
 - Obtain the Feature Key from the Riverbed Licensing site and re-enter it manually.
- Deactivate and reactivate the entire license (virtual edition only):
 - On a virtual edition you can deactivate the entire license, submit the deactivation code on the Riverbed Licensing site or to Riverbed Support and reactivate the license using the same product key.

Note: Deactivating a license stops AppResponse 11 operation until the license is reactivated.

Administration - Authentication

This section is where you create and manage AppResponse 11 users; define roles and their permissions; and configure the user authentication process.

- [“User Administration and Account Policy” on page 26](#)
- [“Roles and Permissions” on page 27](#)
- [“Remote Authentication” on page 34](#)

User Administration and Account Policy

Choosing Administration > Account Management: User Administration displays the User Administration and Account Policy page providing controls for creating and managing user accounts for AppResponse 11.

- **Local Users tab** — Create and manage individual user accounts, including the roles with which they’re associated.
- **Roles and Permissions tab** — Create and manage the profiles that specify the activities to which associated users have Read or Write privileges.
- **Password Policy tab** — Configure global login and password policies for all user accounts.

Note: When the set of user account definitions or user roles has been selected in the Portal Integration page to be managed solely from SteelCentral Portal, the User Administration and Account Policy page in AppResponse 11 will display a message stating that those objects are being managed from the portal, and cannot be edited using AppResponse 11.

Local Users tab

The Local Users tab shows details for each existing user account. User accounts can be added, edited, or deleted.

Creating a New User Account

To create a new user account:

1. Click **Add** in the Local Users tab to display the New User dialog.
2. **Name**—The user account's unique ID. User account names must be from 2 to 32 characters long and start with a letter. Lowercase alphanumeric characters, dash, and underscore can be used.
3. **Description**—Type a brief explanation of the user account's purpose, if desired.
4. **Password**—Type the user account's password.

5. **Verify Password**—Type the user account's password again to ensure that it is defined explicitly.
6. **Roles**—Specify one or more of the user roles defined on the appliance. The set of valid roles is user-defined; only the System Administrator role is built-in.

Editing a User Account

1. Edit an existing user account by highlighting it and clicking the pencil icon to display the Edit User dialog.
2. The Edit User dialog provides the same controls as the New User dialog.

Deleting a User Account

Note: It is possible to delete the admin account that is provided by default. The system does not prompt you for confirmation before executing this action.

1. Highlight the user to be deleted.
2. Click the **x** at the end of the row.
3. Click **Delete** to remove or **Cancel** to keep the user.

Password Policy tab

The Password Policy tab enables you to configure global settings that affect all user accounts.

- Allow Empty Passwords
- Minimum Password Length
- Minimum Number of Lowercase Characters
- Minimum Number of Uppercase Characters
- Minimum Number of Digits
- Minimum Number of Symbols
- Maximum Number of Character Repeats
- Minimum Number of Character Changes
- Check the Password For Common Words
- Number of Days a User Must Wait Between Password Change
- Number of Previous Passwords to Check

Roles and Permissions

Role Based Access Control (RBAC) protects the system by assigning different access privileges to different user roles. User roles are then assigned to user accounts. A user's privileges on the system are determined by which roles the system administrator assigns to their account. Each account can be assigned one or more roles.

Some features of the product are accessible to all users. Others are accessible to only users whose user roles have the required permissions. If a user account does not have a role with permissions for a feature, then the menu choice for the feature is not displayed.

Roles

The product is preconfigured with the System Administrator role. Use the Administration > Account Management: User Administration page, Roles and Permissions tab to create additional user roles.

To create a new user role:

1. Go to the Administration > Account Management: User Administration page and click the Roles and Permissions tab.
2. Choose the Add button to open the New Role page.
3. Enter a name for the role.
4. Enter a description of the role. This is visible on other pages and is optional.
5. Select the access permissions that this role will give the user accounts it is assigned to. You can hover your mouse over the Permission name for a brief description of the associated user privileges. Permissions are described in more detail below.
6. Choose Save.

The definition of the new role is displayed in the Roles and Permissions tab. After being defined, the role becomes available to be assigned to individual user accounts in the Local Users tab.

To edit a user role:

1. Go to the Administration > Account Management: User Administration page and click the Roles and Permissions tab.
2. Hover your mouse in the row for the role you want to edit. This displays an edit icon (pencil) and a delete icon (x). Choose the edit icon to display the Edit Role page.
3. Edit the role definition.
4. Choose Apply to make the changes or choose Revert to return to the previous definition.

Permissions

A permission is a group of rules defining what actions are available to a user role. When the role is assigned to a user account, the permissions for the role define what the user account can do. For each permission, the user role can be given read-only access or read/write access.

The following permissions can be assigned to a user role.

- “RBAC configuration (Role Based Access Control)”

- “All objects”
- “System configuration”
- “Network packets”
- “Job configuration”
- “Application configuration”

The access these permissions grant to a user role are as follows:

- RBAC configuration (Role Based Access Control)
 - Read-only - View all user configurations, including:
 - List of all users and roles
 - Assignment of users to roles
 - Remote authentication configuration
 - Read/write - View and edit all user configurations, including:
 - Creating and removing locally authenticated user accounts
 - Changing user passwords
 - Changing the login and password policies for the user account
 - Note that locally authenticated users can change their passwords without requiring any specific permissions.
- All objects
 - Read-only - View all objects that are stored for users on the system, such as packet capture files.
 - Read/write - View and delete all objects that are stored for users on the system.
- System configuration
 - Read-only - View system settings, including:
 - Base Interfaces
 - Monitoring Interfaces
 - Monitoring Interface Groups
 - DNS and Hosts
 - Time
 - Announcements
 - Reboot/Shutdown
 - Capture Jobs
 - Flow Export
 - Recipients
 - Email
 - SSL Decryption

- Server Response Time Analysis
- System Alert Recipients

Read/write - View and change all the system settings listed above. This permission does not include user administration.

■ Network packets

Read-only - View the following:

- Live packet streams
- Packet capture or trace files (.pcap files) stored on the appliance (viewed from Packet Analyzer Plus).
- Capture job flow data

This permission is required for exporting packets. It is also required for viewing data from packets in a trace clip by accessing Packet Analyzer Plus from the Navigator. It is not required for viewing information about trace clips.

Read/write - Enables you to:

- Upload .pcap files to the appliance
- Save trace clips to .pcap files
- Save live packet streams to .pcap files
- Access packet data requests
- Access the pcap API and the trace clips API

The Network packets permission allows you to view .pcap files that you own or that have been shared with you by another owner. If another owner does not share the file with you, then you cannot view it even with this permission.

■ Job configuration

Read-only - View packet capture job configurations and statistics. If a role has read-only access with the Network packets permission, then the role needs this permission also in order to view packets in capture jobs.

Read/write - Create, modify, delete, start, stop, and clear packet capture jobs.

■ Application configuration

Read-only - View settings for the following:

- Host Groups
- Applications
- Preferred IPs
- Port Aliases
- Policies
- Module configuration
- System Response Time
- Page Analysis

- Information Privacy
- User Session Tracking
- Capture Jobs

Read/write - Change the configurations for these. Access to all data processing configuration.
Does not include job configuration.

Permissions from multiple roles

If more than one role is assigned to a user account, the user receives the highest level of privilege available from any of the roles. For example, assume that Role A and Role B both include the system configuration permission. However, the permission is read-only for Role A and read/write for Role B:

Role A

- RBAC configuration read-only
- System configuration read-only

Role B

- System configuration read/write

If a user account is assigned both Role A and Role B it will have the following permissions:

- RBAC configuration read-only
- System configuration read/write

Roles having no permissions

A user that has logged in to the web UI successfully, but does not have any role associated with its username, does not have any explicit permissions. Such a user can perform the following actions in the web UI:

- Navigate through the metrics visible in the web UI using the Navigator and Insights.
- Change its own password and user preferences (e.g. the time style, or his own language).
- Create/modify/delete its own report schedules and view its own reports (or the ones shared with it). The user can configure an email recipient for such a schedule, but cannot configure the SMTP server.
- Create/modify/delete its own favorites.

Objects such as reports and .pcap files that are owned by a user can be shared with other users. One method of limiting access to an owned object is to create a role with no permissions and then assign that role to user accounts that are to share access to the owned object.

Default User Preferences

Choosing Administration > System Settings: Default User Preferences displays the Default User Preferences page. This page provides controls for setting basic display defaults for all users of this AppResponse 11 system. This page is very similar to “User Preferences”, which provides the same controls to individual users, so that they can customize these display settings to suit their own personal preferences.

There are two tabs: Default User Preferences and “Default Metric Colors”.

- Language: Choose a supported language from the pulldown menu. This is the default language that the web UI will use for all users of this system.
- System Time Zone: This value is read-only on this page, configured elsewhere at Administration > System Settings > Time
- When displaying time zone, show as: The specifics will vary, according to the System Time Zone that is set.
- Date Style: Choose your preference.
- Time Style: Choose your preference.
- Data Units:
 - When displaying Traffic Volume, by default show: Choose your preferred units.
 - When displaying Traffic Throughput, by default show: Choose your preferred units.
- Default Insight:
 - Show an Insight on the Home Page: Deselect if you don't want to see an insight on the home page. Otherwise, choose the insight you want to see every time you transit the Home page.
 - Dashboard auto-refresh interval (minutes): Specify the number of minutes at which you want dashboards to update automatically.
- Search Settings:
 - Timeout after n seconds
 - Limit configuration results to n
 - Search data [selected by default]
 - Search data during last n seconds
 - Limit data results to n

Default Metric Colors

The Default Metric Colors tab, available under Administration > System Settings: Default User Preferences, displays a list of AppResponse 11 metrics and a color associated with each. These colors control how the metrics are displayed in the following widget types, in which a color is associated with each metric:

- Bar Chart widget
- Multi-Metric Time Series Chart widget

- Response Time Composition Chart widget
- TruePlot widget

The Metric checkbox at the top of the list provides a convenient way to select all default metric colors if you want to delete all the default metric colors.

For any metric, click on its color to display the Color Picker and select or define a new color to associate with it.

Metric color definitions can be imported and exported via CSV file. Clicking Export writes the current set of metric color definitions to the file “default-metric-colors-export.csv”. If you want to read in a set of metric color definitions, click Import and specify the name of the CSV file to use. The metric definition file includes three columns: the metric ID, the metric name, and the RGB color definition associated with it. For example:

Id	Metric	Color
avg_web.client_busy_time_normalized	Client Busy Time (Normalized)	rgb(69,114,167)

At any time, click Restore if you want to return to the system default metric colors.

Remote Authentication

AppResponse 11 can use RADIUS and TACACS+ authentication servers in addition to local password user authentication (the default), or can use SAML 2.0 authentication instead of the other types. Once authenticated, a remote user can be assigned a role (authorized) either by the authentication server or identity provider, or by a default role configured in AppResponse 11. If authentication and authorization succeed, the appliance logs the user in. If either authentication or authorization fail, the appliance displays an error message and records an unsuccessful login attempt in the audit logs.

When using remote authorization:

- You can configure a maximum of two RADIUS and two TACACS+ remote servers.
- You can specify a sequence of authentication types with prioritized servers in each type. For example, you could specify RADIUS, TACACS+, and Local as the sequence to be used when authenticating users. Place each authentication server in the order you want requests to be processed. However, if you enable SAML 2.0 authentication, RADIUS, TACACS+, and local authentication all will be disabled, and only the SAML identity provider will authenticate users.
- Command accounting is not supported.

Important: Passwords are encrypted using a RADIUS or TACACS+ shared secret when a request is sent to an authentication server. These keys are not stored in an encrypted format by AppResponse 11.

This section covers:

- [“Remote Authentication” on page 34](#)
- [“RADIUS Authentication” on page 37](#)
- [“TACACS+ Authentication” on page 38](#)
- [“Setting Up Remote Authentication” on page 39](#)
- [“SAML 2.0 Authentication” on page 41](#)

Remote Authentication

By default, AppResponse 11 installs a local user “admin” with a System Administrator role. This user is stored in a local file. AppResponse 11 also supports remote authentication using RADIUS and TACACS+ authentication servers, as well as SAML identity providers. Remote authentication enables an authenticated user to sign in on any AppResponse 11 system in the management network. A remote user does not need a local account to be authenticated when using RADIUS, TACACS+, or SAML.

The authorization (roles) for a remote user can be specified:

- by the remote authentication server using a RADIUS or TACACS+ Vendor Specific Attribute (VSA).
- by a default role configured in AppResponse 11 (see [“Default Roles” on page 36](#) below).

A remote user:

- Does not inherit a role from a local account of the same username.

- Sees the same private files when logged in using remote authentication as if they were authenticated locally.

General Tab

Defining a Login Banner Message

Type a message of up to 20,000 characters to be displayed to all users whenever they begin to log in to the AppResponse 11 system via web UI, console, or Packet Analyzer Plus. The banner supports Unicode; UTF-8 is used for console/serial and SSH sessions.

Configuring the Web UI Session Inactivity Limit

Specify the length of time that a web UI session can be idle before the user is logged out automatically. By default, this is enabled and set for 60 minutes.

Configuring a Sequence of Authentication Types

Note: If you enable SAML 2.0 authentication, RADIUS, TACACS+, and local authentication all will be disabled, and only the SAML identity provider will authenticate users.

When RADIUS and TACACS+ authentication servers are configured in AppResponse 11 you can add them to a sequence of authentication types (Local, RADIUS, or TACACS+) to be used when a user signs in. Authentication requests are made from the highest priority authentication type (1) to the lowest. Within each authentication type, requests are sequentially made to the configured servers in the order they appear in on the RADIUS and TACACS+ tabs. Authentication requests are made until a server accepts or rejects a request or the authentication types are exhausted.

- If a server does not respond, authentication proceeds to the next server.
- If authentication is rejected, there is no provision to try the next server of the same authentication type. For example, if two RADIUS servers are configured and the first server rejects a user, the second RADIUS server is not contacted. You can choose to try the next authentication type if a higher-priority authentication type rejects a request. See [“Setting the Sequence of Authentication Types” on page 36](#) for details.

Important: If not careful, you can lock yourself out of AppResponse 11 by doing the following:

- Removing Local authentication from the sequence and the remote servers (RADIUS or TACACS+) are unreachable.
- Clearing the “Try next method on reject:” check box ([Step 6 on page 36](#)).

Riverbed recommends checking that authentication using RADIUS and TACACS+ works successfully before you remove local authentication or clear the “Try next method on reject.” check box.

If locked out, contact Riverbed Support to recover the AppResponse 11 appliance or virtual edition.

Specifying Authentication Types

1. Go to Administration > Account Management: Authentication to display the Authentication page.

2. Select the General tab.
3. A table shows the authentication types currently selected (Local by default).
4. Click **Add** to display a pop-up menu with other available authentication types.
5. Click **Add** following an authentication type to add it to the table.
6. When finished click the **x** in the upper-right corner of the pop-up menu.

Setting the Sequence of Authentication Types

1. Go to Administration > Account Management: Authentication to display the Authentication page.
2. Select the General tab.
3. A table shows the authentication types currently selected (Local by default).
4. The priority of each authentication type is shown in column 1, highest (1) to lowest.
5. Use three icons on the right-side of each table row to change a row's priority:
 - Click **^** to raise an authentication type's priority.
 - Click **v** to lower an authentication type's priority.
 - Click **x** to remove the authentication type.
6. Selecting the "Try next method on reject:" box (below the table) tries the next authentication type if a higher priority authentication type rejects a request. By default, this box is checked and a rejected request tries the next authentication type in the sequence.

Default Roles

Authorization occurs in one of two ways when using RADIUS and TACACS+ authentication:

- by the remote authentication server using a RADIUS Vendor Specific Attribute (VSA).
- by a default set of roles configured on the requesting AppResponse 11.

When a user is authenticated, roles sent in VSAs are assigned to the user.

- Any role not found in the requesting AppResponse 11 generates a log message and is otherwise ignored.
- If the VSA is empty or contains no valid roles, the user will have no permissions.
- If the VSA is not returned by the remote server, a default role configured on the requesting AppResponse 11 is assigned.
 - If no default roles are configured on AppResponse 11, the user will have no permissions.

Roles are created at Administration > Authentication: Roles and Permissions in the AppResponse 11 web UI ("**Roles and Permissions**" on page 97). These roles are shown under Default Roles at the bottom of the Remote Authentication tab.

Configuring default roles

1. Go to Administration > Account Management: Authentication to display the Authentication page.
2. Select the General tab. The Default Roles table shows the Roles configured on the AppResponse 11.
3. To include a role in the set of default roles, select the check box in the Default column.
4. When finished, the selected roles are the default roles, available if no roles are sent by the authentication server.

Important: Roles sent in a VSA are checked against the roles on the AppResponse 11. If no roles match, the user has no authorization.

RADIUS Authentication

Up to two RADIUS authentication servers can be configured and managed on the RADIUS Configuration tab. A toolbar in the top-left corner of the configured servers is used to add or delete servers. Hover your mouse over the right end of a row containing a selected server to edit or delete that server. When the first authentication server is specified, a priority table appears above the configured servers, along with a drop-down menu used to specify the encryption protocol used.

Configuring RADIUS Authentication

1. Go to Administration > Account Management: Authentication to display the Authentication page.
2. Select the RADIUS tab. A table shows the configured RADIUS Servers.
3. Click the **Add** button in the toolbar. A New RADIUS Server window is displayed.
4. Specify a host, identified using:
 - An IPv4 address
 - A host name
5. Specify the UDP port used for authentication.
6. Specify the shared secret key used to encrypt traffic to and from the server. Toggle the Enable checkbox to make this field editable.
7. Specify the timeout period in seconds. Up to 30 seconds can be entered.
8. When finished, click **Save**. To discard any entries, click **x** in the upper-right corner of the window.

Setting the RADIUS Encryption Protocol

You can change the encryption protocol used by the RADIUS servers (default PAP). Select from the following list of protocols:

- CHAP
- MSCHAP1
- MSCHAP2
- PAP

Setting RADIUS Server Priority

When the first authentication server is specified, a Priority table appears above the configured servers.

Setting the Sequence of RADIUS Authentication Servers

1. Go to Administration > Account Management: Authentication to display the Authentication page.
2. Select the RADIUS tab.
3. A table shows the authentication servers configured.
4. The priority of each server is shown in column 1, highest (1) to lowest.
5. Use the two icons on the right-side of each table row to change a row's priority:
 - Click ^ to raise an authentication type's priority.
 - Click v to lower an authentication type's priority.

TACACS+ Authentication

Up to two TACACS+ authentication servers can be configured and managed on the TACACS+ Configuration tab. A toolbar in the top-left corner of the configured servers is used to add or delete servers. Hover your mouse over the right end of a row containing a selected server to edit or delete that server. When the first authentication server is specified, a priority table appears above the configured servers, along with a drop-down menu used to specify the encryption protocol used.

Configuring TACACS+ Authentication

1. Go to Administration > Account Management: Authentication to display the Authentication page.
2. Select the TACACS+ tab. A table shows the configured TACACS+ Servers.
3. Click the **Add** button in the toolbar. A New TACACS+ Server window is displayed.
4. Specify a host, identified using:
 - An IPv4 address
 - A host name
5. Specify the UDP port used for authentication.
6. Specify the shared secret key used to encrypt traffic to and from the server. Toggle the Enable checkbox to make this field editable.

- When finished, click **Save**. To discard any entries, click **x** in the upper-right corner of the window.

Setting the TACACS+ Timeout

Select the timeout period in seconds (default 3 seconds) in the Timeout box. A time from 1 to 30 seconds can be selected.

Setting TACACS+ Server Priority

When the first authentication server is specified, a priority table appears above the configured servers.

Setting the Sequence of TACACS+ Authentication Servers

- Go to Administration > Account Management: Authentication to display the Authentication page.
- Select the TACACS+ tab.
- A table shows the authentication servers configured.
- The priority of each server is shown in column 1, highest (1) to lowest.
- Use the two icons on the right-side of each table row to change a row's priority:
 - Click **^** to raise an authentication type's priority.
 - Click **v** to lower an authentication type's priority.

Setting Up Remote Authentication

A RADIUS or TACACS+ authentication server needs information about an AppResponse 11 before it can successfully respond to an authentication request. A summary of the required information and an example configuration for RADIUS and TACACS+ servers is provided below. These instructions assume you have an existing authentication server to which you are adding an AppResponse 11. For information on setting up an authentication server, please see the documentation that came with the authentication server.

RADIUS Server Information

Modify or create a vendor file

Add and save an AppResponse 11 attribute to the Riverbed RADIUS vendor file:

- The Riverbed RADIUS vendor ID is 17163.
- Add the attribute 'Riverbed-Roles-List' with value 10, type 'string' to the file.

Here is an example showing this change added to a FreeRADIUS authentication server:

```
/usr/share/freeradius/dictionary.riverbed
# -*- text -*-
VENDOR          Riverbed          17163
BEGIN-VENDOR     Riverbed
ATTRIBUTE        Riverbed-Local-User 1      string
ATTRIBUTE        Riverbed-Roles-List 10     string
```

END-VENDOR Riverbed

The example above also shows the attribute used by Riverbed SteelHead.

Note: A vendor ID can only be used in a single file. If there is an existing file using the Riverbed vendor ID add the AppResponse 11 attribute to the existing file and save the change.

Add available roles (optional)

The authorization (roles) for a remote user can be specified by the RADIUS server using a Vendor Specific Attribute (VSA). If the VSA is not returned by the remote server, then the default role configured on AppResponse 11 is assigned. If the VSA is present, but empty, or if no default roles are configured on AppResponse 11, no roles are assigned to the user.

The vendor value is a comma-separated list of role names (case sensitive). Valid values match the roles created in AppResponse 11. For more information, see [“Roles” on page 97](#).

TACACS+ Server Information

Add available roles (optional)

The authorization (roles) for a remote user can be specified by the TACACS+ server using the Vendor Specific Attribute (VSA) "riverbed-roles-list", added under the "system" service.

An example of a defined role appears below.

```
user = tacplus {
    login = cleartext "tacplus"
    service = system {
        riverbed-roles-list = "System Administrator"
    }
}
```

Restricted packet access (optional)

User access to packet data can be controlled finely through the use of a TACACS+ VSA named “riverbed-hg-pkt-filter”, which enables you to restrict packet access for specific users to only those packets originating from IP addresses in specific host groups. Note that absence of the "riverbed-hg-pkt-filter" entry in the TACACS+ configuration file implies no restrictions on host group based access control.

SAML IDP Information

The SAML IDP needs to provide two pieces of information to AppResponse 11 during the login process: a username and one or more roles associated with that user.

Field	Default SAML Attribute	Description
Username	NameID	The username string to be entered in the AR11 login screen. If this string is not specified, it will default to the Email address of the user, and this will be seen by AR11 as a new user.
Roles	memberOf	Comma-separated, case-sensitive string of roles defined in AR11.

If the Username attribute is missing, the SAML assertion is considered invalid and the login attempt will be denied. If the roles attribute is missing, the user will be granted no roles, but still allowed to log in.

AppResponse 11 has one default user, admin, with the predefined role of System Administrator.

SAML 2.0 Authentication

SAML 2.0 authentication is supported to facilitate single sign-on for use with one or more AppResponse 11 systems or other SteelCentral products accessed from a single browser session. When SAML 2.0 is enabled, AppResponse 11 relies on a specified SAML identity provider (IDP) for authentication, and does not use local authentication or RADIUS or TACACS+ servers in any combination. (Note that enabling SAML 2.0 authentication on AppResponse 11 *disables* all other forms of authentication used by the web UI.) If the SAML identity provider is unable to authenticate a user for any reason, that user will not be able to launch an AppResponse 11 web UI session. Note that SAML 2.0 authentication can be disabled via the AppResponse 11 CLI, using the `no saml enable` command.

When SAML 2.0 is enabled, the first time a user initiates access to an AppResponse 11 system in a browser session, AppResponse 11 will redirect the user to the SAML IDP for authentication. Upon successful authentication, the IDP will redirect the user back to the AppResponse 11 system, and the UI will open. The IDP will send back the user role corresponding to the user name being authenticated, and that user will have permissions in AppResponse 11 as defined by that role. As long as the user keeps that browser session active, any subsequent AppResponse 11 session, even if the user logs out of the system, quits the browser tab, or accesses a new system, will begin immediately without requiring the user re-authenticate. The user will need to re-authenticate with the IDP if they quit the browser session in which they had authenticated earlier.

Configuring SAML 2.0 Authentication

Note: It is strongly recommended that you select Enable SAML 2.0 *only* after running Test successfully. [See the end of this procedure for more information about running Test.] Enabling SAML 2.0 will disable all other authentication types: local, RADIUS, and TACACS+.

1. Go to Administration > Account Management: Authentication to display the Authentication page.
2. Select the SAML 2.0 tab.
3. (Optional) The NameID field specifies what AppResponse 11 uses as the authenticated user's name. If this field is left blank (the default), AppResponse 11 will use the SAML NameID field. If this field

is populated, AppResponse 11 will look for a SAML attribute of the same name, and use it as the username. In either case, if a user name is not found, the user will not be allowed to log in.

4. In the IDP Metadata field, paste in the XML metadata that identifies the identity provider you wish to use. This step is manual, and you need to acquire the XML metadata from your IDP separately.
5. Leave the Roles Attribute field set to “memberOf”, unless your IDP has been configured to use a different attribute.
6. (Optional) If you need to acquire XML metadata that identifies your AppResponse 11 system (the service provider), click the Download as XML link to obtain it.
7. (Optional) Select whether you will return signed authentication requests or require signed assertions when interfacing to the identity provider.
8. (Optional) Specify a fully qualified domain name, if you wish to use one. This is needed only if AppResponse 11 is unable to determine this on its own, or if it otherwise obtains a host address that is not the same as what is required from a web browser.
9. (Optional) Import or generate a certificate that will verify the identity of your AppResponse 11 system (the service provider), if you wish.
10. Click Apply to implement your changes, then click Test to see what will happen without committing to the configuration changes. If the results of the test are satisfactory, click Enable SAML 2.0 and click Apply again. Click Revert to return to the last saved configuration.

Note: It is strongly recommended that you select Enable SAML 2.0 *only* after running Test successfully. Enabling SAML 2.0 will disable all other authentication types: local, RADIUS, and TACACS+.

Virtual Interface Groups (VIFGs)

A *virtual interface group* (VIFG) is a logical collection of one or more monitoring interfaces or VLANs that AppResponse 11 treats as a single interface and uses as a source for traffic analysis or packet capture. Prior to Version 11.5.0, these groups were known as monitoring interface groups (MIfGs), and included monitoring interfaces only, not VLANs. VIFGs, like MIfGs in earlier versions, can be configured with additional properties such as packet deduplication and traffic filters (BPF or SteelFilter). Refer to [“SteelFilter Identifiers Supported For NPM Capture”](#) for the set of SteelFilter identifiers that are supported for use with VIFGs.

VIFGs are configured and managed using the Virtual Interface Groups tab on the Capture Jobs/Interfaces page.

Important: Capture jobs are configured using VIFGs as traffic sources, not monitoring interfaces.

Virtual Interface Groups Tab

Clicking Administration > General Traffic Settings: Capture Jobs/Interfaces and selecting the Virtual Interface Groups tab provides access to these controls:

- **Group by** – This specifies the mode that AppResponse 11 uses to process traffic, either by groups of monitoring interfaces or by groups of VLANs. These modes are mutually exclusive; monitoring interfaces and VLANs cannot be mixed in the same group, and changing the mode from one to the other will delete all existing groups associated with the first mode.
 - **Monitoring Interfaces** – Group by monitoring interface name. This corresponds to the monitoring interface groups (MIfGs) supported prior to Version 11.5.0, and MIfGs created before Version 11.5.0 will be preserved in the process of upgrading to Version 11.5.0.
 - **VLAN Tags** – Group by VLAN tag. Optionally, VLANs can be discovered automatically to create VLAN-based VIFGs; select the Enable Autodiscovery checkbox to do this.
- **Enable Virtual Interface Group Aggregation** – This controls the collection and display of application stream analysis (ASA) metric data for VIFGs, accessible via the Navigator. This feature must be enabled in order to see data in VIFG Insights and VIFG Navigator views.
- **Enable Autodiscovery** – Autodiscovery is disabled by default. If you enable this option, any VLANs visible to the AppResponse 11 system will be added to the list of VIFGs as VLAN-based VIFGs. When autodiscovery is on, every time a new VLAN tag is seen in the network, a new VIFG will be created for it automatically, using default values.

Autodiscovery Defaults:

Enable Deduplication – Packet deduplication is VIFG-aware and can be enabled/disabled on a per VIFG basis.

Filter: BPF | Steelfilter – Select an option and type the filter definition, if you want to use one to process traffic more selectively.

[Link to Flow Export configuration](#)

Apply | Revert buttons – Click one to execute the latest VIFG changes, or to return to the last saved VIFG configuration.

Add – Click Add to display the New Virtual Interface Group dialog and define an individual VIFG manually.

The VIFG table displays the following properties for each known VIFG:

- Name
- Description
- Enabled [toggle]
- VLAN IDs
- Filter
- Deduplication
- Capture Job
- Received Bytes
- Received Packets
- Duplicated Packets

The Default VIFG: other_vifg

A group named “other_vifg” is present by default and always displayed on the Virtual Interface Groups tab. The other_vifg group can be disabled/enabled, but cannot be removed or created. A packet will be associated with other_vifg if other_vifg is enabled and the packet doesn’t belong to any other existing VIFG. This is true for both monitoring interface mode and VLAN mode.

Note the following details pertaining to VLAN mode:

- The other_vifg group is not used when autodiscovery is enabled (regardless of its “enabled” status). It will be used only if 2,000 VIFGs have been discovered already (and more keep being discovered) and if other_vifg is enabled.
- If autodiscovery is enabled, other_vifg cannot be manually disabled or enabled. (This is true for all VIFGs when autodiscovery is enabled.)
- If a packet matches a VIFG that is disabled, it will not be accounted for in that VIFG, and it will not go into other_vifg.
- If a packet matches a VIFG that is enabled, but does not match the VIFG’s filter, the packet will not be accounted for in that VIFG, and it will not go into other_vifg.
- If a packet has been determined to be duplicate traffic, the packet will be accounted for that VIFG in the received bytes/packets and duplicated packets count.

VIFG Modes

Two modes of VIFG operation control the way in which AppResponse 11 recognizes and manages network interfaces for the purposes of capturing and monitoring traffic. Traffic is grouped by monitoring interfaces (the default) or by VLAN ID. The VIFG mode that is set in AppResponse 11 controls which VIFGs are visible in Packet Analyzer Plus.

Note: The two modes of operation are exclusive; it is not possible to create one VIFG that captures from a monitoring interface and a VLAN tag.

Note: Changing the VIFG mode causes all groups created in the other mode to be deleted. Existing capture jobs will be kept, and will remain linked to the deleted VIFG.

Monitoring Interfaces Mode

Monitoring Interfaces mode is the default mode for AppResponse 11. In this mode, VIFGs are defined by explicitly specifying individual monitoring interfaces to include in the VIFG. This corresponds to the monitoring interface groups (MIfGs) supported prior to Version 11.5.0, and MIfGs created before Version 11.5.0 will be preserved in the process of upgrading to Version 11.5.0 and later.

Observe these considerations when planning and configuring VIFGs:

- A VIFG has one or more monitoring interfaces.
- A monitoring interface can be a member of *only one* VIFG.
- The maximum number of VIFGs is the same as the number of monitoring interfaces installed. When running on VMware ESXi 5.5 or 6.0, the maximum number of monitoring interfaces is 8.
- A VIFG must have a unique name. If a VIFG is deleted, that name can then be used by another VIFG.
- Any changes to a VIFG take effect immediately.

VLAN Mode

Selecting the Group By: VLAN IDs option enables you to define VIFGs based on the VLAN tags that are read from incoming packets. As with groups based on monitoring interfaces, you can create new VLAN-based groups manually using the web UI. For example, you could create a new VIFG that includes VLAN 10, VLAN 100, and VLAN 150. Two different VLAN-based groups cannot have VLAN tags in common, so, for example, you cannot create a VIFG including VLAN 10 and VLAN 100, and another VIFG including VLAN 20 and VLAN 100. A VIFG in VLAN mode can aggregate up to 32 VLANs.

You can use wildcards ("*") when specifying VLANs, including when specifying inner or outer VLAN IDs. For example, typing VLAN "45:*" would match the VLAN "45:48:3" as well as the VLAN "45:2". Be conscious of the interaction of the wildcard character with Q-in-Q delimiters: For example, "3:*:5" will match "3:12:5", but not "3:1:2:5". In addition, overlap between definitions is not allowed: For example, "4:*" and "*:3" both match "4:3", so the second such definition would be rejected.

Note: The Packet Analyzer Plus Windows client does not support VLAN mode.

For each VLAN-based VIFG, you can specify a default filter, enable/disable deduplication, and/or export the VIFG to SteelCentral NetProfiler (with a custom filter).

As of Version 11.10.0, VLAN UNTAGGED is used for untagged packets instead of VLAN 0. Autodetect will assign VLAN 0 packets to a group named "vifg_0", and will assign untagged packets to a group named "vifg_untagged". When upgrading to Version 11.10.0 and later, groups that used VLAN 0 will be converted to VLAN UNTAGGED. (When defined manually, the "UNTAGGED" label must be typed in all capital letters.)

“Q-in-Q” tunneling is supported, but VLAN inside VLAN is considered separate from a single VLAN. That is, VLAN 10 and VLAN 10 inside VLAN 11 will be considered two different non-overlapping groups. Comma-separated values are treated as distinct VLANs; Q-in-Q would be denoted with a semicolon, such as, “3102:300”.

VLAN Autodiscovery

In addition to the default behavior that enables you to define VLAN-based VIFGs manually, VLAN mode supports VLAN-based VIFG creation by autodiscovery. Autodiscovery is useful when you don't know in advance what VLAN IDs are configured in the network you're working with. The VIFG will be created with a default name ("VIFG %d" or "VIFG%d:%d" for Q-in-Q tunneling), and there will be a new VIFG for each VLAN tag; Q-in-Q VLANs count as separate groups.

Note: Autodiscovery is available only when working in VLAN mode.

Be aware of these aspects of VLAN autodiscovery behavior:

- When autodiscovery is off, new VIFGs can only be created manually using the Web UI (or through REST).
- When autodiscovery is on, it is not possible to create new VIFGs or edit existing ones manually.
- When autodiscovery is on, each time a new VLAN tag is seen in the network, a new VIFG is created automatically.
- If the number of VIFGs doesn't exceed the maximum, then the other_vifg group will not be used, regardless of whether it's enabled or not. If the number of VIFGs exceeds 2,000, the other_vifg group will be used if it's enabled.
- As of Version 11.10.0, VLAN 0 packets are assigned to a group named "vifg_0", and untagged packets are assigned to a group named "vifg_untagged". When upgrading to Version 11.10.0 and later, VIFGs with 0s are converted to untagged.
- Autodiscovery will not modify existing groups, nor will it create overlapping groups.
- The deduplication and filter of pre-existing groups will not be modified when autodiscovery is on. If a VIFG was already configured manually on specific VLANs (for example, VLAN10), and a packet with VLAN10 is received, it will be added to the existing VIFG, and no new group will be created.
- When autodiscovery is on, although it is not possible to edit the membership of existing groups manually, it is possible to change the autodiscovery settings (for example, using a filter).

You may find this workflow helpful for using autodiscovery:

1. Enable autodiscovery.
2. Wait for VLAN-based VIFGs to appear automatically.
3. Disable autodiscovery.

4. Edit groups manually (for example, join two VLAN IDs in the same VIFG).

VIFG Usage Considerations

Considerations that apply to both VIFG modes:

- A maximum of 2,000 VIFGs can be configured or discovered automatically.
- The ID of the VIFG will not change if its members change.
- One capture job can be associated with multiple VIFGs.
- Capture jobs provide the option to include all configured groups.
- If a subset of the VIFGs associated with a capture job are removed, the capture job will continue capturing traffic from the remaining VIFGs.
- A capture job is not removed if all of its associated VIFGs are removed. The capture job can be modified to include different VIFGs.
- Every VIFG (in either mode of operation) will return these new settings:
 - MTU: This will be the maximum of the MTUs of the interfaces the VIFG collects (in monitoring interface mode) or the maximum of all interfaces' MTUs (in VLAN mode).
 - Bandwidth Capacity: This will be the sum of the link speeds of the interfaces the VIFG collects (in monitoring interface mode) or the maximum of all interfaces' link speeds (in VLAN mode).
- While the MTU is a read-only value, the Bandwidth Capacity can be configured through REST (and in the Web UI).

Creating or Editing a VIFG

Note: A VIFG cannot be edited if a capture job is running on that VIFG.

1. Choose Administration > General Traffic Settings: Capture Jobs/Interfaces, and click the Virtual Interface Groups tab.
2. Add or Edit?
 - Click **Add** to create a new VIFG.
 - To edit, hover the cursor over an existing VIFG and click the pencil icon on the right to display the Edit Virtual Interface Group dialog.
3. Specify or select the following fields:
 - Name
 - Description
 - Enabled
 - Enable Deduplication - Packet deduplication is done on a per VIFG basis - packets are only identified as duplicates of other packets in the same VIFG.
 - Interfaces - For monitoring interface mode, select a monitoring interface from the drop-down list. Click **x** next to an existing interface name to remove it from the VIFG.

- VLAN IDs - For VLAN mode, type one or more VLAN IDs in this field. You can use wildcards ("*") when specifying VLANs, including when specifying inner or outer VLAN IDs. For example, typing VLAN "45:*" would match the VLAN "45:48:3" as well as the VLAN "45:2". Be conscious of the interaction of the wildcard character with Q-in-Q delimiters: For example, "3:*:5" will match "3:12:5", but not "3:1:2:5". In addition, overlap between definitions is not allowed: For example, "4:*" and "*:3" both match "4:3", so the second such definition would be rejected.
- Filter- Enter a BPF (default) or SteelFilter filter for VIFG traffic. Traffic dropped by a filter is not analyzed or stored in packet storage.
- Bandwidth Capacity

Deleting a Virtual Interface Group

A VIFG cannot be deleted if it is configured in a running capture job. To delete a VIFG, hover over an existing VIFG with your mouse and click the **x** on the right.

Managing Virtual Interface Group Members

You can change the membership of monitoring interfaces in a group as follows.

1. Choose Administration > General Traffic Settings: Capture Jobs/Interfaces, and click the Virtual Interface Groups tab.
2. Hover with your mouse over a monitoring interface and click the pencil icon on the right.
3. In the Monitoring Interface Group field, click the expansion icon to open a drop-down list of choices.
4. To change membership to a different VIFG, click the target VIFG name from the list.
To remove from a VIFG, click **Unassigned**.
5. Click **Save** to complete your change.

Select Monitoring Interface Groups to view your changes. Unassigned monitoring interfaces are listed at the bottom of the table.

Importing and Exporting VIFG Definitions

VIFG definitions can be exported from and imported to AppResponse 11 via CSV file. The VIFG table in the Virtual Interface Groups tab of the Capture Jobs/Interface page provides buttons for executing the import and export actions.

For exporting VIFGs:

- Click the Export button to create a CSV file listing the existing VIFGs.
- If the Group By setting is Monitoring Interfaces, the VIFG Name, Description, Enabled, Interface, is other vifg, Bandwidth, and Deduplication information are exported to the CSV.
- If the Group By setting is VLAN IDs, the VIFG name, Description, Enabled, VLAN IDs, is other vifg, Bandwidth, and Deduplication information are exported to the CSV.

For importing VIFGs:

- Click the Import button to choose a CSV file for importing the VIFGs.
- If the Group By setting is Monitoring Interfaces, the validation rules for interface will be enforced. The interface has to be a valid interface and not be used in another VIFG already.
- If the Group By setting is VLAN IDs, the validation rules for VLAN ID will be enforced. The VLAN ID has to be a number between 0 and 4095 or in X:Y format, in which X and Y must be a number between 0 and 4095. In addition, the VLAN ID cannot be used by another VIFGs already.
- The import process will add only new VIFGs, or update/override existing VIFGs. It does not delete existing VIFGs.

Flow Export

AppResponse 11 can export in parallel:

- NetFlow v9 records over SSL/MNMP to NetProfiler 10.9.5 (or later).
 - A maximum of two (2) NetProfiler/Flow Gateway appliances are supported.
- Standard NetFlow v9 records using standard UDP packets to NetFlow Collectors.
 - A maximum of two (2) NetFlow Collectors are supported.

AppResponse 11 must see both directions of traffic flow on the same Virtual Interface Group (VIFG) to calculate and export the following metrics to a NetProfiler/Flow Gateway appliance:

- DPI metrics for applications
- VoIP metrics for IP telephony
- Service Response Time metrics for TCP connections

Otherwise, only basic flow metrics are calculated and exported.

You can specify one filter (BPF or SteelFilter) per VIFG. Refer to [“SteelFilter Identifiers Supported For NPM Capture”](#) for the set of SteelFilter identifiers that are supported for use with VIFGs.

You can view the configured NetProfiler Export and Flow Collector settings and their export statistics by selecting the Status tab on this page.

This section covers the following:

- [“Configuring Flow Export” on page 50](#)
- [“Checking Flow Export Status” on page 51](#)

Configuring Flow Export

Flow export must be enabled before you can export to AppResponse 11 or a flow collector.

To export flows to NetProfiler/Flow Gateway

1. Go to Administration > Integration > Net Profiler Integration in the web UI, and click the Flow Export Settings tab.
2. Select Enable Flow Export. This enables export to NetProfiler/Flow Gateway and NetFlow collectors.
3. Select VOIP Quality metrics to export VOIP quality metrics (no Telchemy metrics).
4. Enter the hostname or IP address of each NetProfiler/Flow Gateway to receive the flow exports.
 - NetProfiler does not support NetFlows from IPv6 exporters.
5. To manage port name and custom application definitions from a NetProfiler to ensure consistent traffic identification, select Manage Port Names and Custom Applications from NetProfiler and select the NetProfiler to use. The definitions on this NetProfiler replace the definitions on an

AppResponse 11 exporting traffic. Port Aliases and Application Configuration are disabled in AppResponse 11.

6. Click **Apply** to begin flow export.

To export flows to NetFlow Collectors

1. Go to Administration > Integration > Net Profiler Integration in the web UI,, and click the Flow Export Settings tab.
2. Select Enable Flow Export. This enables flow export to NetFlow v9 flow collectors.
3. Enter the hostname or IP address of the NetFlow collectors to receive the flow exports.
4. Enter the UDP port to use for flow export.
5. Click **Apply** to begin flow export.

Checking Flow Export Status

The Flow Export Status tab on the Net Profiler Integration web UI page contains status information on flow recipients as well as traffic volumes in the past minute and the previous week for NetProfiler/ Flow Gateway and Flow Collector exports.

Capture Jobs

Capture jobs define and manage network traffic packet capture on VIFGs. A maximum of 32 capture jobs can be configured. A capture job specifies:

- if a filter is used.
- if an index is built.
- the maximum amount of storage used by retained captured packets and index data.
- the maximum timespan that captured packets and an index are retained.

Note: Exporting packets or Launching SteelCentral Packet Analyzer Plus from a right-click menu are only possible when packets are captured and retained by a capture job.

This section includes the following topics:

[“Adding a New Capture Job” on page 52](#)

[“Downloading Packets From a Capture Job” on page 55](#)

[“Analyzing Traffic with Packet Analyzer Plus” on page 56](#)

[“Analyzing Traffic with Transaction Analyzer” on page 56](#)

[“Restricting User Access to Packets” on page 57](#)

From the Capture Job menu bar you can choose to:

- Add a new capture job
- Delete selected jobs
- Start or stop selected jobs
- Export packets from a selected job
- Clear the packets captured in a stopped job

Hover with the mouse over a capture job to:

- Select—by clicking the check box
- Edit—by clicking the pencil icon
 - A stopped job’s configuration can be changed.
 - A running job’s configuration can be viewed.
- Delete—by clicking the x icon on the right.

Note: All stopped jobs will lock their storage automatically. If space is required to start a new job, then a stopped job will need to be deleted.

Adding a New Capture Job

To create a new capture job:

1. Go to the Administration > General Traffic Settings: Capture Jobs/Interfaces page, and click the Capture Jobs tab.

2. Choose the Add button to open the New Capture Jobs Definition dialog.
3. Enter a name for the capture job (required). The name must be unique. A maximum of 128 Unicode characters can be used (required).
4. Select a VIFG with the traffic to be captured (required). By default, All VIFGs are selected. Uncheck All to manually select one or more VIFGs from the list.
5. Specify a filter (optional). SteelFilter is the default filter type and the recommended filter type; see [“SteelFilter Identifiers Supported For NPM Capture”](#) for the list of SteelFilter identifiers supported for capture jobs. No filter is used if the text box is empty.

Any BPF filter can be used without complication when indexing is not checked. If BPF and indexing are both selected, a message is displayed about potential issues that could occur. BPF filters using IP addresses, ports, or IP protocols will work as expected. However, BPF filters that create a subset of a flow could result in an incorrect microflow index and an incorrect view in Packet Analyzer Plus. If you have a capture job with a microflow index and a BPF filter, the packets stored on disk and the associated microflow index might not be identical, because the index might not reflect the actual packets stored on disk. This can happen because the index stores data per flow or per connection, while a BPF filter can filter out any packet within a given flow or connection. One possible example of this: Consider a filter that causes only packets with even sequence numbers to be stored to disk. The microflow index would include all the packets in the flow, but only half of those packets would be stored. A workaround, if packets are available, is to force Packet Analyzer Plus to create the view from the packets, not from the microflow index, by holding down the Shift key when you apply a view.

6. Enter a maximum packet size (snaplen) for capture (optional). Values from 1 to 65535 bytes are valid. The default, 65535 bytes, captures the entire packet.
7. Packet data retention is set based on the size of the storage used by the captured packets and the timespan that the captured packets are kept. Time retention rules are calculated from the current time. For running capture jobs the following rules apply:
 - Minimum specifications are targets and may not be met for some or all jobs. Storage space is shared equally among jobs whose target has not been met, yet.
 - If a maximum retention size is set, a job cannot store more data than the specified limit.
 - If a maximum retention time is set, a job cannot contain a longer timespan than the specified limit.
 - If the total size of all capture jobs reaches the size of the packet storage, data is pruned using the minimum parameters to set priority. Jobs that have not reached their minimum parameters have a low pruning priority; jobs that have reached their minimum parameters have a high pruning priority. Pruning reduces the size and time of each job.

Option	Notes
Min Retention Size	Specify a target minimum amount of packet storage for captured packets. Enter the number of bytes and select a unit of measure from the drop-down list.
Max Retention Size	Specify the maximum amount of packet storage for captured packets. Enter the number of bytes and select a unit of measure from the drop-down list.
Min Retention Time	Specify the minimum timespan to retain captured packets. Enter a number and select a unit of time from the drop-down list.
Max Retention Time	Specify the maximum timespan to retain captured packets. Enter a number and select a unit of time from the drop-down list.

8. Enable Indexing (optional). If the box is checked (default), a microflow index is created for the capture job. Packet Analyzer Plus uses the microflow index by default to speed the presentation of views.
9. Microflow Index retention is set based on the size of the index and the timespan that the index is kept. Time retention rules are calculated from the time of the last entry stored, not the current time. For running capture jobs the following rules apply:
 - Minimum specifications are targets and may not be met for some or all jobs. Storage space is shared equally among jobs whose target has not yet been met.
 - The minimum retention size is 50 MB for a Microflow Index.
 - If a maximum retention size is set, an index cannot store more data than the specified limit.
 - If a maximum retention time is set, an index cannot contain a longer timespan than the specified limit.
 - If the total size of all capture job indexes reaches the size of the index storage, data is pruned using the minimum parameters to set priority. Jobs that have not reached their minimum parameters have a low pruning priority; jobs that have reached their minimum parameters have a high pruning priority. Pruning reduces the size and time of each job.

Option	Notes
Min Retention Size	Specify a target minimum amount of microflow index data to store. Enter the number of bytes and select a unit of measure from the drop-down list.
Max Retention Size	Specify the maximum amount of microflow index data to store. Once this size is reached the oldest data is overwritten as new data is received. Enter the number of bytes and select a unit of measure from the drop-down list.
Min Retention Time	Specify the minimum timespan for an index to be stored. Enter a number and select a unit of time from the drop-down list.
Max Retention Time	Specify the maximum timespan for an index to be stored. Enter a number and select a unit of time from the drop-down list.

10. Click Save to save your settings.

SteelFilter Identifiers Supported For NPM Capture

The following SteelFilter identifiers are supported for use with capture jobs, as well as with VIFGs and with exporting to NetProfiler:

- ip.src—Source IP address
- ip.dst—Destination IP address
- ip.addr—Any IP address
- ip.proto—Any protocol in use
- tcp.port—Any TCP port
- tcp.src_port—Source TCP port
- tcp.dst_port—Destination TCP port
- udp.port—Any UDP port
- udp.src_port—Source UDP port
- udp.dst_port—Destination UDP port
- transport.port—Any transport port
- transport.src_port—Source transport port
- transport.dst_port—Destination transport port

Refer to the SteelCentral Packet Analyzer Plus User's Guide, Appendix A: SteelFilter Identifiers for a complete list of SteelFilter identifiers.

Downloading Packets From a Capture Job

After packets have been captured, you can save them to a trace file to examine them. Note that for Host Groups, IP addresses, and VIFGs associated with an alert, right-clicking in the Alert Event Details Insight gives you the option of accessing captured packets, using the Download Packets command (for IP addresses and VIFGs) and Packet Download Preview command (for Host Groups).

Note: If volume initialization is in process, you may observe a drop in packet download speeds of up to 50%. This can occur when a RAID 5/6 initialization has been initiated on the system and a packet download is executed before the initialization is complete.

To save captured packets as a trace file:

Note: In order to be to download a packet trace, you need to have at least Read-Only access to Network packets.

1. Go to the Administration > General Traffic Settings: Capture Jobs/Interfaces page, and click the Capture Jobs tab.
2. Click Download Packets to open the Download Packets dialog. The Packet Download Statistics section of the dialog is not populated until the approximate size of the capture job download has been estimated. This estimate will give you some idea of how long the download process could take.
3. Specify an export time interval. You can change this time range at any time without needing to click Restart Download; the packet download estimate will update automatically. The updated time range will be taken into consideration when you execute the download.

4. Select the file format and time stamp resolution desired.
5. Select the number of bytes in each packet to be exported.
6. Specify a BPF definition if you want to download only a specific subset of the data in the capture job. The BPF is not validated automatically, and is not taken into account in the estimated size of the download. Any issues caused by an invalid BPF will be cited after the download has executed completely.
7. Click Download Packets to send the packets to a trace file on your local system. The export object is available for a limited amount of time only (three minutes), so the download should be executed promptly after the export process is complete. If the packets are not downloaded promptly and the export object times out, it will be necessary to re-execute the export process.

Packet Download Preview Insight

For Host Groups, IP addresses, and VIFGs associated with an alert, right-clicking in the Alert Event Details Insight gives you the option of accessing captured packets, using the Download Packets command (for IP addresses) and Packet Download Preview command (for Host Groups and VIFGs).

The Packet Download Preview Insight furnishes:

- Summary table—Various high level traffic metrics.
- Packet Download Interval Selection time series chart
- IPs tab—Top IPs table.
- IP Conversations tab—Top IP Conversations table.
- VIFGs tab—Top Virtual Interface Groups table.

Analyzing Traffic with Packet Analyzer Plus

Packet Analyzer Plus contains an extensive collection of network traffic analysis metrics (views) and is closely integrated with AppResponse 11. Packet Analyzer Plus provides:

- analysis of packets sent from AppResponse 11.
- access to an AppResponse 11 Web interface for managing capture jobs.
- drag-and-drop drill down (successive application of views).
- visualization and analysis of:
 - long-duration packet captures.
 - multi-source packet captures.
- report generation.

Analyzing Traffic with Transaction Analyzer

Certain objects in the AppResponse 11 web UI can be selected for export to Transaction Analyzer, to be examined there. The exportable objects are:

- host
- host pair
- host group
- host group pair
- TCP connection
- page object
- web host
- web host group

Select an object in the web UI and right-click on it to send the associated traffic (downloaded as a capture file) to Transaction Analyzer. Choose Launch SteelCentral Transaction Analyzer from the context menu, and choose one of the following destinations within Transaction Analyzer:

- Trace Explorer
- Tree View
- App Doctor

The Transaction Analyzer launcher invokes an installed instance of Transaction Analyzer. A series of dialogs will appear, showing the progress of Transaction Analyzer launching, including authentication.

In order for Transaction Analyzer to work with AppResponse 11 in this way, you need to have AppTransaction Xpert Version 17.0.T-PL1 installed and licensed, and also SteelCentral Transaction Analyzer Launcher Setup Version 11.2.0 or later installed. Invoking the launcher application in Windows after it is installed prompts you for permission to run the extension *.rtal; this is the file extension of the script that AppResponse 11 generates for sending packet data to Transaction Analyzer.

Restricting User Access to Packets

In general, user access to packet data (downloading and exporting) is controlled through the Network Packets permission setting for the user's role (see ["Roles and Permissions"](#)). The Network Packets permission controls access to any available packets. However, user access can be controlled more tightly through the use of a TACACS+ VSA named "riverbed-hg-pkt-filter", which enables you to restrict packet access for specific users to only those packets originating from IP addresses in specific host groups.

Note: This host group based restriction to packets is supported only via TACACS+.

To do this, the configuration file for the TACACS+ server ("tac_plus.conf") must contain an entry "riverbed-hg-pkt-filter" = "hostgroup1,hostgroup2,hostgroupn", per user, where each "hostgroup" is a host group name that specifies the IP addresses for which the user has permission to download/export packets. Absence of the "riverbed-hg-pkt-filter" entry implies no restrictions on host group based access control, and, similarly, a "riverbed-hg-pkt-filter" entry with an empty list of host groups means there are no restrictions on packet access.

Note: Remember that TACACS+ VSAs are limited to 255 characters in length.

Packet Format

These parameters provide instruction for how packet dissection is performed in AppResponse 11, modifying the way in which information is collected from the packets, without altering the packets themselves. For example, these parameters can be used to determine whether the inner or the outer TCP/IP headers will be used with GRE encapsulation.

Supported Parameters

- **L3 GRE** — The Analyze inner IP only option is selected by default, causing packet analysis to be performed on the inner packet. Selecting Analyze outer IP only disables this feature, causing packet analysis to happen only on the outer packet.
- **VxLAN** — The Analyze VxLAN header option is selected by default, causing the outer packet to be analyzed. If the Ignore VxLAN option is selected, instead, then only the inner packet will be analyzed. That means that VxLAN views will show no data, since the inner packet likely does not use VxLAN.
- **MAC in MAC** — The Recognize 802.1ah option is selected by default, causing the 802.1ah frame to be recognized, and the rest of the frame will be parsed. If, for example, an IP header follows, the packet will be identified correctly as an IP frame. If the Ignore (entire) 802.1ah packets option is selected, packet dissection will stop at the 802.1ah header; the IP packet of the previous example will not be recognized as IP.
- **CAPWAP** — Control and Provisioning of Wireless Access Points (CAPWAP) enables the management and deployment of 802.11 (WiFi/WLAN) networks. The Ignore CAPWAP option is selected by default, meaning that, when CAPWAP traffic is encountered, packet analysis is performed on the outermost header only, ignoring the fact that CAPWAP is in use. You can select Recognize CAPWAP to cause packets to be analyzed according to the first header encapsulated within the CAPWAP wrapper.
- **UDP Port for VxLAN** — This is set to 4789, by default.
- **UDP Ports for CAPWAP** — Specify ports to monitor for the presence of CAPWAP traffic. Port 5247 is specified by default.
- **MPLS Level** — By default, the bottom MPLS Label (1) is set. This is the position from the bottom of the MPLS label stack, to be used. Values range from 1 to 10; values start from 1 (bottom of the stack) and increase.
- **VLAN Level** — By default, VLAN Level 1 is set. Values range from 1 - 255; values start from 1 and increase.

Configuring Packet Dissection

1. Go to Administration > General Traffic Settings: Packet Format.
2. Enable or disable L3 GRE, VxLAN, MAC in MAC, or CAPWAP by clicking the radio button that specifies the behavior you want to have configured.
3. If VxLAN is enabled, specify the UDP port used by VxLAN. The default UDP port is 4789.
4. If CAPWAP is enabled, specify any additional UDP ports on which to monitor for CAPWAP traffic. UDP port 5247 is specified by default.

5. Specify the MPLS level.
6. Specify the VLAN level.
7. Click **Apply** to make or **Revert** to reset the changes made.

Web Server Settings

An SSL Certificate, ciphers, and protocols can be configured to protect access to the AppResponse 11 web UI. A self-signed certificate is generated automatically when a system boots if no certificate is installed. You also can provide a certificate of your own, signed by a Certificate Authority of your choice. You must log in with read/write system configuration permissions to make changes to this page.

Important: Intermediate or chained certificates are not supported.

You manage SSL certificates at Administration > System Settings: General, in the Web Server Settings tab. Here you can:

- view, retrieve, or replace the installed certificate.
- change the port used for HTTPS.
- choose the ciphers and protocols used.

You also manage the use of HTTP to access the web UI:

- enable or disable (default) HTTP access
- if enabled, configure HTTP access.

This section covers:

- [“Secure Vault For Encrypted Security Files” on page 60](#)
- [“Configuring HTTPS Settings” on page 61](#)
- [“Configuring HTTP Access” on page 61](#)
- [“Viewing the SSL Certificate” on page 62](#)
- [“Replacing the SSL Certificate” on page 62](#)
- [“FIPS Mode” on page 63](#)

Secure Vault For Encrypted Security Files

AppResponse 11 keeps sensitive security objects such as certificates and decryption keys in an encrypted filesystem, or “secure vault,” that allows AppResponse 11 to access them while preventing tampering or access by any other means. The secure vault is not user-accessible, and cannot be used for protecting other files. In the event that AppResponse 11 is unable to unlock the secure vault and access its contents, the web UI will prevent access to the system via the web UI.

Two CLI commands are available for administering the secure vault:

- `show secure_vault status` — This admin CLI command will return one of three possible statuses:
 - `locked` — AppResponse 11 cannot access the secure vault and its contents. The web UI cannot be used in this state.
 - `active` — AppResponse 11 is able to access the secure vault and its contents.

- resetting — The secure vault is in the process of returning to its original, default state. This state will persist until the system has rebooted successfully.
- secure_vault reset — This command is available only in configure terminal mode. Executing it will prompt for confirmation before returning the secure vault to its default state, with all HTTPS settings (including ports), certificates, and decryption keys removed or returned to their default states. A reboot is required to complete a reset of the secure vault.

Configuring HTTPS Settings

To configure the HTTPS port

1. Go to Administration > System Settings: General, then select the Web Server Settings tab.
2. Under Settings, specify the HTTPS TCP port to be used. The following ports are accepted:
 - 443
 - 8443
 - 24000 - 24999

Valid entries have a green shadow; invalid entries have a red shadow with hover text showing valid entries.

3. Specify OpenSSL ciphers. All entries are passed to OpenSSL for validation.
 - The default ciphers enable:
 - Ciphers with key lengths larger than 128 bits.
 - Ciphers offering no authentication
 - KRB5
 - MD5
 - 3DES
4. Select Security Protocols to use by checking the box before any listed protocols.
5. Click **Apply** to save your changes, **Revert** to discard your changes.

Configuring HTTP Access

To configure HTTP access to the web UI

1. Go to Administration > System Settings: General, then select the Web Server Settings tab.
2. Select the desired HTTP Access mode from the drop-down list of choices:
 - Disabled—No HTTP access to the web UI.
 - Enabled—Provides HTTP access using the specified TCP port. Valid ports are: 80 or 24000 - 24999.
 - Redirect to HTTPS—Sends traffic on the specified TCP port to the specified HTTPS port.

3. Click **Apply** to save your changes, **Revert** to discard your changes.

Viewing the SSL Certificate

To view the SSL certificate

1. Go to Administration > System Settings: General, then select the Web Server Settings tab.
2. Under the Certificate heading the certificate details are displayed for the current certificate:
 - Issued to
 - Issued by
 - Validity
 - Fingerprint
 - Key
 - PEM—Click Show/Hide PEM to display or hide (default) the PEM.

Replacing the SSL Certificate

You can replace the current certificate with an existing certificate or generate a new, self-signed certificate.

To replace the SSL certificate

1. Go to Administration > System Settings: General, then select the Web Server Settings tab.
2. Under the Certificate heading, click Replace.
3. The Specify Certificate window opens. Select to add an existing certificate or to generate a new one.
4. To import an existing certificate, supply the following information:
 - In the Certificate text box—paste the PEM-formatted certificate and private key.
 - In the Passphrase text box—enter the passphrase used to create an encrypted private key.
Note: the passphrase is only used to decrypt the key, it is not stored.
 - Click **Save** to replace the existing certificate with the imported certificate or **Revert** to discard the information just entered.
5. To generate a new, self-signed certificate supply the following information:
 - Common name
 - Organization name
 - Organization unit name
 - Locality
 - State

- Country code
- Email
- Click **Save** to generate a new certificate that replaces the existing certificate or **Revert** to discard the information just entered.

Important: It is important to make sure that the hostname and domain name are properly configured before generating the new certificate, as the new certificate contains hostname.domainname as the Common Name record. The hostname and domain name are specified on the Administration > System Settings: Host Settings web UI page. See [“Hostname and DNS Servers” on page 89](#) for more information. The certificate details for each certificate show the Common Name record and other records encoded into the certificate.

FIPS Mode

This section describes the use of certified Federal Information Processing Standard (FIPS) cryptography on AppResponse 11 appliances.

AppResponse 11 supports the use of certified Federal Information Processing Standard (FIPS) cryptography. This feature uses a FIPS-140-3 compliant module (Riverbed cryptographic module 2.0), based on OpenSSL, for all cryptographic operations. FIPS affects any client that makes a secure connection to the appliance, including the web UI, Packet Analyzer Plus, NetProfiler, Portal, SSH, and raw REST calls over HTTPS. Precision Time Protocol (PTP) is not affected by this feature.

Setting FIPS to ON runs AppResponse 11 in FIPS mode, which means that, by default, only FIPS-approved ciphers and algorithms are used. Whenever non-approved algorithms (such as MD5) are used anyway, they use a non-FIPS-compliant implementation, and cannot be considered FIPS-compliant. Non-FIPS-compliant algorithms, when used, may not work as ordinarily expected.

Note: Enabling FIPS mode activates the use of FIPS on the system. However, individual features may require additional configuration in order to be properly FIPS-compliant; users are responsible for being familiar with what constitutes FIPS-compliance for each feature, and configuring it appropriately. Refer to comments in the “Feature Support” section that follows for more information. Be aware that AppResponse 11 will continue to operate even if one or more features have not been configured for FIPS-compliance; in such a case, the system will not provide any warning that a particular feature is not FIPS-compliant. Any exceptions to this behavior are noted in the “Feature Support” section.

Note: After FIPS is enabled, any SNMP traps configured to use MD5 authentication or AuthPriv security will not be delivered. Email notifications and SNMP traps configured to use other security levels still will be delivered.

Supported AppResponse Platforms

FIPS is supported on AppResponse hardware appliances and virtual systems. FIPS is not supported on AppResponse Cloud (AWS and Azure).

General Considerations When Using FIPS Mode

When FIPS mode is enabled, it affects many other AppResponse 11 behaviors. Be aware of the following considerations when using FIPS mode:

- Software updates cannot be performed when FIPS mode is on. AppResponse 11 can be updated after disabling FIPS mode.
- The message authentication codes that can be used for SSH in FIPS mode are listed in [“SSH” on page 66](#).
- When connecting to the web UI and Packet Analyzer Plus in FIPS mode, only TLS1.2 is supported (out of TLS1.0/1.1/1.2, SSL2.0/SSL3.0).
- In FIPS mode, NTP is not FIPS-compliant when MD5 encryption is in use.
- Wireshark dissection is not FIPS-compliant.

Traffic Handling

Non-FIPS traffic is decrypted in FIPS mode. The system is not trusting nor using the monitored traffic except for analysis purposes, and this allows a system in FIPS mode to detect and monitor non-FIPS traffic on the network.

Enabling FIPS Mode

To access the control for enabling and disabling FIPS, click Administration > System Settings: General, then select the Web Server Settings tab and look for the Enable FIPS checkbox. Click it to enable or disable FIPS. (Note that FIPS is disabled by default.) When you change the setting, the web UI will display a banner notifying you that a reboot is needed, and the status dot will turn yellow. The reboot alert is persistent until the reboot is executed. In the Web UI, if the appliance is running in FIPS mode, then 'FIPS Mode' is displayed in the header on the Web UI page. Nothing is displayed in the header if the appliance has FIPS disabled.

Note: Enabling FIPS mode activates the use of FIPS on the system. However, individual features may require additional configuration in order to be properly FIPS-compliant; users are responsible for being familiar with what constitutes FIPS-compliance for each feature, and configuring it appropriately. Refer to comments in the “Feature Support” section that follows for more information. Be aware that AppResponse 11 will continue to operate even if one or more features have not been configured for FIPS-compliance; in such a case, the system will not provide any warning that a particular feature is not FIPS-compliant. Any exceptions to this behavior are noted in the “Feature Support” section.

Feature Support

This section details FIPS compliance per feature.

Feature	Supported	Comments
Appliance Licensing	No	None
Backup/Restore	No	See “Backup/Restore”
Email Notifications	Yes	See “Email Notifications”

Feature	Supported	Comments
Encrypted Syslog Notifications	No	See “Encrypted Syslog Notifications”
Integration Links	No	See “Integration Links”
Local Account Passwords	Yes	See “Local Account Passwords”
NetProfiler Integration	Yes	See “NetProfiler Integration”
NTP	Yes	See “NTP”
RADIUS	No	See “RADIUS”
REST API Access	Yes	See “REST API Access”
Secure Vault	Yes	See “Secure Vault”
ServiceNow Notifications	No	None
SNMP	Yes	See “SNMP”
Software Update	No	See “.Software Update”
SSH	Yes	See “SSH”
Syslog Notifications	Yes	See “Syslog Notifications”
TACAC+	No	See “TACACS+”
Web UI	Yes	See “Web UI”

Backup/Restore

Backup/restore to a remote server is not FIPS-compliant. However, note that the server must be configured to allow FIPS-compliant *systems* to connect. Specifically, if the server only allows Diffie-Hellman key exchange algorithms, it must be configured to use approved primes (/etc/ssh/moduli on Red Hat-based systems), or the backup will fail. Either delete the primes file, or enable one or more ecdsa algorithms: ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521.

See the Red Hat Customer Portal article on SSH interoperability of RHEL8+ in FIPS mode (RedHat login required).

Email Notifications

No user interaction is necessary; ciphers and algorithms of the outgoing connection are changed to FIPS-compliant ones automatically. The Email server must be configured to support them.

Encrypted Syslog Notifications

Outgoing connection does not disable non-FIPS ciphers.

Integration Links

Communication with other applications that is enabled via the Integration Links page is not FIPS-compliant.

Local Account Passwords

Local passwords are FIPS-compliant, stored as a SHA512-based hash.

NetProfiler Integration

A FIPS-compliant MNMP certificate is used in FIPS mode.

NTP

NTP using either SHA authentication keys or no authentication keys is FIPS-compliant. NTP using MD5 keys is not FIPS-compliant.

RADIUS

The RADIUS protocol is not FIPS-compliant, as it uses a non-compliant hash algorithm.

REST API Access

REST calls use the same HTTPS settings as the web UI, so the web UI must be configured properly, also.

Secure Vault

Secure Vault is FIPS-compliant; no configuration is necessary.

SNMP

When FIPS mode is enabled on the AppResponse 11 appliance, it will change the behavior of some SNMP version 3 functionality. SNMP versions 1 and 2c do not use encryption or hashing and are not affected by FIPS.

Note the following effects when using SNMP version 3:

- NoAuthNoPriv – This is not affected by FIPS.
- AuthNoPriv – Using MD5 as the authentication protocol does not work in FIPS mode. SHA does work, however.
- AuthPriv – Neither MD5 nor SHA works with either privacy protocol in FIPS mode.
- SNMP recipients will not receive notifications when the recipient definition violates FIPS requirements.
- SNMP polling (snmpget/walk/etc.) against an AppResponse 11 system will continue to function even if the polling system's SNMP settings violate FIPS requirements.

Software Update

Software update is not FIPS-compliant. FIPS must be disabled in order to update the software. Once the update has completed, FIPS may be re-enabled.

SSH

SSH requires the use of one of these ciphers to run in FIPS mode:

FIPS Mode

- aes128-cbc
- aes192-cbc
- aes256-cbc
- aes128-ctr
- aes192-ctr
- aes256-ctr
- 3des-cbc

The following MACs are allowed in FIPS mode:

- hmac-sha1
- hmac-sha2-256
- hmac-sha2-512

Syslog Notifications

This is unencrypted, and, therefore, FIPS-compliant.

TACACS+

The TACACS+ protocol is not FIPS-compliant, as it uses a non-compliant hash algorithm.

Web UI

Enable only TLSv1.2, and set the cipher string to the FIPS-compatible value
“TLSv1.2:kRSA:!eNULL:!aNULL”

You need to ensure imported and generated certificates for the web interface adhere to FIPS size requirements.

SSL Decryption

Decryption keys allow AppResponse 11 to develop and display performance metrics for SSL-encrypted data streams. An administrator at an endpoint of the encrypted data connection gives an AppResponse 11 administrator a PEM-formatted private key and, if necessary, a password or passphrase. The AppResponse 11 administrator places the private key into the Administration > General Traffic Settings: SSL Decryption Keys page and, if necessary, enters the password or passphrase. AppResponse 11 uses this to monitor the encrypted data for measuring packet statistics and obtaining information from packet headers.

Packets are decrypted “on the fly” as needed for Insights. You cannot store, dump or export decrypted packets. Decrypted packets or data cannot be exported to Wireshark, NetProfiler or other devices or applications outside the appliance.

Installed Keys Tab

To add a private key for SSL decryption

1. Go to Administration > General Traffic Settings: SSL Decryption Keys to open the SSL Decryption Keys page.
2. Choose Add to open the Add New SSL Decryption Key dialog.
3. Enter the name and description as you want it to appear on the SSL Decryption Keys page.
4. Copy the private key, including the BEGIN and END statements. The private key must be in PEM format, which appears similar to this:

```
-----BEGIN RSA PRIVATE KEY-----
MIIBAsTCCARqgAwIBAgIJJAQqvvgxZRcO+ZMA0GCSqGSIb3DQEBAUAMA8xDTALBgNVBAMTBElhenUwHhcNMDYxMDAyMTY0Mz
QxWhcNMTY
...
ehyejGdw6VhXpf4lP9Q8JfVERjCoroVkiXenVQe/zer7Qf2hiDB/5s02/
+8uiEeqMJpzsSdeYZUSgpyAcws5PDyr2GVFMI3dfPnl28hVavIkR8r05BP
-----END RSA PRIVATE KEY-----
```

DER format is not supported.

5. If required, enter the password or passphrase.
6. Choose Save to exit from this page and view the entry for the key on the SSL Decryption Keys page.

For AppResponse 11 to use the private key to decrypt data, SSL Decoding must be enabled on the Administration > Web Page Analysis page, in the Data Collection Options tab.

To delete a private key, either hover over the entry in the table and choose the delete (x) icon, or else select the check box at the beginning of the row and choose Delete near the top of the page.

Certificates With Installed Keys Tab

This tab shows the details for each certificate that matches the installed private keys. The details are the same we show in the “missing” tab.

Certificates With Missing Keys Tab

This tab lists streams for which encryption keys are not currently installed. Click Ignore to add a stream to the list of keys that should be ignored. Click Delete to remove a certificate from the database explicitly.

Ignored Keys Tab

This tab lists streams for which encryption keys are not currently installed, and are disregarded. Click Unignore to move a stream to the Certificates With Missing Keys tab. Click Delete to remove a certificate from the database explicitly.

PFS Tab

When communicating with systems using Perfect Forward Secrecy (PFS) for encryption, the AppResponse 11 system will need to buffer packets until it has received and accepted the unique Diffie-Hellman master secret to be used for the session. Select the Enable buffering for PFS decryption option in the PFS tab to activate this buffering. Refer to [KB article S35638](#) for additional information.

SSL Ciphers Supported For Decryption

The following RSA ciphers are supported for decoding:

OpenSSL Name	IANA Name
EXP-RC4-MD5	TLS_RSA_EXPORT_WITH_RC4_40_MD5
RC4-MD5	TLS_RSA_WITH_RC4_128_MD5
RC4-SHA	TLS_RSA_WITH_RC4_128_SHA
EXP-RC2-CBC-MD5	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
EXP-DES-CBC-SHA	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
DES-CBC-SHA	TLS_RSA_WITH_DES_CBC_SHA
DES-CBC3-SHA	TLS_RSA_WITH_3DES_EDE_CBC_SHA
AES128-SHA	TLS_RSA_WITH_AES_128_CBC_SHA
AES256-SHA	TLS_RSA_WITH_AES_256_CBC_SHA
NULL-SHA256	TLS_RSA_WITH_NULL_SHA256
AES128-SHA256	TLS_RSA_WITH_AES_128_CBC_SHA256
AES256-SHA256	TLS_RSA_WITH_AES_256_CBC_SHA256
CAMELLIA128-SHA	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
EXP1024-RC4-MD5	TLS_RSA_EXPORT1024_WITH_RC4_56_MD5
EXP1024-RC2-CBC-MD5	TLS_RSA_EXPORT1024_WITH_RC2_CBC_56_MD5
EXP1024-DES-CBC-SHA	TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA
EXP1024-RC4-SHA	TLS_RSA_EXPORT1024_WITH_RC4_56_SHA

OpenSSL Name	IANA Name
CAMELLIA256-SHA	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
SEED-SHA	TLS_RSA_WITH_SEED_CBC_SHA
AES128-GCM-SHA256	TLS_RSA_WITH_AES_128_GCM_SHA256
AES256-GCM-SHA384	TLS_RSA_WITH_AES_256_GCM_SHA384
CAMELLIA128-SHA256	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
CAMELLIA256-SHA256	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
AES128-CCM	TLS_RSA_WITH_AES_128_CCM
AES256-CCM	TLS_RSA_WITH_AES_256_CCM

The following Diffie-Hellman Ciphers ciphers are supported for decoding:

OpenSSL Name	IANA Name
DH-DSS-DES-CBC-SHA	TLS_DH_DSS_WITH_DES_CBC_SHA
DH-DSS-DES-CBC3-SHA	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA
DH-RSA-DES-CBC-SHA	TLS_DH_RSA_WITH_DES_CBC_SHA
DH-RSA-DES-CBC3-SHA	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA
DH-RSA-DES-CBC3-SHA	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA
EDH-DSS-DES-CBC-SHA	TLS_DHE_DSS_WITH_DES_CBC_SHA
EDH-DSS-DES-CBC3-SHA	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
EDH-RSA-DES-CBC-SHA	TLS_DHE_RSA_WITH_DES_CBC_SHA
EDH-RSA-DES-CBC3-SHA	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
DHE-RSA-DES-CBC3-SHA	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
DH-DSS-AES128-SHA	TLS_DH_DSS_WITH_AES_128_CBC_SHA
DH-RSA-AES128-SHA	TLS_DH_RSA_WITH_AES_128_CBC_SHA
DHE-DSS-AES128-SHA	TLS_DHE_DSS_WITH_AES_128_CBC_SHA
DH-DSS-AES256-SHA	TLS_DH_DSS_WITH_AES_256_CBC_SHA
DH-RSA-AES256-SHA	TLS_DH_RSA_WITH_AES_256_CBC_SHA
DHE-DSS-AES256-SHA	TLS_DHE_DSS_WITH_AES_256_CBC_SHA
DHE-RSA-AES256-SHA	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
DH-DSS-AES128-SHA256	TLS_DH_DSS_WITH_AES_128_CBC_SHA256
DH-RSA-AES128-SHA256	TLS_DH_RSA_WITH_AES_128_CBC_SHA256
DHE-DSS-AES128-SHA256	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
DH-DSS-CAMELLIA128-SHA	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA
DH-RSA-CAMELLIA128-SHA	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA
DHE-DSS-CAMELLIA128-SHA	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA

OpenSSL Name	IANA Name
DHE-RSA-CAMELLIA128-SHA	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
DHE-RSA-AES128-SHA256	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
DH-DSS-AES256-SHA256	TLS_DH_DSS_WITH_AES_256_CBC_SHA256
DH-RSA-AES256-SHA256	TLS_DH_RSA_WITH_AES_256_CBC_SHA256
DHE-DSS-AES256-SHA256	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
DHE-RSA-AES256-SHA256	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
DH-DSS-CAMELLIA256-SHA	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA
DH-RSA-CAMELLIA256-SHA	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA
DHE-DSS-CAMELLIA256-SHA	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA
DHE-RSA-CAMELLIA256-SHA	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
DH-DSS-SEED-SHA	TLS_DH_DSS_WITH_SEED_CBC_SHA
DH-RSA-SEED-SHA	TLS_DH_RSA_WITH_SEED_CBC_SHA
DHE-DSS-SEED-SHA	TLS_DHE_DSS_WITH_SEED_CBC_SHA
DHE-RSA-SEED-SHA	TLS_DHE_RSA_WITH_SEED_CBC_SHA
DHE-RSA-AES128-GCM-SHA256	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
DHE-RSA-AES256-GCM-SHA384	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
DH-RSA-AES128-GCM-SHA256	TLS_DH_RSA_WITH_AES_128_GCM_SHA256
DH-RSA-AES256-GCM-SHA384	TLS_DH_RSA_WITH_AES_256_GCM_SHA384
DHE-DSS-AES128-GCM-SHA256	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
DHE-DSS-AES256-GCM-SHA384	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
DH-DSS-AES128-GCM-SHA256	TLS_DH_DSS_WITH_AES_128_GCM_SHA256
DH-DSS-AES256-GCM-SHA384	TLS_DH_DSS_WITH_AES_256_GCM_SHA384
ECDH-ECDSA-RC4-SHA	TLS_ECDH_ECDSA_WITH_RC4_128_SHA
ECDH-ECDSA-DES-CBC3-SHA	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
ECDH-ECDSA-AES128-SHA	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
ECDH-ECDSA-AES256-SHA	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
ECDHE-ECDSA-NUL-SHA	TLS_ECDHE_ECDSA_WITH_NULL_SHA
ECDHE-ECDSA-RC4-SHA	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
ECDHE-ECDSA-DES-CBC3-SHA	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
ECDHE-ECDSA-AES128-SHA	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
ECDHE-ECDSA-AES256-SHA	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
ECDH-RSA-NUL-SHA	TLS_ECDH_RSA_WITH_NULL_SHA
ECDH-RSA-RC4-SHA	TLS_ECDH_RSA_WITH_RC4_128_SHA
ECDH-RSA-DES-CBC3-SHA	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA

OpenSSL Name	IANA Name
ECDH-RSA-AES128-SHA	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
ECDH-RSA-AES256-SHA	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
ECDHE-RSA-NULL-SHA	TLS_ECDHE_RSA_WITH_NULL_SHA
ECDHE-RSA-RC4-SHA	TLS_ECDHE_RSA_WITH_RC4_128_SHA
ECDHE-RSA-DES-CBC3-SHA	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
ECDHE-RSA-AES128-SHA	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
ECDHE-RSA-AES256-SHA	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
ECDHE-ECDSA-AES128-SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
ECDHE-ECDSA-AES256-SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
ECDH-ECDSA-AES128-SHA256	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
ECDH-ECDSA-AES256-SHA384	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
ECDHE-RSA-AES128-SHA256	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
ECDHE-RSA-AES256-SHA384	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
ECDH-RSA-AES128-SHA256	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
ECDH-RSA-AES256-SHA384	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
ECDHE-ECDSA-AES128-GCM-SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
ECDHE-ECDSA-AES256-GCM-SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
ECDH-ECDSA-AES128-GCM-SHA256	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
ECDH-ECDSA-AES256-GCM-SHA384	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
ECDHE-RSA-AES128-GCM-SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
ECDHE-RSA-AES256-GCM-SHA384	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
ECDH-RSA-AES128-GCM-SHA256	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
ECDH-RSA-AES256-GCM-SHA384	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
DHE-RSA-AES128-CCM	TLS_DHE_RSA_WITH_AES_128_CCM
DHE-RSA-AES256-CCM	TLS_DHE_RSA_WITH_AES_256_CCM
ECDHE-ECDSA-AES128-CCM	TLS_ECDHE_ECDSA_WITH_AES_128_CCM
ECDHE-ECDSA-AES256-CCM	TLS_ECDHE_ECDSA_WITH_AES_256_CCM
ECDHE-RSA-CHACHA20-POLY1305	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
ECDHE-ECDSA-CHACHA20-POLY1305	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
DHE-RSA-CHACHA20-POLY1305	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
TLS_AES_128_GCM_SHA256	TLS_AES_128_GCM_SHA256

OpenSSL Name	IANA Name
TLS_AES_256_GCM_SHA384	TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256	TLS_CHACHA20_POLY1305_SHA256
TLS_AES_128_CCM_SHA256	TLS_AES_128_CCM_SHA256
TLS_AES_128_CCM_8_SHA256	TLS_AES_128_CCM_8_SHA256

NetProfiler Integration

When using flow export to a NetProfiler:

- AppResponse 11 uses an SSL certificate to certify the identity of a target NetProfiler. AppResponse 11 has two default certificates that can be used by a NetProfiler.
- AppResponse 11 has a self-signed SSL certificate that it uses when it connects to a NetProfiler for flow export.

A self-signed certificate is generated automatically when AppResponse 11 boots if no certificate is installed. You also can provide a certificate of your own, signed by a Certificate Authority of your choice.

Important: Intermediate or chained certificates are not supported.

SSL certificates for flow export to NetProfiler are managed on the NetProfiler Integration page of the AppResponse 11 web UI. You must log in with read/write system configuration permissions to make changes to this page.

Here you can:

- view, retrieve, or replace the NetProfiler Export certificate.
- view, add or delete Trusted NetProfiler certificates.

Select the tab at the top of the page for the certificates of interest.

This section covers:

- [“Viewing the NetProfiler Export Certificate” on page 74](#)
- [“Replacing the NetProfiler Export SSL Certificate” on page 75](#)
- [“Viewing the Trusted NetProfiler Certificates” on page 76](#)
- [“Adding a Trusted NetProfiler Certificate” on page 76](#)

Viewing the NetProfiler Export Certificate

To view the SSL certificate

1. Go to Administration > Integration: NetProfiler Integration.
2. Select the NetProfiler Export Certificate tab.
3. The certificate details are displayed for the current certificate:
 - Issued to
 - Issued by
 - Validity
 - Fingerprint
 - Key

- PEM
- + Click Show/Hide PEM to display or hide (default) the PEM.

Replacing the NetProfiler Export SSL Certificate

You can replace the current certificate with an existing certificate or generate a new, self-signed certificate.

To replace the SSL certificate

1. Go to Administration > Integration: NetProfiler Integration.
2. Select the NetProfiler Export Certificate tab.
3. Click Replace at the top of the page.
4. The Specify Certificate window opens. Select to add an existing certificate or to generate a new one.
5. To import an existing certificate, supply the following information:
 - In the Certificate text box—paste the PEM-formatted certificate and private key.
 - In the Passphrase text box—enter the passphrase used to create an encrypted private key.
 - Note:** the passphrase is only used to decrypt the key, it is not stored.
 - Click **Save** to replace the existing certificate with the imported certificate or **Revert** to discard the information just entered.
6. To generate a new certificate, supply the following information:
 - Common name
 - Organization name
 - Organization unit name
 - Locality
 - State
 - Country code
 - Email
 - Click **Save** to generate a new certificate that replaces the existing certificate or **Revert** to discard the information just entered.

Important: It is important to make sure that the hostname and domain name are properly configured before generating the new certificate, as the new certificate contains hostname.domainname as the Common Name record. The hostname and domain name are specified on the Administration > System Settings: General web UI page, in the Hostname/DNS tab. See [“Hostname and DNS Servers” on page 89](#) for more information. The certificate details for each certificate show the Common Name record and other records encoded into the certificate.

Viewing the Trusted NetProfiler Certificates

To view the SSL certificate

1. Go to Administration > Integration: NetProfiler Integration.
2. Select the Trusted NetProfilers tab. A table is displayed showing the existing SSL certificates.
3. Hover with your mouse over the left end of the row that contains the SSL certificate to view. Click the eyeball icon.
4. The certificate details are displayed for the certificate:
 - Issued to
 - Issued by
 - Validity
 - Fingerprint
 - Key
 - PEM
 - Click Show/Hide PEM to display or hide (default) the PEM.
5. Click the 'x' in the top left corner of the window to close it.

Adding a Trusted NetProfiler Certificate

A new trusted certificate may be added using a name and a CA-signed public certificate in PEM format.

To Add an SSL Trusted NetProfiler certificate

1. Go to Administration > Integration: NetProfiler Integration.
2. Select the Trusted NetProfilers tab. A table is displayed showing the existing SSL certificates.
3. Click **Add** in the toolbar at the top of the table.
4. The Specify Certificate window opens.
5. Give the certificate a name.
 - The name must be unique, but the actual certificate does not need to be.
6. Add an existing CA-signed public certificate:
 - In the Certificate text box—paste the CA-signed public certificate in PEM format.
7. Click **Add** to save the new certificate or **Revert** to discard the information just entered.

Deleting a Trusted NetProfiler Certificate

To delete a Trusted NetProfiler certificate

1. Go to Administration > Integration: NetProfiler Integration.
2. Select the Trusted NetProfilers tab. A table is displayed showing the existing SSL certificates.
3. Hover with your mouse over the left end of the row that contains the SSL certificate to delete. Click the x icon.
4. Click **Delete** to remove the certificate or **Cancel** to keep it.

Flow Export Settings tab

The Flow Export Settings tab provides these controls:

- Enable Flow Export
- VoIP Quality metrics
- Configuring NetProfiler hostname/IP
- Manage Port Names and Custom Applications
- NetFlow v9

Click Apply or Revert.

Flow Export Traffic Selection tab

The Flow Export Traffic Selection tab provides these controls:

- Enable Flow Export on autodiscovered VIFGs, Export filter
- Integration with VIFG auto-discovery
- Options to Enable Flow Export, Disable Flow Export, Set Export Filter
- Table of VIFGs, Autodiscovered VIFGs

Flow Export Status tab

The Flow Export Status tab provides these controls:

- Brief description of each possible export status, info
- Brief explanation of flow count, including rejected flows

Server Response Time Analysis

Server Response Time (SRT) metrics can be reported for applications using TCP connections carrying request/response application layer protocols, for example, web, email, or SSH connections. To report these metrics AppResponse requires the following:

- AppResponse must see both directions of traffic flow on the same monitoring interface group (VIFG).
- TCP connection history expires on AppResponse when a long-lived connection is silent for more than five minutes. No SRT metrics are available for that connection.
- No SRT metrics are available for optimized connections.

Applications that meet these requirements for SRT analysis can be specified using one of the following modes:

- **Port Whitelist Mode**—This mode uses two steps to specify applications. The first step uses the first table to specify the ports and optional servers to *include* when reporting Server Response Time metrics. The second step uses the bottom table to specify ports and optional servers included by the first table that are to be *excluded* when reporting Server Response Time metrics.

For example, you may want SRT metrics for internal web traffic but not for external web traffic. You could add information to the first table on the ports used for web traffic. In the second table you would use the same ports and add external Web Server IP addresses to exclude reporting SRT metrics for the external web traffic.

- **All Ports Mode**—The table entries exclude the ports and optional servers specified from Server Response Time reporting. Server Response Time is reported for all other ports and servers.

Configuring the Mode

The Server Response Time (TCP) page is used to configure the mode to be used and to specify the ports and optional servers for reporting SRT. The mode is set on the General tab and the ports and servers for each mode are specified on their respective tabs, Port Whitelist or All Ports.

1. Go to Administration > Feature Settings: Server Response Time (TCP), General tab.
2. Click the radio button next to the mode you wish to use. By default, Port Whitelist mode is enabled.
3. Click **Apply** to make or **Revert** to reset the change made.

Configuring Port Whitelist Mode

In this mode, AppResponse 11 includes only traffic matching the ports and optional server specifications in the first table not excluded by the second table when reporting Server Response Time metrics.

- Port entries with no server(s) specified apply to applications on those ports on *all* servers.
- Port entries with a server or servers specified apply only to applications on those ports on those servers.

Note: The mode currently being used is shown above the table.

In the first table, specify ports and optional servers to be included when reporting SRT metrics:

1. Go to Administration > Feature Settings: Server Response Time (TCP), Port Whitelist tab.
2. Click the **Add** button to open the New Ports and optionally Servers to Include window.
3. Select or clear the check box to enable or disable the entry.
4. Enter a comma-separated list of the TCP ports to include. The list can contain:
 - one or more ports.
 - a range of ports.
5. Optionally, enter a comma-separated list of IPv4 and IPv6 server IP addresses to include. Standard or CIDR IP addresses are supported. The list can contain:
 - one or more IP addresses.
 - a range of IP addresses.
6. Click **Save** to add the ports and servers to the table.

In the second table, specify ports and optional servers in the first table to be excluded when reporting SRT metrics:

1. Go to Administration > Feature Settings: Server Response Time (TCP), Port Whitelist tab.
2. Click the **Add** button to open the New Ports and optionally Servers to Include window.
3. Select or clear the check box to enable or disable the entry.
4. Enter a comma-separated list of the TCP ports to exclude. The list can contain:
 - one or more ports.
 - a range of ports.
5. Optionally, enter a comma-separated list of IPv4 and IPv6 server IP addresses to exclude. Standard or CIDR IP addresses are supported. The list can contain:
 - one or more IP addresses.
 - a range of IP addresses.
6. Click **Save** to add the ports and servers to the table.

Configuring All Ports Mode

In this mode, Server Response Time metrics are reported only for traffic *not* matching the port and optional server specifications in the table. Traffic that matches the ports and optional server specifications listed in the table are excluded.

- Port entries with no server(s) specified apply to applications on those ports on *all* servers.

- Port entries with a server or servers specified apply only to applications on those ports on those servers.

Note: The mode currently being used is shown above the table.

To add ports and servers to the table:

1. Go to Administration > Feature Settings: Server Response Time (TCP), All Ports tab.
2. Click the **Add** button to open the New Ports and optionally Servers to Exclude window.
3. Select or clear the check box to enable or disable the entry.
4. Enter a comma-separated list of the TCP ports to exclude. The list can contain:
 - one or more ports.
 - a range of ports.
5. Optionally, enter a comma-separated list of IPv4 and IPv6 server IP addresses to exclude. Standard or CIDR IP addresses are supported. The list can contain:
 - one or more IP addresses.
 - a range of IP addresses.
6. Click **Save** to add the ports and servers to the table.

Editing Table Entries

The table entries in the tables on the Port Whitelist tab or the All Ports tab can be edited as follows:

1. With the mouse, hover over the table row to be edited.
2. Click the pencil icon that appears near the right end of the row.
3. The contents of the row can be modified as needed.
 - Set or clear the check box to enable or disable the entry.
 - Each port or port range can be deleted by clicking the **x** at the end of an item.
 - Each server or range of servers can be deleted by clicking the **x** at the end of an item.
4. Click **Save** to make or **Revert** to reset the change made.

Deleting a Table Entry

To delete a row in a table:

1. With the mouse, hover over the row to be deleted.
2. Click the **x** that appears at the right end of the row.

To delete multiple table rows at once:

1. With the mouse, hover over the row to be deleted.

2. Set the check box on the left end of each row to be deleted.
3. Click the **Delete** button in the toolbar at the top of the table.

General Settings

Management Interfaces

Initial configuration of the management interfaces, primary and aux, is done through the CLI when AppResponse 11 is installed. Additional configuration and updates can be done on this page.

Primary Interface — The primary interface is the appliance management interface. You connect to the primary interface to use the Web UI or the CLI.

Auxiliary Interface — The auxiliary interface is an optional port you can use to connect to a non-Riverbed network management device.

Note: The IP address for the auxiliary interface must be on a subnet different from the primary interface subnet.

Main Routing Table — Displays a summary of the main routing table. If necessary, you can add static routes that might be required for out-of-path deployments or particular device management subnets. If there are multiple subnets on the Aux interface network, or if you need to use a gateway router other than the default gateway, it may be necessary to define static routes.

When configuring the management interfaces:

- IPv4 and IPv6 addresses are supported on both management interfaces.
- Interface changes require a system reboot.
- Available routes include system-defined routes, DHCP-supplied routes, and user-defined routes. The listed routes may change when a configuration change occurs.

This section covers the following:

- [“Default Gateway” on page 82](#)
- [“Configuring Management Interfaces” on page 83](#)
- [“Managing Routes” on page 83](#)

Default Gateway

The default gateway provides network access beyond the local area network to the management interfaces. This can be important when a static IP address is specified for a management interface. When DHCP is used, the default gateway may be ignored and a gateway defined by the DHCP server may be used instead. The System Gateways are displayed in read-only fields just to the right of the Default Gateway input panel.

Configuring Management Interfaces

1. Go to Administration > System Settings: General, and select the Management Interfaces tab.
2. Select the management interface to configure, primary or aux, from the drop-down list.
3. Enable the interface by selecting the check box.
4. Select the interface settings or choose to auto-negotiate them:
 - Speed (drop-down list)
 - Duplex (drop-down list)
 - MTU can range from 68 - 16110 bytes; default is 1500 bytes
 - Information shows the current status of the interface.
5. Select the interface IP addresses:
 - DHCP can only be used for the primary *or* the aux interface, not both. In addition, DHCP can be used for *either* the IPv4 or the IPv6 address on the interface, but not both. If available, Dynamic DNS can be enabled.
 - Static IP address and prefix. See [“Default Gateway” on page 82](#) for related information.
 - Disabled is checked when an IPv4 or IPv6 address is not used.
6. Click **Apply** or **Revert** to make or reset the changes made. Interface changes require a system reboot.

Managing Routes

IPv4 and IPv6 routes are listed at the bottom of the web UI page. The routes listed can come from three sources:

- Automatically generated by the system. These routes cannot be edited or deleted.
- Added automatically by a DHCP server. These routes cannot be edited or deleted.
- Defined by a user. These are also referred to as static routes. These routes can be edited or deleted.

Note: Routes from the first two sources can change or disappear when management interface settings are changed.

The following examples illustrate typical route definitions:

- Route to a specific destination:
 - Destination IP Address: 192.0.2.7
 - Subnet Mask: 32
 - Gateway: 10.33.158.1
- Route to a range of IP addresses:
 - Destination IP Address: 198.51.100.0
 - Subnet Mask: 24

- Gateway: 10.33.158.1 or 0.0.0.0

Adding Routes

A toolbar in the top-left corner of a route table contains Add and Delete icons.

1. Click **Add**.
2. Specify the route information requested.
 - Destination IP address.
 - Subnet Mask (prefix).
 - Gateway IP address.
 - Select the Interface to use this route.
3. Click **Save** to save the route.

Editing a Route

Routes added by a user can be edited by roles with read/write access. System routes or DHCP supplied routes cannot be edited.

1. With the mouse, hover over the route to be edited.
2. Click the pencil icon at the end of the row.
3. In the Edit Route window, make the changes required.
4. Click **Apply** to save the revised route.

Deleting a Route

Routes added by a user can be edited by roles with read/write access. System routes or DHCP supplied routes cannot be edited.

1. With the mouse, hover over the route to be deleted.
2. Click the **x** at the end of the row.

Alternatively, you can use the Delete icon in the toolbar to delete a route as follows.

1. Hover over a route to be deleted.
2. Select the check box on the left for the route to be deleted.
3. Click **Delete** to remove the route.

The delete button is disabled if the selected route cannot be removed.

Time

The system date and time are configured in the command line interface (CLI) when AppResponse 11 is installed. You can change the system date and time in the Time tab on the Administration > System Settings: General page. Changes to these settings can only be made by a user with read/write system configuration permissions.

The system date and time changes can be entered manually or synched with a PTP or NTP server. By default, AppResponse uses the Riverbed-provided NTP server and these public NTP servers:

- 0.riverbed.pool.ntp.org
- 1.riverbed.pool.ntp.org
- 2.riverbed.pool.ntp.org
- 3.riverbed.pool.ntp.org

Important: PTP is not supported when using AppResponse 11 virtual edition.

This section covers the following:

- “Time zone”
- “Configuring PTP”
- “Configuring NTP”
- “Manually Setting Date and Time”

Time zone

Select your time zone from the drop-down list. The default is America/Los_Angeles. You also can select GMT or UTC for the time zone.

Note: To select how the time zone is displayed, go to the Administration > Other: User Preferences page and see [“Language and Time” on page 94](#).

Configuring PTP

To use PTP a clock source must be reachable using the selected interface.

1. On the Time tab, select PTP.
2. Select the base interface connected to the PTP clock source from the drop-down list.
3. Select the transport protocol used from the drop-down list.
4. Click **Apply** to submit the changes or **Revert** to dismiss them.
 - If you click Apply the time is changed and you are automatically logged out.

PTP Status

The PTP status is reported on the PTP Status tab at the Administration > System Settings: General page, in the Time tab:

- the Active Sync status.
- the local clock offset from the Master clock.
- the IP address of the PTP clock source.

Configuring NTP

1. On the Time tab, select NTP.
2. Click **Apply** to submit the change or **Revert** to dismiss it.
3. You are automatically logged out and must log in with read/write system configuration permissions to have the changes made.

Configuring NTP Servers

Four Riverbed public NTP servers are defined by default. These servers can be edited or deleted. Configure new NTP servers as follows.

1. Go to Administration > System Settings: General page, and select the Time tab. Go to the NTP Servers section.
2. Click **Add** in the toolbar at the top of the table.
3. In the New NTP Server window enter the following:
 - **Hostname or IP Address** supports IPv4 and IPv6 addresses.
 - **Prefer** can be enabled for this NTP server by checking or unchecking the box.
 - **Version** is the NTP protocol version used. Select the version from the drop-down list.
 - **Encryption** the type used is selected from the drop-down list. Select N/A if no encryption used (default).
 - **Key** is an 8-character ASCII string used in server authentication.
 - **Enter the key ID** is a value from 0 to 65534, used in server authentication.
4. Click **Save** to add the NTP server.

Editing NTP Servers

To revise an existing NTP server do the following.

1. With the mouse, hover over the NTP server to be edited.
2. Click the pencil icon at the end of the row.
3. In the Edit NTP Server window, make the changes required.

4. Click **Save** to make the changes to the NTP server.

Deleting an NTP Server

1. With the mouse, hover over the NTP server to be deleted.
2. Click the **x** at the end of the row.

Alternatively, you can use the Delete icon in the toolbar to delete an NTP server as follows.

1. Hover over a route to be deleted.
2. Select the check box on the left for the route to be deleted.
3. Click **Delete** to remove the route.

NTP Server Status

1. Go to Administration > System Settings: General page, and select the Time tab. Go to the NTP Servers section.
2. A table lists the current available NTP servers with the following information:
 - **Active:** Only one NTP server can be active and it has a value of true. All other servers have a value of false.
 - **Server:** NTP server name or IP address.
 - **Auth Status:** True if authentication is used and the server is authenticated.
 - **Key ID:** Specified when the NTP server is configured.
 - **Ref ID:** System peer ID used to identify the time source.
 - **Configured:** True if you configured this server, False if it was discovered on the network.
 - **Offset [ms]:** The time difference between the reference clock and the system clock.

Manually Setting Date and Time

1. On the Time tab, select Use Local Clock.
2. Click the pencil icon to the left of the displayed date and time.
3. In the Local System Time window, Change Time, click to revise the date and time. The format is MMM DD, YYYY HH:MM:SS AM *or* PM.
4. To change the displayed time zone, select a new time zone from the drop-down list in the Time Zone field at the top of the page.
5. Click **Save** to make the changes, **Revert** to dismiss them.
6. Click **Apply** to submit the changes or **Revert** to dismiss them.

7. You are automatically logged out and must log in with read/write system configuration permissions to have the changes made.

Hostname/DNS

Use the controls on this tab only if you require modifications, additional configuration, or want to verify the DNS configuration:

Hostname—Modify the hostname only if your deployment requires it.

DNS Settings—Riverbed recommends you use DNS resolution.

Static Name Resolution—If you do not use DNS resolution, or if the host does not have a DNS entry, you can create a host-IP address resolution map.

Hostname and DNS Servers

The default hostname, *appresponse*, can be changed if required. DNS servers and domains can be added and revised on this tab. Note that if DHCP is in use, DNS settings configured by DHCP will be shown in the read-only System DNS Settings field. Only the first three DNS servers that are set are displayed. Go to Administration > System Settings: General, and click the Hostname/DNS tab.

1. Open the Hostname and DNS tab.
2. Hostname is an alphanumeric name or IPv4 address. The hostname appears on the left in the fixed heading of the AppResponse 11 web UI.
3. DNS Servers are added in priority order (primary, secondary, tertiary). Up to three IPv4 addresses can be specified. If there are DNS servers set by DHCP, the user-supplied servers are prepended to the list. Only the first three DNS servers that are set are displayed.
4. DNS Domain List entries are added in priority order, high-to-low, one DNS domain per line. Type a DNS domain and press Enter to advance to a new line. If you specify domains, the system automatically finds the appropriate domain for each of the hosts that you specify in the system.
5. When finished, click **Apply** to save your entries or **Revert** to discard them.

Static Name Resolution

To specify a static hostname and IP address, follow the instructions below.

1. Go to Administration > System Settings: General, and click the Hostname/DNS tab.
2. Go to the Static Name Resolution section and click Add to display the New Host dialog.
3. Hostname is an alphanumeric name or IPv4 address to replace the default hostname.
4. Enter the IPv4 or IPv6 address to be used for the Hostname.
5. When finished click **Save**.

Editing a Static Hostname

A static name can be edited using the instructions below.

1. Go to Administration > System Settings: General, and click the Hostname/DNS tab.
2. Go to the Static Name Resolution section.
3. With the mouse, hover over the static hostname to be edited and click the pencil icon on the right-end of the row.
4. Revise the Hostname and IP Address as needed.
5. When finished, click **Save** to save your changes or **Revert** to discard them.

Deleting a Static Hostname

Statics names can be deleted using the instructions below.

1. With the mouse, hover over the hostname to be deleted.
2. Click the **x** that appears at the end of the row.

To delete a group of static names all at once, do the following:

1. With the mouse, hover over a hostname to be deleted and click the check box that appears to the left of the name.
2. Repeat Step 1 for all hostnames to be deleted.
3. Click **Delete** in the toolbar at the top of the table to remove the hostnames.

Exporting and Importing Static Hostnames

Static hostnames can be exported and imported via CSV (comma-separated value) file. Click Export to create the file, “staticNames.csv”, or click Import to read in a CSV file listing static hostnames. The import function replaces all existing hosts with those defined in the imported CSV file.

The CSV file displays lists each static host by hostname and IP address columns. Here is an example of the file format:

```
#Version:,AR11
#Data Type:,Hosts
#Timestamp:,Thu Jul 13 2017 12:23:51 GMT-0700 (EDT)
Hostname,IP
www.google.com,1.1.1.1
www.google.com,1.1.1.2
www.google.com,1.1.1.3
www.google.com,1.1.1.4
www.google.com,2.1.1.5
www.apple.com,3.2.2.2
```

SNMP

AppResponse 11 supports the use of SNMP for traps and polling. No license is required for SNMP support.

Configure SNMP polling for the AppResponse 11 appliance by clicking Administration > System Settings:General and selecting the SNMP tab. The following controls are provided:

- Enable SNMP – Activate or deactivate SNMP.
- Download MIB – Download the device's MIB to your local system.
- SNMP Version – Choose the version of SNMP to use.
- Location – Type information about where the device resides. This can be between 0 and 255 characters long.
- Description – Type a meaningful description of the device. This can be between 0 and 255 characters long.
- Contact – Provide contact information for the administrator. This can be between 0 and 255 characters long.
- Community – Type the SNMP community string if you're using version 1 or version 2c. This must be between 1 and 31 characters long.
- Username – Specify the user account
- Security Level – For version 3, choose one of:
 - NoAuthNoPriv – Authentication and privacy both are disabled.
 - AuthNoPriv – Authentication is enabled and privacy is disabled.
 - AuthPriv – Authentication and privacy both are enabled.
- Authentication Passphrase – For AuthNoPriv or AuthPriv, specify the string to use for authentication. This must be at least 7 characters long.
- Authentication Protocol – Choose MD5 or SHA as the authentication regime.
- Privacy Passphrase – For AuthNoPriv or AuthPriv, specify the string to use as an additional password. This must be at least 7 characters long.
- Privacy Protocol – Choose DES or AES. For each, 128 bit encryption is supported.
- Apply/Revert – Make the changes take effect, or return to the previous saved settings.

Considerations For Using SNMP In FIPS Mode

When FIPS mode is enabled on the AppResponse 11 appliance, it will change the behavior of some SNMP version 3 functionality. SNMP versions 1 and 2c do not use encryption or hashing and are not affected by FIPS.

Note the following effects when using SNMP version 3:

- NoAuthNoPriv – This is not affected by FIPS.
- AuthNoPriv – Using MD5 as the authentication protocol does not work in FIPS mode. SHA does work, however.

- AuthPriv – Neither MD5 nor SHA works with either privacy protocol in FIPS mode.
- SNMP recipients will not receive notifications when the recipient definition violates FIPS requirements.
- SNMP polling (snmpget/walk/etc.) against an AppResponse 11 system will continue to function even if the polling system's SNMP settings violate FIPS requirements.

Integration Links

Click Administration > Integration: Integration Links to display the Integration Links page for managing communication to other applications; the Integration Links command also is available in the right-click menu for relevant objects. The page provides two tabs: Riverbed SteelCentral for managing communication to other SteelCentral applications, and External, for managing communication to third party applications.

- Riverbed SteelCentral tab – Configure communication with other supported Riverbed SteelCentral applications. Each of these applications is enabled by default.
- External tab – Configure communication with third party applications. Click Add to display the New External Link dialog, and specify the parameters and values that are necessary for establishing communication with the other application. The following parameters are supported:
 - hostname
 - protocol
 - port
 - integer
 - string

Administration - Other

This section is where you configure other system settings and access important system tools, such as system dumps and licenses.

The following topics are covered here:

- [“User Preferences” on page 94](#)
- [“Email Server” on page 96](#)
- [“Recipients” on page 98](#)
- [“System Dumps” on page 106](#)
- [“Licensing” on page 22](#)
- [“Storage Status and Usage” on page 113](#)

User Preferences

Change default AppResponse 11 settings for language, information style, and search using this page. An example of your selections for date, time, and time zone styles appears in a shaded box under those settings.

This section covers the following:

- [“Language and Time”](#)
- [“Appearance”](#)
- [“Data Units”](#)
- [“Default Insight”](#)
- [“Search Settings”](#)
- [“Built-In Policy Preferences”](#)

Language and Time

Change the language used in the UI and your time zone and style as follows:

1. Go to Administration > Other: User Preferences page.
2. Choose a supported language from the drop-down list.

3. Change the time zone by deleting the current entry and entering the geographic area or city name. Scroll through the displayed list and select the desired time zone.
4. Select the format used to display the time zone: the abbreviated time zone name, the UTC offset, or both.
5. Select a date style from the options displayed.
6. Select a time style from the options displayed.
7. Click **Apply** to save or **Revert** to reset the change(s) made.

Appearance

The Appearance settings enable you to control the overall aesthetic presentation of the web UI.

Change the appearance of your web UI as follows:

1. Go to Administration > Other: User Preferences page.
2. Choose the Theme that controls the web UI's overall display scheme: Light (the default) or Dark.
3. If you want to display in the flag of the country of origin of traffic in IP conversations, choose Display Country Flag for IP/IP Conversation.
4. Click **Apply** to save or **Revert** to reset the change(s) made.

Data Units

Change the default data units used to display Traffic Volume and Traffic Throughput style in the UI as follows:

1. Go to Administration > Other: User Preferences page.
2. Select a default unit for displaying Traffic Volume from the drop-down list.
3. Select a default unit for displaying Traffic Throughput from the drop-down list.
4. Click **Apply** to save or **Revert** to reset the change(s) made.

Default Insight

Choose to display an Insight on the Home and select the Insight to display by default as follows:

1. Go to Administration > Other: User Preferences page.
2. Set or clear the check box to display an Insight on the Home page.
3. Change the current Insight by deleting the current entry and:
 - typing a term to filter the list of choices

- clicking in the empty text box to display a list of all Insights to choose from.
4. Click **Apply** to save or **Revert** to reset the change(s) made.

Search Settings

Configure the search behavior using these controls:

1. Click the Perform data search option if you want searches to look at recorded data in addition to the configuration.
2. Specify the default data search time interval, in seconds. The default is 3600.
3. Specify the search timeout value, in seconds. The default is 15.
4. Specify the number of matches in the configuration that can be returned in search results. The default is 2000.
5. Specify the number of matches in recorded data that can be returned in search results. The default is 50.
6. Click **Apply** to save or **Revert** to reset the change(s) made.

Built-In Policy Preferences

When you are logged in to the web UI, by default, you will receive a summary of events for built-in policies every ten minutes. This behavior can be configured: you can disable the built-in policy notifications, or you can change the interval at which the summary notification is sent.

To configure your preferences for built-in policy notifications:

1. Go to Administration > Other: User Preferences page.
2. The option, Enable built-in policy live notifications, is selected by default. Deselect it if you do not want to receive these notifications.
3. Optionally, change the Built-in policy live notification frequency. This is set to 10 minutes, by default.
4. Click **Apply** to save or **Revert** to reset the change(s) made.

Email Server

AppResponse 11 can automatically notify you by email when an alert occurs. An alert can be triggered by a policy violation. The email notification indicates the cause of the alert, with tag information included in HTML emails.

Specifying an email server

To send email, AppResponse 11 requires the address of an external SMTP email server.

To specify an email server

1. Go to the Administration > System Settings: General page and click the Email tab.
2. In the SMTP Server field, enter the IP address of the email server to be used for relaying email. This cannot be the AppResponse 11 appliance itself.

If a DNS server has been specified on the Administration > System Settings: General page, Hostname/DNS tab and is functioning, you can enter a hostname instead of the IP address. Alternatively, you can enter a fully qualified domain name.
3. Enter the port that AppResponse 11 should connect to. The default port is 25, but port numbers 1 through 65535 are valid. Note that this field will be populated automatically if you choose a Security option: port 587 for SSL/TLS, or port 587 for STARTTLS.
4. Enter the SMTP Timeout value as seconds. This is the length of time AppResponse 11 waits after attempting to connect to the email server before assuming that the connection attempt failed. The default value is 30 seconds.
5. Choose an option for providing security between the client and server at the transport layer (SMTPS): None (the default, using a plaintext socket), SSL (uses SSL handshake), or STARTTLS (begins with plaintext socket, but encrypts data after connecting). The server certificate is not validated automatically, so connections to SMTP servers using SSL or STARTTLS will be accepted even if the server certificate is invalid.
6. Optionally, type a username and password to use to authenticate with the SMTP server before sending mail. If either the username or the password is set, and not empty, then both values must be provided.
7. Enter the From Address. This can be any email address in a valid format. This address appears in the "From" field when AppResponse 11 sends a notification email to a recipient. (The SMTP server may also forward a copy of the notification to the "From" address.)
8. If you are ready to send email notifications, select the Enabled check box. If you are not ready for the appliance to start sending email, deselect the check box.
9. Choose Apply. Alternatively, choose Revert to delete any changes you have made and revert to the previous settings.

Recipients

Recipients can be notified by Email, SNMP trap, Syslog notification (including encrypted Syslog), or ServiceNow incident when a policy violation causes an alert. Recipients can be defined on the Definitions > Recipients page to make them available for inclusion in policy definitions, or they can be defined as needed when defining a policy.

Defining Recipients

A recipient is a named list consisting of one or more Email addresses, or a single SNMP receiver, Syslog host, Encrypted Syslog host (see [“Encrypted Syslog Support,”](#) for details), or ServiceNow URL (see [“ServiceNow Support”](#) for details).

To specify a recipient

1. Go to the Definitions > Recipients page.
2. Choose Add to create a new recipient entry.
3. Type the name of the recipient as you want it to appear wherever a user looks at a recipients list.
4. Select the type of the recipient: Email, SNMP, Syslog, Encrypted Syslog, or ServiceNow, with each recipient being a single type. Selecting an option makes relevant fields for it accessible. Specify the details that will enable a notification to reach that recipient.
5. Choose Save.

Recipients and their details are listed on the Recipients page. You can click Test to send a notification to the recipient to confirm that it's been configured as you expect.

To edit a recipient entry

1. Hover your mouse over an entry to display the edit icon (pencil).
2. Choose the edit icon and make your edits on the Edit Recipient page.
3. Choose Save to keep your edits or Revert to return to the previous specification.

To delete recipient entries

1. Hover your mouse over an entry to display the check box at the beginning of the entry and the delete icon (x) at the end of the row.
2. Either
 - choose the delete icon to delete a single entry, or
 - select the check box at the beginning of the row and then choose Delete near the top of the page.

Encrypted Syslog Support

Encrypted Syslog is supported as an alert recipient (see “[Recipients](#),” for details) for sending secure notifications to a remote syslog server, as defined in RFC 5425.

These controls are provided for configuring an encrypted syslog recipient:

- Click to configure encrypted syslog local certificate – This displays the General System Settings page, open to the Encrypted Syslog Certificate tab. This is the certificate that the remote server uses to verify the AppResponse 11 system's identity, and it is used only when connecting to a remote syslog server. A self-signed certificate can be generated, or a certificate and private key can be imported.
- Host – Type the hostname or IP address of the syslog server.
- Port – This defaults to 6514, the well known port for encrypted syslog.
- Auth method – For both of these methods, the certificate must match the hostname being contacted (the Subject/Common Name). If validation of the server fails, the connection will be terminated, and no syslog message will be sent.
 - Certificate validation – This is the preferred authentication method. Add the root CA and any intermediate certificates for the remote syslog server. When the remote server is connected, the server's certificate is verified as properly signed; the same as for a typical browser connection. The server's certificate does not need to be known ahead of time.
 - Certificate matching – For this, enter the server's certificate here. When a connection is made, the certificate presented by the server is compared with this certificate, and the server is authenticated if the two match.
- Certificates
 - Add – Click this to display the Add Certificate dialog, in which you can type a certificate name and paste in its CA-signed certificate, in Privacy Enhanced Mail (PEM) format. Up to 30 certificates can be added for one remote syslog server.

Backup/Restore Considerations

Encrypted syslog uses a private key to identify the AppResponse 11 system. Configuration backups are not encrypted, so that private key is not included in the backup. After a restore, the system creates a new self-signed certificate and key for itself. Depending on how the remote syslog server is configured, it's likely that you will need to reconfigure the AppResponse 11 system's old certificate and key manually. This behavior is the same as the certificate/key used for web UI connections. Note that certificates for the remote servers are public by nature, and these *are* included in configuration backups.

ServiceNow Support

ServiceNow is supported as an alert recipient (see [“Recipients”](#) for details). The ServiceNow instance does not require the presence of an AppResponse app in order to integrate with AppResponse. In ITSM mode (the default), AppResponse writes to the default ServiceNow incidents table.

When defining a ServiceNow recipient, choose one of the following modes:

- Incidents Table in ITSM - (Default) In this mode (IT service management), a ServiceNow Incident is created (or updated if it exists already) when an AppResponse alert notification is sent.
- Events Table in ITOM - In this mode (IT operations management), a ServiceNow Event is created (or updated if it exists already), and a ServiceNow Alert is created and associated with the Event whenever an AppResponse alert notification is sent.

In addition, if you want to pass along to ServiceNow information contained in user-defined tags for apps and Host Groups, you can enable Send Tags to ServiceNow; this is disabled by default. If you do wish to send tags, you must also specify the names of the ServiceNow fields that are to receive the tags. Only the first tag name (alphabetically) listed in the Alert Detail report is included in the ServiceNow notification. Refer to [“Tag Configuration”](#) if you want to see the corresponding description.

Note that the ServiceNow account that AppResponse 11 uses to facilitate integration must be created manually in ServiceNow. The ServiceNow account requires the following roles:

- ITOM integration:
 - evt_mgmt_integration
 - evt_mgmt_operator
- ITSM integration:
 - itil

Business Hour Profiles

Click Definitions > Business Hour Profiles to display the Business Hour Profiles page for working with flexible time definitions for use with “Policies”, “Insights”, and the “Navigator”. Business hour profiles provide a means for you to enable policies for one or more specific time ranges, and to specify time intervals for Insights and the Navigator.

Click Add on the Business Hour Profiles page to display the New Business Hour Profile dialog. Type a name (up to 255 characters in length) and a description for the profile, then specify one or more (up to 100) non-overlapping time ranges that will define it. Once the profile definition has been saved, it is available for use and listed in the Business Hours pulldown menu in the Create New Policy dialog, and when specifying a time interval for Insights and the Navigator.

One business hour profile, named Work Week, is built in and cannot be deleted, but can be edited. It specifies a time period of 9:00 AM to 5:00 PM, Monday through Friday.

Note: Policies outside of their profile period will not be evaluated, and will not generate alerts. If the policy is monitoring a data source that is a few minutes behind the current clock time, alerts may appear for a minute or two after the profile period is over; this is because the data queries are based on the *data* timestamps, not the current clock timestamp.

System Operations

This section describes system level tools and operations such as rebooting or shutting down AppResponse 11. There is a command-line interface (CLI) available, but most operations are available under the Administration tab in the AppResponse 11 menu bar in the web UI.

Special operations, such as reinitializing and changing storage unit RAID mode can only be done through the CLI.

Configuring and managing storage units

The AppResponse 11 6170 base unit (SCAN-06170) and the 8170 base unit (SCAN-08170) have no internal storage. You can connect storage units *of the same model*, either SCAN-SU-48TB or SCAN-SU-72TB to a base unit.

- Up to eight external storage units can be connected to a 6170 base unit for storage.
- Up to sixteen external storage units can be connected to an 8170 base unit for storage.

A base unit runs an initialization process to identify connected and powered on storage units and formats storage.

- If a base unit has no initialized storage units, for example, when first installed, an automatic initialization is performed when it is booted. Automatic initialization is *always* performed at boot time, and reinitializes any uninitialized storage unit independent of the state of any other storage unit.
- Initialization is done at the storage unit level, that is, an uninitialized storage unit is initialized whenever the base unit boots.
- Initialization fails
 - if an invalid storage unit is detected
 - if a disk fails
 - If an incompatible disk is found
- The initialization process formats storage as RAID 0 storage by default. After initialization, storage can be reinitialized as RAID 1, RAID 5, or RAID 6 for storage redundancy, using the AppResponse 11 CLI.
- If a storage unit fails or is removed, storage may continue to function but with a limited capacity. If all storage units fail or are removed, storage will not function.
- Reinitializing a storage unit destroys all data on that single storage unit. All other storage units are unaffected.

AppResponse 11 CLI Storage and Service commands

Storage unit configuration and management is done using the AppResponse 11 Command-Line Interface. For more information see [“Command-Line Interface Operation” on page 233](#).

Storage Unit Status

- `show storage units`—displays storage units status and details
- `show storage unit <name>`—displays storage unit <name> status and details

Storage Data Section Status

- `show storage data_sections`—displays storage data sections status and details
- `show storage data_section <name>`—displays storage data section <name> status and details

Storage Data Module Status

- `show storage data_modules`—displays storage data modules status and details

- `show storage_data_module <name>`—displays storage data module <name> status and details

Storage Data Section Reinitialization

- `storage_data_section <name> reinitialize`—reinitializes data section <name> using the default RAID0 mode

Storage Data Section Mode Change

- `storage_data_section <name> reinitialize mode <raid0|raid1|raid5|raid6>`—Changes the RAID mode used by the data section <name>

Initializing storage units

When a base unit boots, it detects connected and powered up storage units. It then automatically initializes each identified storage unit and formats it for storage. Each storage unit's identity is stored by the base unit and the storage unit is formatted as RAID 0 storage by default.

If other storage units are connected and powered on after a base unit boots, they are not detected or displayed until the base unit is rebooted. After a reboot, the storage units are automatically initialized and their "Status:" is "active" and "In Use:" is "yes" indicating that packet_storage is configured on the storage unit.

For AppResponse 11 installation instructions and troubleshooting see the *SteelCentral AppResponse 11 Installation Guide, Models xx70* available on the Riverbed Support site.

Changing the Storage RAID level

For redundancy, storage can be reinitialized to RAID 0, RAID 1, RAID 5, or RAID 6 using the AppResponse 11 CLI. When changing the format of storage all existing packet data is lost.

For example, to change the storage RAID level on storage unit LDABC12345678 follow the steps below.

1. Using a terminal emulator such as PuTTY or Tera Term, SSH to the AppResponse 11 CLI.

2. Enter:

```
no storage_data_area packet_capture section LDABC12345678
```

3. Enter:

```
storage_data_section LDABC12345678 reinitialize mode <RAID0|RAID1|RAID5|RAID6>
```

storage is available within seconds but the storage status will be rebuilding until it is completed. When the storage is reinitialized in RAID 1, RAID 5, or RAID 6, the rebuild process starts after a few minutes. If changing the storage to RAID 0, it is available immediately.

4. Enter

```
storage_data_area packet_capture section LDABC12345678
```

5. Once completed you can use the following command to check the storage unit mode:

```
show storage unit LDABC12345678
```

System Dumps

Three types of system dumps can be created and stored as a compressed file (.tgz) by an AppResponse 11 system:

- **Logs**—includes log files, stack traces, and some additional diagnostics as well as version information and the msot recent core dump.
- **Cores**—includes all core dumps, versions, and all stack traces.
- **Both**—includes the logs and the core dumps.

This section covers the following:

- **“Creating a System Dump”**
- **“Managing System Dumps”**
- **“Downloading a System Dump”**

Sysdump employs a storage quota that limits the amount of disk space that can be consumed by a sysdump as it is being created; this prevents a rapidly growing sysdump from consuming an excessive amount of storage before the exhaustion of storage is recognized. Essentially, the amount of space that is available for sysdumps that is not used already is divided in half; if a newly created sysdump reaches the size of half the remaining sysdump space, the sysdump is stopped at that point as marked as “partial.”

Creating a System Dump

1. Go to Administration > System Settings: System Operations, then click the System Dumps tab.
2. Select the Log Type from the drop-down list:
 - Logs
 - Cores
 - Both
3. Optionally, type a customer case ID if you have received one from Riverbed support. The case ID will be prepended to the sysdump filename, and will be inserted also in the file metadata so that it will be easy to recognize which customer case the sysdump is associated with.
4. The Include System Metrics option is selected by default, but you can deselect it if you wish. System metrics occupy a majority of the space used by a sysdump, up to 3.5 GB. You can deselect this option if you’re certain that the salient information in the sysdump is not in the system metrics.
5. Click **Generate**. The compressed log file is generated in the background and is listed as pending under Available System Dumps until it is completed.

Managing System Dumps

System dumps that have been started are listed under Available SysDumps. The following information is provided for each dump:

- Created—the date and time the system dump was created.
- Status—The present state of the system dump.
 - Pending indicates that the system dump is in progress in the background.
 - Done indicates that the file is complete and ready for downloading.
- Size—The compressed file size, in bytes.

Downloading a System Dump

1. Go to Administration > System Settings: System Operations, then click the System Dumps tab.
2. With the mouse, hover over the system dump to be downloaded and select the check box to the left of the Created column.
3. Click **Download Selected SysDump**. The compressed folder is downloaded to your local system.

System Health

Click Administration > System Status: System Health to display the System Health page.

The System Health page is a dashboard for three categories of system issue: Product Health, Reboot Status, and System License. For each category and its constituents: Status [color dot indicator]; Time; Reason.

Note that recipients (refer to the “**Recipients**” topic for a description) for system health notifications are configured on the Administration > System Settings: System Health Notifications page; see the “**System Health Notifications**” topic for details.

- Product Health: Each of these issues is a link to the corresponding configuration page:
 - Hardware Health
 - SU Controller Temperature – This indicates that the temperature has exceeded the threshold for safe operation specified by the component manufacturer.

Model	Storage Unit Controller Temperature (degrees C)
SCAN-SU-48TB, SCAN-SU-72TB	100
SCAN-SU-4, SCAN-SU-10	100

- Chassis Health – This indicates the status of the system itself, reflecting the Chassis Availability status on the Storage Configuration > Hardware Status page, and changes if any hardware attached to the system (such as Storage Units) changes in its availability status. This indicator *does not* take into account the overall status of components *within* the system, such as disks or sensors. The overall Health status shown per chassis on the Storage Configuration > Hardware Health page does take those components into account, however.
- Exhaust Air Temperature – This indicates that the temperature has exceeded the threshold for safe operation specified by the component manufacturer.

Model	Exhaust Air Temperature (degrees C)
2170	85
4170, 6170, 8170	80
SCAN-SU-48TB, SCAN-SU-72TB	100
2180	75
4180, 8180	75
SCAN-SU-4, SCAN-SU-10	46

- Intake Air Temperature – This indicates that the temperature has exceeded the threshold for safe operation specified by the component manufacturer.

Model	Intake Air Temperature (degrees C)
2170	50
4170, 6170, 8170	60
SCAN-SU-48TB, SCAN-SU-72TB	33
2180	45
4180, 8180	45
SCAN-SU-4, SCAN-SU-10	no sensor

- CPU Temperature – This indicates that the temperature has exceeded the threshold for safe operation specified by the component manufacturer.
- Disk Health – This indicates the health of each disk in the system, rolling up the worst severity of any disk installed in the system, based on its status as shown on the Hardware Health page, as follows:

Green: OK

Yellow: New or Rebuilding

Orange: Failing

Red: Failed, Missing, or Invalid

- Data Volume Status – This is orange or red if the storage volume provided by a Storage Unit or head unit is failing/rebuilding, or has failed (for example, due to a disk failure or removal).
- Power Supply – This indicates if the power supply is missing, or if firmware has identified an error in the component's behavior.
- System Fan – This indicates if the fan is missing, or if firmware has identified an error in the component's behavior.

■ Software Health

- Flow Export Connection – For an AppResponse system that is connected to a NetProfiler system, this indicates if there is an error in the connection that prevents the exchange of data.
- Time Synchronization – This indicates a problem if NTP or PTP is enabled, and the system has not synchronized to a clock for 60 seconds. (It checks every 30 seconds, and triggers if two consecutive checks show that the clock is not synchronized.)
- WTA Configuration – This indicates the existence of any WTA errors.

■ Traffic Load Health

- Analysis Packet Drops – This indicates problems when the Packet Analysis module is too slow in processing packets that are being captured.
- Capture Job Packet Drops – This indicates packets being dropped because the disks are too slow in writing packets to the packet storage.

- Monitoring Interface Packet Drops – Drops are occurring at the input level because the system is too slow in processing the packets coming from the network card, or there is insufficient buffer space left to copy new incoming packets.
- Reboot Status
- System License
 - Riverbed Framework Feature Key
 - SteelCentral AppResponse 2000v Base Feature Key
 - Application Stream Analysis Feature Key
 - Web Transaction Analysis Feature Key
 - Database Analysis Feature Key
 - Citrix Analysis Feature Key
 - Unified Communications Analysis Feature Key

Storage Status and Usage

Choose Administration > System Status: Hardware/Storage to display the Hardware/Storage page. This page furnishes tabs for viewing the high-level overall status of the chassis, a summary of how available storage is used, and a set of controls for customizing how storage is allocated for different types of data.

This service polls the status of storage devices in the system periodically (every 60 seconds, by default), and reports on chassis status and disk status.

- Chassis Health and Availability
- Disk Status

Note that the web UI header includes a status dot in its header at the upper left that summarizes the system health by its color. This takes into account chassis availability, storage health, and also whether a reboot is needed:

- Green – The most severe value shown for chassis health is either OK or NOTICE.
- Yellow – The most severe value shown for a health value is FAILING.
- Red – This is shown if a health value is FAILED.

Hardware Status

There are two status indicators for the chassis:

- Health – A summary of the health of the chassis itself and the statuses of its disks. This can be OK, NOTICE, FAILING, or FAILED.
- Chassis Availability – The status of the chassis' usability to the system. This status affects the chassis' Health status. The possible chassis availability statuses are:
 - Available – The chassis is usable. The chassis health will be OK.
 - Foreign – The chassis was moved from another system and requires reinitialization before use (not possible for the head unit chassis). The chassis health will be NOTICE.
 - Missing – The chassis was storing data, but could not be found. The chassis health will be FAILED.
 - Invalid – The chassis is an unsupported type. The chassis health will be FAILED.

The chassis serial number and model number are displayed, also.

Disk Status

Every disk belongs to a chassis, and these statuses are considered when determining the chassis health. The possible disk statuses are:

- OK – No problems with the disk. The chassis health will be OK.
- Failed – The disk has stopped functioning. The chassis health will be FAILED.
- Failing – The disk is operational, but may fail soon. The chassis health will be FAILING.

- Rebuilding – The disk is being re-added to a previously degraded array. The chassis health will be NOTICE. During disk array rebuilding, it may take 120 seconds or more for the Rebuilding status to appear when a volume begins rebuilding.
- Missing – The disk was not found on its expected array. The chassis health will be FAILED.
- Invalid – The replacement disk is of an invalid type or size. The chassis health will be FAILED.
- New – The disk has been added or replaced but is not yet part of an array. This is a transient status that you may notice very briefly before the status is updated to one of the other status values. The chassis health will be NOTICE.

Notifications

Status notifications will be sent to Email and/or SNMP trap recipients (defined through the Administration > Other: Recipients page) when chassis status or disk status has changed. Specifically, notifications are sent when:

- Disk transitions from any good status (OK, New, or Rebuilding) to a bad status (Failing, Failed, Missing, or Invalid). This also triggers an alert that's visible in the Alert Events log in the web UI.
- Disk transitions back from a bad status to a good status. In alert terms, the alert has ended.

Notifications can be sent continuously if a bad storage condition persists for some period of time.

The status polling interval is every 60 seconds. It may be up to 120 seconds before a triggered notification is sent.

Syslog messages will be written to log storage change events, regardless of any notification subscriptions that are configured.

Storage Usage

The Storage Usage tab comprises three sections, displaying the amount of storage allocated and consumed by the following data types:

- Capture Data
 - Total Space - The space within the volume that is reserved for packet capture data.
 - Used - The data size of packets that are actually stored.
- Microflow Index
 - Reserved
 - Used
- Trace Files
 - Reserved
 - Used

Storage Configuration

Note that this tab can be accessed directly by choosing Administration > System Settings: Storage Configuration from the menu bar.

The Storage Configuration tab enables you to customize and configure how storage capacity is allocated to different types of data. Your system's storage will be configured to use one of two possible preset modes: Packet Priority Mode or Metrics Priority Mode.

- **Packet Priority Mode** – Packet data priority mode (pktprio) is the default, maximizing packet storage and using a smaller retention time for other data. It is similar to the configuration of the legacy Shark platform.
- **Metrics Priority Mode** – Metrics priority mode (metprio) increases the retention time of analysis modules including aggregates, probe, WTA, DB performance, and VoIP, but reduces the packet storage accordingly. It is similar to the configuration of the legacy AppResponse 9 platform. On the ARX-6000, metprio mode does not allow selection of a storage unit (EXP-300).

Note: Resetting the storage layout will cause all custom settings to be lost.

In each mode, the general behavior of the system is the same, but the location where packet and analysis data is stored changes, and the amount of space allocated for each type of analysis data and for packet data varies. If you have a lot of existing analysis data, the transition from pktprio to metprio could take a long time. The layout configuration process should preserve all analysis data, except that packet capture data on the destination data section will be lost.

Note: Changing the RAID mode of a Storage Unit will result in the loss of any stored data.

The Storage Configuration tab furnishes these controls:

- **Current Storage Layout** – This indicates the storage layout currently in use. This will be “Custom” if you’ve committed any changes to either of the preset modes.
- **Reset to Packet Priority or Metrics Priority** – Click to change to a different storage layout mode. A warning will appear, reminding you that changing the mode will delete all custom settings, and asking you to confirm that you want to change the mode.
- **RAID Configuration controls** – This section furnishes controls for changing or reinitializing each data volume's RAID configuration, and, for SCAN-08180 appliances only, controls for configuring data encryption. For the primary and secondary data volumes, the Mode and Total Size are shown; click the pulldown menu to access the commands available for administering each storage volume.
 - Primary System/Data Volume
 - Secondary Data Volume

For SCAN-08180 appliances only, the Storage Encryption tab provides the following controls for configuring data encryption only on SCAN-SU-10 storage units:

- **Previous Encryption Key** – This represents the existing encryption key, obscured for security. The encryption key is stored only on the RAID controllers; it is not stored in the secure vault or anywhere else on disk.
- **Generate/Remove** – Create a new encryption key or delete the existing encryption key. If you click the Generate button, the generated key will be displayed and auto-filled in the New Encryption Key field. You must subsequently enter the displayed key in the Confirm field manually to set the generated string.
- **New Encryption Key** – Type the new encryption key to use. Encryption keys must obey these rules:
 - Must be at least 8 characters long, and no more than 32 characters

- Must include at least one uppercase letter (A-Z)
- Must include at least one lowercase letter (a-z)
- Must include at least one digit (0-9)
- Must include at least one special character, from the set:
!"#\$%&'()*+,-./:;<>?@[\\]^_`{|}~
Note that the the space character and the "=" (equal sign) are not permitted in encryption keys.
- New Encryption Key (Confirm) – Type the new encryption key again, to confirm that it's the correct key you want to set.
- Encrypt All Storage Units – Checking or unchecking this box automatically triggers all Storage Unit RAID mode dropdown menus to change to Reinitialize in their current modes. You cannot reset these dropdowns to the current (non-reinitializing) RAID mode item; reinitialization of all supported devices is required if the state of encryption is changed.
The encryption settings are applied only after you click Commit to submit the storage configuration, causing all Storage Units to be reinitialized.
- Data/Space Allocation controls: For each supported data type, values are displayed for Total Space and Total Used:
 - System Data – This allocation is not user-configurable.
 - Packet Traces (PCAP)
 - Packet Microflow Indexes
 - Capture Jobs – Note that all of the space that is allocated for capture jobs is reserved for that purpose, even if the amount of that space that is actually consumed by stored packets is less. The Total Used value that is shown for capture jobs indicates the size of a buffer that is created for packets to be written into when they are captured. To see the data size of packets that are actually stored, click the Storage Usage tab and read the numbers in the Capture Data section.

Note: If capture storage is enabled, it must be at least 51200 MiB (~50GB) for hardware appliances, or at least 16000 MiB (~16GB) for virtual systems.

- DBA Aggregates
- ASA/UCA/WTa/CXA Aggregates
- Transaction Data
- Data Section: Total Size & Allocation bar chart
- Primary System/Data Volume
- Secondary Data Volume

For each volume, you can click the pencil icon at the right end of the bar chart to display the Data Volume Allocation dialog, which enables you to customize the storage space allocated to Packet Traces, Packet Microflow Indexes, DBA Aggregates, and ASA/UCA/WTa/CXA Aggregates. Note that changing any of these allocations trades a corresponding amount of space (increase or decrease) with that allocated for Transaction Data.

- Transaction Storage controls – For each transaction data type, select from the Assign To pulldown menu the volume on which that data will reside (either Primary System or Secondary Data Volume). Also for each transaction data type, the current retention time and maximum estimated retention time are displayed. In addition, for each transaction data type, you can configure the Desired Minimum Retention Time (in days), as well as the Maximum Retention Time (in days). Note that these values are configured as *retention times*, rather than as storage sizes.
- Data Section – This summarizes the configured transaction data assignments for each storage volume, including the total amount of transaction data, as well as the transaction data types assigned to that volume.
- Uncommitted Changes controls – This section summarizes the changes you’ve made to the storage configuration, and furnishes controls for reverting to the last saved storage configuration.

The undo history enables you to select a step in the change history and roll back the configuration to that step.

Click the Revert To button if you want to return to the last saved storage configuration.

Click the Commit Changes button to finalize the current set of changes and make them take effect. Note that this could take a long time to complete, so make certain to review the change summary and determine that the configuration is correct before committing. The system will prompt you for confirmation before executing the commit.

Software Update

Software updates to AppResponse 11 can be installed using the Software Update tab in the web UI, or, if SteelCentral Portal is being used to manage multiple AppResponse 11 systems, from the Portal. A single update image can be used to update AppResponse 11 from one or more earlier versions. Check the release notes and the Riverbed Support site for more information on update paths for earlier versions.

Note: An update to an *earlier* software version cannot be installed. Databases are modified during the update process, preventing a reversion to a previous release.

Note: The Remote Software Update feature in SteelCentral Portal supports only the updating of AppResponse 11 systems running AppResponse Version 11.5.0 and later. Refer to the *SteelCentral Portal User Guide* or online help for instructions for updating AppResponse 11 software from the Portal.

The update process requires:

- a user signed in with System configuration read/write permission in one or more roles.
- an update image uploaded from your local file system or fetched from a remote source.
- a successful system check that the uploaded or fetched update image is valid and that adequate system resources, for example, storage, are available.
- other signed-in users of AppResponse 11 are automatically signed out when an update starts. Users can sign in again once the update is completed and AppResponse 11 has booted.

Updating AppResponse 11 Software

Update images are available as an ISO file. The term “Update ISO File” means an update image in ISO format.

Follow the steps below:

1. Go to Administration > System Settings: System Operations, then click the Software Update tab to display the update controls.
2. Select an update source, either:
 - **Upload new Update ISO File**—Select this radio button and click **Browse** to select an update ISO file in the local file system. The selected update image is loaded by AppResponse 11.
 - **Remote File URL**—Select this radio button and enter the path to an update image on a web server, then click **Fetch** to load the update image for installation on AppResponse 11.
3. Monitor the update image loading status, displayed in State under Update Information. When the status is Initialized, review the State Description, Current Version and Target Version.
4. Click **Install** to load the new software or click **Revert** to uninitialize the update.
5. Check the status displayed in State under Update Information. to determine the success of the update. For more information see [“Update Information”](#) below.

Update Information

The following information is made available:

- **State**—Indicates whether an update image is loaded and ready for installation. The state can be any of the following: Fetching, Initializing, Initialized, Failed Graceful, or Failed Critical.
 - If the state is Failed Graceful, click **Revert** to uninitialize the update.
 - If the state is Failed Critical, contact Riverbed customer support for assistance.
- **State Description**—Information is provided here only when an update is being installed.
- **Current Version**—The software version of AppResponse 11 currently installed.
- **Target Version**—The software version of the update image about to be installed.

Update Source

You can select an update image on your local file system or fetch an update image from a remote web server.

- **Upload new Update ISO File**—Select this radio button to specify an update ISO file residing on the local file system.
 - **Browse...**: Click to explore the local file system and select an update image residing there. The selected file is automatically loaded by AppResponse 11.
- **Remote File URL**—Select this radio button and enter the URL identifying an update image residing on a web server. Click **Fetch** to load the update image for installation.

Reboot/Shutdown

Important: AppResponse 11 should always be shut down gracefully. Shutting down the appliance using the power switch may result in data loss.

Use this tab to gracefully reboot or shutdown an AppResponse 11 appliance or virtual-edition. Only a user signed in with System configuration read/write permission in one or more roles can reboot or shutdown AppResponse 11.

This section covers the following:

- “Rebooting AppResponse 11”
- “Shutting Down AppResponse 11”

Rebooting AppResponse 11

A reboot restarts an appliance or virtual machine. Users are signed out and must sign in after AppResponse 11 restarts. The reboot process can take several minutes to complete.

To reboot AppResponse 11:

1. Go to Administration > System Settings: System Operations, then click the Reboot/Shutdown tab.
2. Click **Reboot** to begin the reboot process.
3. In the Reboot window, Click **OK** to continue or **Cancel** to stop the reboot process.
4. A Rebooting message appears when the reboot begins.
5. Once a reboot completes you are directed to the sign in page.

Shutting Down AppResponse 11

A shutdown gracefully halts AppResponse 11 and powers off an appliance or virtual machine. To restart AppResponse 11, you must manually turn on the appliance or virtual machine.

To shutdown AppResponse 11:

1. Go to Administration > System Settings: System Operations, then click the Reboot/Shutdown tab.
2. Click **Shutdown** to begin the shutdown process.
3. In the Shutdown window, Click **OK** to continue or **Cancel** to stop the shutdown process.
4. A Shutting down message appears when the shutdown begins.
5. Click **x** in the upper-right corner of the message to close it.
6. Once the shutdown completes you must manually turn on the appliance or virtual machine.

Backup and Restore

Clicking Administration > System Settings: Backup and Restore displays the Backup and Restore page for saving an AppResponse system's configuration and performance data and uploading it to a separate host (a predefined backup server) for safekeeping. A backed up configuration can be restored later to write it to a new system. This capability is provided in case it is necessary to replace an AppResponse system; it is not intended as a means of cloning a configuration rapidly to deploy new systems.

Note: The AppResponse 11 software version and the appliance model must match exactly when performing a restore operation.

For local backups, each backup is created as a .tgz (G-zipped TAR) file; for backing up to a remote server, each backup is created as a separate directory containing the corresponding files. The backup operation can include configuration data and traffic data:

■ Configuration Data

This includes all parameters necessary to configure the system, as well as all database tables relevant for configuring (or reconfiguring) it. Most configuration information is backed up, although some is omitted for security reasons, or due to issues caused by not backing up data. Backups are not encrypted, so nothing that is a potential security risk is backed up.

- All settings under Administration > General are backed up, with the exception of the web certificate and the Syslog certificate. Upon reboot after a restore, the system will create a new self-signed web certificate.
- User accounts and passwords are backed up and restored, stored in one-way hash format.
- Sensitive configuration such as SSL certificates/keys is not backed up, and will be reset to defaults upon a restore operation. This includes the default SSL certificate used when logging into the web UI; your browser will complain about a self-signed certificate after a restore operation. The SSL certificate for encrypted syslog recipients is not backed up.
- The SSH key for the backup server is not backed up. It will be preserved during a restore operation when possible, but you should verify this.
- Licenses will be left untouched, neither backed up nor deleted. Licenses belong to each individual system and are essential to its operation. Licenses are non-transferable to other hardware-based AppResponse 11 appliances. Virtual AppResponse 11 systems (Cloud AWS, Cloud Azure, and ESXi) can have their licenses transferred, but they must be deactivated on the original system first.

■ Traffic Data

This includes performance data and system metrics with performance data. You can specify the data type (CXA, DBA, VOIP, and WTA), as well as the granularity of the aggregated data to be backed up.

Note that packets, saved reports, and transactions are not backed up.

All backup activity is logged in audit trails.

Backup/Restore Workflow Overview

In general, the backup and restore procedure follows this sequence; refer to the individual sections that follow for details about each action:

1. Define a backup server. You can specify multiple backup servers with different paths, protocols, and security settings on the same host machine.
2. Define a backup operation (either on demand or scheduled).
3. Restore an existing backup to a target AppResponse system running the exact same software build. The target system will reboot, and come back up running the restored configuration. Licenses will remain untouched.

Note: On each AppResponse system, verify that the AppResponse user account has write privilege on the system. (Write privilege is required to perform a recovery.)

Backup/Restore Page and Operations

Clicking Administration > System Settings: Backup and Restore displays the Backup and Restore page. The page comprises four tabs, corresponding to four relevant operations:

- On Demand Backup – Define a backup operation to begin immediately. This includes selecting the backup server and specifying the data to be backed up.
- Scheduled Backups – Define a backup operation to run at regular time intervals. This includes selecting the backup server, specifying the data to be backed up, and configuring the recurrence schedule.
- Restore – Transfer and restore data from a remote location. Alternatively, restore a backup stored locally.
- Backup Servers – Specify and manage one or more servers used to store backup data. You need to have a backup server defined in order to back up performance data..

Define a Backup Server

You need to have a backup server defined in order to back up performance data. The backup server must support SSH and SFTP. Use of a UNIX or Linux-based server is recommended.

On each backup server, verify that:

- SSH and SFTP are installed and configured. The "cat" binary must be available, also.
- The user account for the backup server has access to the backup directory with read, write, delete, and execute privileges.
- The user account associated with the backup has sufficient disk space allocated to it on the backup server for the planned backups.

Note: The Backup and Restore functionality includes minimal file management to ensure that scheduled backups do not grow unbounded, but, the user is responsible for ensuring that backups are managed correctly on the backup server.

To define a backup server:

1. Click the Backup Servers tab.
2. Click Add to display the New Backup Server dialog.

3. Specify the details for the backup server you are adding: a meaningful name, an informative description, the hostname, the SSH port, the path to the file system destination, and the user account ID. Each backup is written to its own directory under the specified path, and you should make certain to write backups from separate AppResponse 11 systems to separate directories, also. This will facilitate better performance when finding backups to be restored.
4. Enter (copy and paste) a private key in the field provided, or click the Apply button to have one generated for you. If you have a private key generated for you, the Generated Keys dialog will appear, showing the public and private keys. For security purposes, the private key is exposed only at generation time. If you plan to re-use this key, make sure to save the private and public keys before you click OK.
5. The backup server is defined, and appears in the Backup Servers list for use in subsequent backup and restore operations.

Note: A backup server cannot be deleted if it is associated with a scheduled backup. If you want to delete a backup server, you must first delete all scheduled backups that use it.

Back Up on Demand

To execute a backup on demand:

1. Click the On Demand Backup tab.
2. Type a name for the backup operation, along with an informative description.
3. Choose the backup server to use. This can be the AppResponse system's local file system, if you are backing up only configuration data, or you can choose a predefined backup server.
4. Specify the content to be backed up; this can be the configuration only, or it can be the configuration plus currently available network data. If you choose Configuration plus data, all data modules are selected by default; deselect any that you do not want to back up. In addition, check that the minimum granularity for aggregated data is acceptable; this defaults to 1 minute. This is the *smallest* grain of time that will be included in the backup, so, whatever you specify as the minimum, all *larger* granularities will be backed up, as well. Choosing 1-Min as the minimum granularity means that all granularities are backed up; choosing 5-Min means that all granularities *except* 1-Min will be backed up, and so on. Note that the Backup Size Estimates will change according to the data you choose to back up, and its granularity.
5. Click Create Backup to execute the backup immediately. Click Cancel Backup if you need to quit the backup process for any reason.

Note: It is also possible to select a scheduled backup and execute it immediately.

Note: Concurrent backups are not supported; a single backup can run at any one time.

Schedule A Backup For Another Time

To schedule a backup for another time:

1. Click the Scheduled Backups tab.

2. Click Add to display the Create New Schedule dialog.
3. Type a name for the backup operation, along with an informative description.
4. Choose a predefined backup server from the pulldown menu.
5. The new backup is enabled by default. You can also select the option to execute the backup each time the configuration is saved; use this with caution, as the backup operation needs time to execute, according to how much data it backs up.
6. Click Next to advance to the Content tab.
7. Specify the content to be backed up; this can be the configuration only, or it can be the configuration plus currently available network data. If you choose Configuration plus data, all data modules are selected by default; deselect any that you do not want to back up. In addition, make sure to specify a minimum granularity for aggregated data; this defaults to 1 minute. This is the *smallest* grain of time that will be included in the backup, so, whatever you specify as the minimum, all *larger* granularities will be backed up, as well. Choosing 1-Min (the default) as the minimum granularity means that all granularities are backed up; choosing 5-Min means that all granularities *except* 1-Min will be backed up, and so on. Note that the Backup Size Estimates will change according to the data you choose to back up, and its granularity.
8. Click Next to advance to the Recurrence tab.
9. Specify the interval at which the backup operation will execute. Note the options for setting the overall rate of recurrence (Once, Daily, Weekly, etc.), as well as the options for fine tuning the interval, including start and end times. Note also the options for configuring retries, and the number of old backups to keep.
10. Click Finish to complete the backup definition. The backup will execute according to the schedule you defined.

Restore Previously Backed Up Data

Note: The AppResponse 11 software version and the appliance model number must match exactly when performing a restore operation. The hardware configuration, such as the number of Storage Units and the size of the hard drives, should match, also. When restoring to a hardware appliance with a freshly replaced hard disk, you must make sure that the newly added disk is properly initialized, or the restore process will fail.

Note: For virtual AppResponse 11 systems (Cloud AWS, Cloud Azure, and ESXi), the target volume must be at least as large as that of the original volume. The restore process will not proceed if the capture disk of the VM has not been reinitialized (in a valid state). This is because the restore process cannot tell the size of the capture disk unless it has been initialized first.

When restoring a large amount of performance data, the restore process can take hours. The information provided in the Report Progress screen provides a good approximation of how far the restore process has progressed. Be prepared to allow the process a period of time to run to completion, and monitor it occasionally to see if it has finished.

To restore previously backed up data from a backup server:

1. Click the Restore tab.
2. Choose a backup server and click Find Backups. This will show the existing backups stored on that server. By default, the filter restricting the backups to those created by the current AppResponse 11 system is selected. If you want to see all available backups, deselect the option and click Find Backups.
3. Select a backup to perform an operation with it. You can restore the backed up data to the current system, or, for local backups, you can download the backup to the current system's file system without actually loading it, upload the backup to a new specified destination, or delete the backup completely.

The Restore Process

The Restore process executes in this order:

1. The restore process starts when you select a backup and initiate a restore action.
2. The initialization phase of the restore process starts.
3. The system reboots upon completion of the initialization phase.
4. The system resets to factory defaults (see the section that follows for more information).
5. The configuration portion of the backup is restored.
6. If performance data needs to be restored, the system enters a "restore mode," and the performance data is transported and restored.
This phase of the restore process can take a significant amount of time to complete, possibly hours. While in "restore mode," the system becomes largely unavailable and the only functionality available is the Restore Progress screen that reports the list of tasks completed as the restore action progresses.
7. The system becomes fully functional again upon completion of the restoration of the performance data.

Implicit Reset to Factory Defaults During Restore Operation

When a restore operation is initiated from the web UI, the AppResponse 11 system is reset to its factory default state prior to the restoration of the backed up configuration information. This is achieved by the implicit execution of the CLI command, `system reset-factory`. This command is accessible only in the CLI, and it deletes all configuration, data, and logs from the AppResponse 11 system and resets it to the state it was in when it was powered on the very first time. The command does not perform a full disk wipe or affect the AppResponse 11 software itself; the installed version and any patches will not be touched.

Note: Licenses are not affected by the `system reset-factory` command.

Hard Drive Encryption When Restoring to SCAN-08180

For SCAN-08180 appliances with SCAN-SU-10 Storage Units only: During the *restore* operation, you can encrypt the data. (Data is always backed up *unencrypted*.) To encrypt your data at restore time, click the Encrypt Data option. To make the Encrypt Data option available, make sure that an encryption key is properly configured (Administration > System Settings: Storage Configuration, Storage Encryption tab). If the Encrypt Data option is not present or not selected, the data will be written back to the system unencrypted.

Transferring Licenses For RMA Situations

AppResponse hardware appliances always get their perpetual licenses from the public Riverbed license server. These licenses are not transferred if and when the appliances are RMA'd.

Virtual AppResponse 11 systems (Cloud AWS, Cloud Azure, and ESXi) can have their licenses transferred, but they must be deactivated on the original system first, and must be re-activated on the new system (before or after the restore process completes).

The overall process for transferring the licenses between virtual AppResponse 11 systems is:

1. Perform the backup.
2. Deactivate the old license.
3. Replace/reinstall the virtual system.
4. Re-activate the license on the new/re-installed virtual system.
5. Perform the restore operation.

If you no longer have access to the original virtual system (and its deactivation key), contact Riverbed customer support for assistance.

Definitions

Host Group Configuration

Devices on the monitored network are tracked individually. However, for reporting and alerting it is often convenient to track similar devices as a group. For example, the traffic statistics for all hosts in the same geographical location can be aggregated and reported as one host group. Similarly, all web servers or all database servers can be tracked as a host group.

A host group can contain individual members and one or more other host groups. The Navigator and Insights features can report selected performance metrics for host groups. Network usage policies can be defined for host groups and alerts sent when the policies are violated.

A host group is defined by the IP addresses of its members. AppResponse 11 is shipped with four default host groups: one for each of the three blocks of reserved IP addresses and one for all public IP addresses.

Recommended Practices When Using Host Groups

Take care to observe these considerations when defining and using Host Groups:

- **Limit the Total Number of Host Groups to No More Than 1500 per System**
AppResponse 11 was designed for deployments that accommodate up to 1500 Host Groups. The user interface will not prevent you from defining more than 1500, but more than 1500 is not supported, and can cause significant performance issues.
- **Limit the Number of Host Group Members to No More Than 100**
To avoid an excessive load on the system, minimize the number of comma-separated items in the Members field when you define each Host Group. When the system calculates metrics in real time, it checks monitored packets against each comma-separated item (IP address, IP range, or IP subnet) in each Host Group definition. A complex Host Group definition that includes a long list of members can increase computation loads and affect monitoring performance on the system.

To keep your Host Group definitions as simple as possible, it is recommended practice to:

- Include no more than 100 comma-separated entries in any Host Group definition.
- Specify IP address ranges, rather than individual IP addresses, whenever possible.
- **Expect Some Delay When Drilling Down In an Aggregated Host Group**
AppResponse 11 supports Host Group aggregation up to three levels: parent > child > grandchild. A Host Group is a union of all its member Host Groups and all the IP addresses in those Host Groups. You may observe a visible delay in the updating of the user interface when you drill down from a Host Group to IP addresses or IP conversations.

Defining Host Groups

To define an additional host group

1. Go to the Definitions > Host Groups page.
2. Choose Add to open the New Host Group page.
3. Enter the name and description as you want them to appear throughout the product.
4. Select the Active check box if you want to start collecting and reporting data for the group as soon as you add it.
5. Specify the Inbound and Outbound bandwidth you want to allocate to the host group. This is typically the full capacity of the links. However, it can be less than that.

The Insights feature reports the percent utilization of the bandwidth you specify here.

- If the full bandwidth of an Inbound or Outbound link is dedicated to this host group, you can specify the full link capacity and AppResponse 11 will report the percentage of the full link capacity that this host group is consuming.
 - If you want to allocate only a portion of the link capacity to this host group, you can specify an amount that is less than the full link capacity. AppResponse 11 will report the percent utilization of the amount you allocated. Note that if the host group consumes more bandwidth than you allocated, the percent utilization value will exceed 100%.
6. Specify the IP addresses of the members. The following formats are accepted:
 - Individual IP addresses.
 - Comma-separated list of individual IP addresses.
 - Address ranges specified as the first address and last address of the range separated by a dash. Do not include spaces. For example, 10.0.0.0 – 10.0.0.100
 - If an IPv6 range such as ::1 – ::ffff:ffff:ffff is added, it will include all IPv4 addresses. Embedded IPv4 addresses such as ::ffff:a0a:a0a are treated as IPv4 addresses by AR11, i.e., 10.10.10.10. The IPv4 embedded addresses are in the range ::ffff:0:0 – ::ffff:ffff:ffff.
 - For IPv4 only, address ranges using full CIDR format are supported. For example, 10.0.0.0/8 is supported, but 10/8 is not supported.

Press Tab or Enter to move to the next entry.

7. If the host group you are defining is to include members of another host group that has already been defined, choose the plus sign (+) beneath the Member Host Groups field. This opens a list in which you can select host groups to add. If the list is long, you can search on the name of the host group you want to add.
8. Choose OK to add the host group(s) and return to the New Host Group page.
9. If you need to delete a host group you added, select the host group in the Member Host Groups section and choose the minus (-) icon below the text field.

10. Choose Save.

The new group is included in the list. Note that if you added an existing host group as a member of your new host group, that existing host group is now listed under your new host group. It no longer appears at the first level of the list. Expand your new host group in the list if you want to view or edit the host group that it now contains.

Importing Business Groups from an Upgraded AppResponse 9.6.x Appliance

Customers using a 2200, 3300, 3800, 4300, 5100, or 6000 appliance can choose to export business groups (BGs) and import them into AppResponse 11 when they upgrade their software. For information on exporting business groups, see the AppResponse 9.6.2 release notes.

All BGs and BG containers can be imported and merged with AppResponse 11.1.0 and later host groups.

Important: Autonomous System (AS) numbers are not supported and they should be removed from an exported .csv file before it is imported by AppResponse 11.1.0.

Importing 9.6.x Exported Business Groups

1. Go to Definitions > Host Groups in the AppResponse 11 web UI.
2. Click **Import** in the top-right corner of the page header.
3. Specify or choose the name of the exported .csv file in the window that opens, for example, AR9-BG-Export.csv.
4. Business groups are imported as follows:
 - Corrupted business group definitions in an exported .csv file generate errors. These definitions must be fixed before the .csv export file can be imported.
 - If a business group has the same name as a host group, a warning is displayed that the host group exists and its definition will be overridden. Click **Proceed** to continue or close the window and revise the export .csv file.
 - AppResponse 11 host groups do not support IPv6 CIDR blocks. Convert IPv6 CIDR blocks to IPv6 ranges before importing a .csv file.

Editing a Host Group

To edit a host group

1. Go to the Definitions > Host Groups page.
2. Hover your mouse over the row that lists the host group. This displays the edit (pencil) and delete (x) icons.

3. Choose the edit icon to open the Edit Host Group page.
4. After you make your changes, choose either Apply to save and exit or Revert to return to the previous settings.

To delete an individual host group, hover your mouse over the entry for the host group and choose the delete (x) icon.

To delete multiple host groups, select the check boxes at the beginning of the rows listing the host groups and the choose Delete near the top of the table.

Exporting and Importing Host Groups

Host group definitions can be exported to a CSV (comma separated value) file, a format used by many spreadsheet applications, edited in the CSV file, and subsequently imported back in to AppResponse 11. This provides a convenient mechanism for editing a large number of host group definitions in a short amount of time.

The Host Group CSV file provides the existing host group definitions with the following fields:

- Version [AR11]
- Data Type [Hostgroups]
- Timestamp
- Name
- Description
- Enabled
- Bandwidth In
- Bandwidth Out
- Hosts
- Member Hostgroups

The Import and Export controls are located at the upper right of the Host Group Configuration page.

To export host group definitions to CSV file:

1. Go to the Definitions > Host Groups page.
2. Click Export at the upper right of the Host Group Configuration page. The host group table is written to CSV file immediately; the default file name is “hostgroupsAR11.csv”.
3. Double-click the CSV file to open it in your default spreadsheet application, or drag the file to a folder to edit it at a later time.

To import host group definitions from CSV file:

1. Go to the Definitions > Host Groups page.

2. Click Import at the upper right of the Host Group Configuration page. A dialog box appears; type the name of the CSV file you want to import, or click Choose File to browse the file system and select it. Click Import to execute the process, and the contents of the file are read in to the host group table.

Application Configuration

AppResponse 11 identifies applications that are communicating over the monitored network by matching traffic attributes against application definitions. If the traffic attributes match your definition of an application, then AppResponse 11 collects and reports traffic statistics and performance metrics for the application. For more details, see [“Traffic Matching Mode” on page 133](#) below.

You can create the following types of definitions for applications:

- **“General”** - combinations of ports, protocols, server IP addresses and automatically recognized applications.
- **“URL”** - one or more URLs or patterns occurring in URLs.
- **“Web”** - one or more combinations of:
 - URLs or patterns occurring in URLs
 - Values of web page content
 - Values of web page properties
- **“Auto-recognized”** - pre-configured application definitions. The product is shipped with a large library of definitions for common applications. It recognizes traffic from these applications automatically. These definitions can also be included as parts of General definitions.

Choosing Definitions > Applications displays the Application Configuration page, which includes a separate tab for each of these approaches to specifying application definitions. Additionally, it reports the number of General and URL applications for which high priority definitions have been enabled (up to 600) and the number of Advanced Web App for which definitions have been enabled (up to 300).

Note: When a set of application definitions has been selected in the Portal Integration page to be managed solely from SteelCentral Portal, the relevant fields will be visible in the Edit dialog, but will be read-only.

Importing Applications from an Upgraded AppResponse 9.6.x Appliance

Customers using a 2200, 3300, or 3800 appliance or a VMon or v2000 virtual appliance can choose to export applications and import them into AppResponse 11.1.0 (or later) when they upgrade their software. For information on exporting applications, see the AppResponse 9.6.2 release notes.

Important: Corrupted application definitions in an exported .csv file generate errors. These definitions must be fixed before the .csv export file can be imported.

Importing 9.6.x Exported Applications

1. Choose Definitions > Applications to open the Application Configuration page in the AppResponse 11 web UI.
2. Click **Import** in the top-right corner of the page header.
3. Specify or choose the name of the exported .csv file in the window that opens, for example, AR9-App-Export.csv.

4. General and server applications are imported as follows:

- URL applications are imported as Advanced Web applications, not URL applications. The server information for the URL applications is preserved in the import.
- Applications are imported as High Priority applications. AppResponse 11 supports up to 600 High Priority applications. If you have more than 600 applications, create two .csv files, one (FILE A.csv) with no more than 600 High Priority applications, the second (FILE B.csv) with the remaining applications. Import FILE B.csv first and then edit the applications to change each to Medium or Low Priority applications. Next, import FILE A.csv.
- AppResponse 11 application names are case-sensitive and must be unique. The names of the imported AppResponse 9.6.x applications cannot duplicate the name of existing AppResponse 11 applications. An error message with the list of duplicate names is displayed when duplicates are found during an import. Those application names must be changed in the .csv file before they can be imported.

Conflicts with AppResponse 11 Auto-Recognized applications may occur. For example, these default applications in AppResponse 9.6.x will have conflicting names during import: DNS, HTTP, ICMP, IMAP, POP3, RTCP, SMTP, and SSH. These applications can be imported by changing their names to all lowercase in the .csv file.

- When imported, an AppResponse 9.6.x Auto-Recognized application is replaced by the corresponding AppResponse 11 Auto-Recognized application.

Traffic Matching Mode

To ensure that the most useful and relevant traffic data is retained, AppResponse 11 applies a set of criteria to select the top network elements, such as applications, IP conversations, and web pages, for each time window. Detailed metric data is only kept for these top elements. However, AppResponse 11 calculates total traffic, throughput, and utilization metrics based on ALL the traffic seen. Priority, high to low, is used to determine what traffic has detailed metrics retained.

Note: Traffic that is matched to URL applications is never matched to any other application type. As a result, any enabled URL application definition always has a Traffic Matching Mode of High Priority. This priority cannot be changed.

The matching process follows these steps:

1. High Priority Traffic Matching Mode

- General applications can be any combination of user-supplied ports, protocols, server IP addresses, and Auto-Recognized applications.
- High Priority applications are matched to all incoming traffic. If traffic, for example, an individual TCP connection, matches more than one General application *it contributes metrics to all those applications*.
- Performance data that ASA records for these applications are not affected by topping, that is, metrics for all General applications with high priority that were seen in a minute are recorded in the AppResponse 11 performance database.

2. Medium Priority Traffic Matching Mode

- These General applications also can be any combination of user-supplied ports, protocols, server IP addresses, and Auto-Recognized applications.
- These medium priority applications are matched to all incoming traffic. If traffic matches more than one General application with this priority setting it contributes metrics to all those applications.
- Performance data that ASA recorded could be affected by topping - this is why this is a lower priority than High.

3. Unmatched Traffic Priority

Traffic that doesn't match any application definitions in steps 1) and 2) is matched to Auto-Recognized applications that were not matched in steps 1) and 2). If the traffic matches more than one previously unmatched Auto-Recognized application, it contributes metrics to all those applications. Performance data that ASA recorded could be affected by topping.

4. Low Priority Traffic Matching Mode

- Users also can create General applications with Traffic Matching Mode set to Low Priority. AppResponse 11 prevents these General applications from using any Auto-Recognized application definitions. Instead, these General applications only use combinations of user-supplied port, protocols and server IP addresses.
- These applications will be matched against traffic that did not match any applications in steps 1), 2), and 3) above. These could be considered user-defined applications.
- Performance data that ASA recorded could be affected by topping.

5. Final matching

- Traffic that did not match any applications in steps 1) through 4) above is matched against Port Alias definitions. A user can modify port alias definitions or create new definitions of their own at Definitions > Port Aliases. Performance data that ASA recorded could be affected by topping.

General

On the General tab you can add an application to be tracked and then add one or more definitions for that application. If monitored traffic matches any one of the definitions, it is recognized as belonging to the application.

On the General tab you can:

- define an application more narrowly or more broadly than it is defined in the library of applications listed on the Auto-recognized tab.
- define an application that is not included in the library of applications listed on the Auto-recognized tab.
- enable or disable recognition of an application.
- change the matching mode for checking traffic against application definitions.
- edit or delete an existing application definition on the General tab. (This does not change any application definition in the library of auto-recognized applications.)

To specify application definitions in terms of ports, protocols, server IP addresses and auto-recognized applications

1. Choose Definitions > Applications to open the Application Configuration page. Click the General tab and choose Add.
2. Enter the name and description of the application as you want it to appear throughout the product.
3. Select Enabled to have AppResponse 11 start monitoring for the traffic as soon as you save your definition.
4. If you want auto-recognized apps to collect metric data separately, click the Collect Auto-Recognized Application data separately checkbox. Enabling this option allows included auto-recognized apps to calculate metric data. By default, metrics are not calculated for an auto-recognized app if that app was used in a General app definition.
5. Select the traffic matching mode you want to use for the application.

High and medium priority matching take precedence over matching the definitions in the library for auto-recognized applications. Low priority matching is used only if no definition in the library of auto-recognized applications has been found to match.

The product saves all statistics for applications configured for high priority matching. It saves statistics for applications set to medium and low priority matching modes if storage capacity is available. If storage capacity is limited, statistics for medium and low priority applications are saved for only the applications with the top traffic volumes. However, all traffic that matches any definition is included in computing performance metrics and reporting total traffic volumes.

6. Choose Add to open the new definition window.
7. Enter the values you want to include or else select them from the drop-down menus where they are provided.

The definition is the logical AND of all the elements you specify. That is, the traffic must meet all the criteria you specify in this definition in order to be recognized as belonging to the application. You can specify the definition entirely in terms of ports and protocols, or you can choose an auto-recognized application definition and restrict it to specified server IP addresses.

Note that auto-recognized applications cannot be used as part of Low priority matching criteria. This is because auto-recognized application definitions take precedence over Low priority definitions.

8. Click Save to save the definition and return to the New General Application window. The new definition is listed.
9. Choose Add again if you want to create another definition for the application. You can add many individual definitions. The product uses the logical OR of all the definitions you specify. That is, traffic that matches any one of the definitions is tagged as belonging to the application.
10. Click Save to save the definition and return to the New General Application window. The new definition is listed.

11. When you finish adding definitions for the application, choose Save on the New General Application page to return to the General tab. The new application is added to the list of applications on the General tab.

To delete an application from the General tab, either

- Hover your mouse over the entry for the definition and choose the delete (x) icon, or
- select one or more entries from the list of applications and choose Delete at the top of the table.

URL

The URL tab enables you to define application traffic in terms of one or more URLs or patterns occurring in URLs. If a page object matches any of the URLs or URL patterns, then the traffic containing that page object is tracked and reported as belonging to the application.

The traffic matching mode is always High for URL-based application definitions. A URL-based definition takes precedence over any definition in the library of auto-recognized applications. The product saves all statistics for application traffic that matches a URL-based definition.

To define an application in terms of URLs or patterns occurring in URLs

1. Choose Definitions > Applications to open the Application Configuration page. Click the URL tab and choose Add.
2. Enter the name and description of the application as you want it to appear throughout the product.
3. Select Enabled to have AppResponse 11 start monitoring for the traffic as soon as you save your definition.
4. Enter one or more URLs or patterns occurring in URLs. Press Enter after each entry.
If a page object matches any of the URLs or URL patterns, then the traffic containing that page object is tracked and reported as belonging to the application. You can include only a single wildcard character (“*”) in each entry.
5. Choose Save. The definition is saved and the application is added to the list of applications on the URL tab.

To delete an application from the URL tab, either

- Hover your mouse over the entry for the definition and choose the delete (x) icon, or
- select one or more entries from the list of applications and choose Delete at the top of the table.

Web

The Web tab enables you to track application traffic using highly specific matching criteria. You can define an application in terms of:

- URLs or patterns occurring in URLs

- Values of web page content
- Values of web page properties

The traffic matching mode is always High for application definitions on the Web tab. A Web definition takes precedence over any definition in the library of auto-recognized applications. The product saves all statistics for application traffic that matches a Web definition.

To define an application on the Advanced Web tab

1. Choose Definitions > Applications to open the Application Configuration page. Click the Web tab and choose Add.
2. Enter the name and description of the application as you want it to appear throughout the product.
3. Specify a Slow Page Threshold of 1 to 600 seconds.
If a web page matching this criteria does not load within the time you specify here, it is considered to be a slow page. AppResponse 11 can be configured to alert on slow pages.
4. Select Enabled to have AppResponse 11 start monitoring for the traffic as soon as you save your definition.
5. Specify any or all of the following page match criteria:
 - URL Patterns - limit the match to patterns in the URL of the “MAIN” object (that is, the page, such as www.riverbed.com). If monitored traffic matches this specification, then the product tracks traffic for not only this page, but also any objects the page includes. Note that those objects could be referenced by URLs that do not include the URL patterns you specify in this section.
 - Content Values - limit the match to web page specifications containing specific content values. Refer to the “[Content Values Page Match Criteria](#)” section for descriptions and examples of content value specifications.
 - Advanced - limit the match to web page specifications containing combinations of URL patterns, web page content or web page properties. Refer to the “[Advanced Page Match Criteria](#)” section for descriptions and examples.
6. Choose Save. The definition is saved and the application is added to the list of applications on the Advanced Web App tab.

To delete an application from the Advanced Web App tab, either

- Hover your mouse over the entry for the definition and choose the delete (x) icon, or
- select one or more entries from the list of applications and choose Delete at the top of the table.

Note: A deleted Web App is displayed as *Unnamed: <xxxx>* instead of *Not Available* as was done in earlier versions of AppResponse.

Content Values Page Match Criteria

The Content Values options in the Page Match Criteria section enable you to narrow the page match criteria to specific values being present or absent. The matching criteria for each type of page content can be set to equal or not equal patterns seen in the monitored traffic.

To specify web page content values

1. Expand the Content Values option in the Page Match Criteria section of the New Advanced Application page.
2. Select the format and location of the data.
3. Enter the name and value of the data to be matched. Refer to the examples below.
4. Specify whether all content values must match or if the traffic should be tracked if any of the content values match.
5. Choose Add to specify additional content values. Use the delete icon (x) at the end of the entry if you want to delete a content specification.

Examples of traffic equaling the content value you specify are as follows.

Content Type	Content Name (Example)	Content Value (Example)	Matched Traffic (Example)
SOAP value	CustomerID	12345	<CustomerID>12345</CustomerID>
URL parameter	trade	sell	path?type=web&trade=sell
Form value	origin	web	transaction=sales&origin=web
HTTP header value	X-DataType	customer	X-DataType: customer
Cookie	beta	two	Cookie: alpha=one;beta=two or Set-Cookie: alpha=one;beta=two
Custom Regular Expression		DataField=[0-9]*XXX	DataField=43543XXX

Advanced Page Match Criteria

The Advanced text box in the Page Match Criteria section enables you to narrow the page match criteria to specific properties of the page. AppResponse 11 provides predefined variables for most web page properties. You can specify the values of these property variables and combine them in expressions.

The table below lists the predefined web page properties for which you can specify values. For example, if you want to collect statistics about traffic for all web pages that use server port 8080, you could enter:

```
$serverPort=8080
```

After the table, rules for combining properties into expressions are presented.

Property Name (case insensitive)	Type
clientContinent	String
clientCountry	String
clientIP	IP
clientPort	Integer
clientRegion	String
hostname (normalized to lowercase)	String
HTTPS	Boolean
incomplete	Boolean
incompleteObjects *	Objvector
method	String
numTcpConns *	Integer
objects *	Objvector
optimized (retrieved through a SteelHead)	Boolean
optimizedObjects (retrieved through a SteelHead) *	Objvector
originIP	IP
pageTime *	Double
path (normalized to UTF-8 and %HH for values < 0x20)	String
requestBody	String
requestBytes (sum of header + body)	Integer
requestHeader	String
responseBody	String
responseBytes	Integer
responseHeader	String
serverContinent	String
serverCountry	String
serverIP	IP
serverPort	Integer
serverRegion	String
session	String
statusCode	Integer
title	String

Property Name (case insensitive)	Type
URL	String
username	String
soapmethod *	String

Notes on web page properties variables:

- Asterisks denote properties that apply to only pages and not to individual objects.
For example: \$pageTime
- These properties (with the exception of those marked with an asterisk) are based on the main object of the page. For example, the "\$method" of the page is actually the method of the main object (i.e., the first object) of the page.
- Type objvector - vector of objects, number with size(<var>), access Nth element with [N]
For example, an expression to detect pages that have any incomplete objects is:
size(\$incompleteObjects) > 0

The following rules apply when combining variable definitions into expressions to enter in the Advanced text box in the Page Match Criteria section.

- Expressions can be of any length within the limits of the Page Match Criteria section. Refer to the [“Page Match Criteria Limits”](#) section below.
- If there is an error in the construction of the expression, then there will never be a match with monitored traffic.
- The expression can contain any of the following:
 - References to properties in the table above by using a dollar variable.
For example: \$url
 - A match against a regular expression by using the “in” operator with the regex contained in quotes.
For example: \$url in "pattern"
 - A match against an IP address by using the “in” operator with the address in CIDR format.
For example: \$serverIP in 192.168.1.0/24
 - For a specifically assembled IP address range such as 192.16.1.10 - 192.168.2.20, specify:
\$serverIP >= 192.168.1.10 and \$serverIP <= 192.168.1.20
 - For a specifically assembled IP address range such as 192.168.1.0/26 except 192.168.1.10, specify:
\$serverIP in 192.168.1.0/26 and not (\$serverIP = 192.168.1.10)
 - Numerical comparisons: <, <=, >, >=, =, <>, !=
For example: \$packetsIn > 2
 - Boolean logic: and, or, not
For example: \$url in "pattern1" or \$url in "pattern2" or not \$url in "pattern3"
 - Grouping (by using parenthesis).
For example: \$url in "pattern" and (\$serverIP in 192.168.1.0/24 or \$pageTime > 5.0)

- Check against a set of values with the “in” operator and {{ }} as delimiters.
For example: `$responseCode in {{ 404, 501, 502 }}`

Page Match Criteria Limits

The Page Match Criteria section of the New Web Application dialog supports a total of approximately 600 tokens, where tokens are counted as follows:

- In the URL Patterns section, each URL pattern counts as two tokens.
- In the Content Values section, each entry counts as two tokens.
- In the Advanced section, each property variable counts as one token and each constant counts as one token. For example, the following expression has six tokens, which are indicated in boldface type:

(`$clientPort = 1001` or `$clientPort = 1002`) and `$url in "mypage[0-9]*"`

Operators (=, and, or, in) do not count as tokens.

Note: Riverbed recommends that the combined total of the tokens in all three sections should not exceed 600. This number is a strong advisory, not an enforced limitation.

Auto-recognized

The Auto-recognized tab lists the applications that are already defined when you purchase or update AppResponse 11. These cannot be deleted or modified.

To track traffic for an auto-recognized application using a more inclusive or exclusive definition, add the application on the General tab and set the new definition to High priority or Medium priority. Alternatively, add the application to the URL tab or the Advanced Web tab.

Importing and Exporting Application Definitions

Definitions of general applications and URL applications can be exported to a CSV (comma separated value) file, a format used by many spreadsheet applications, edited in the CSV file, and subsequently imported back in to AppResponse 11. This provides a convenient mechanism for editing a large number of application definitions in a short amount of time. Definitions of web applications can be exported to a JSON file to be worked with in a similar way.

The Import and Export controls are located at the upper right of the Application Configuration page.

Clicking Export displays a dialog with checkboxes for General Applications, URL Applications, and Web Applications. Each is selected by default. Click Export to create a zip file that contains separate CSV files for URL applications and general applications, as well as a JSON file for web applications.

The general applications CSV file provides the existing application definitions with the following fields:

- Version [AR11]
- Data Type [general applications]
- Timestamp
- Name

- Description
- Enabled
- Priority
- Auto-recognized app definitions
- Transport protocol definitions

The URL applications CSV file provides the existing application definitions with the following fields:

- Version [AR11]
- Data Type [URL applications]
- Timestamp
- Name
- Description
- Enabled
- Preferred
- URLs

The Web applications JSON file provides the existing application definitions with the following fields:

- Version [AR11]
- Data Type [Web applications]
- Timestamp
- Slow Page Threshold
- Content Values
- Name
- Use Advanced Criteria
- Description
- Use URL Patterns
- Enabled
- Preferred
- URL Patterns
- Use Content Values
- Match
- Advanced Criteria
- Tags

To export application definitions to CSV file:

1. Choose Definitions > Applications to open the Application Configuration page.

2. Click Export at the upper right of the Application Configuration page. Clicking Export displays a dialog with checkboxes for General Applications, URL Applications, and Web Applications. Each is selected by default. Click Export to create a zip file that contains separate CSV files for URL applications and general applications, as well as a JSON file for web applications. By default, the file names are: “applications.zip”, “gen_apps_ar11.csv”, “url_apps_ar11.csv”, and “web_apps_ar11.json”. The application definitions table is written to the specified CSV file and/or JSON file immediately.
3. Double-click the file to open it in the associated application, or drag the file to a folder to edit it at a later time.

To import application definitions from CSV file:

1. Choose Definitions > Applications to open the Application Configuration page.
2. Click Import at the upper right of the Application Configuration page. A dialog box appears; type the name of the CSV file you want to import, or click Choose File to browse the file system and select it. Click Import to execute the process, and the contents of the file are read in to the application definition table.

Preferred IPs

In a busy network AppResponse might observe 100,000 unique IP addresses in a single minute. To store detailed metrics for the most important IP addresses over time, AppResponse aggregates information from some IP addresses, based on their throughput. Preferred IPs are given priority over other IP addresses, regardless of their throughput. For example, preferred IPs are useful for monitoring Web Client IP addresses of interest that might not have high throughput but whose metrics are important to monitor.

AppResponse stores detailed metrics for a combination of preferred IP addresses and IP addresses with the highest throughput in a given time period. While having a priority, detailed information is not guaranteed to be stored for all preferred IP addresses all of the time.

Important: Specifying a heavily-used Web Server IP can result in that server and its clients “crowding out” most or all other IPs because AppResponse 11 also “prefers” all Web Client IPs that talk to a server.

Note: Preferred addresses can be exported to a .csv file on your local system. AppResponse can import preferred IP addresses from a .csv file on your local system.

Specifying Preferred IP Addresses

You specify a preferred IP address as follows:

1. Go to Administration > Feature Settings: Preferred IPs page.
2. Click **Add** in the toolbar at the top of the table.
3. In the New Preferred IP window, enter an IPv4 or IPv6 address. Multiple addresses, address ranges, and CIDR notation are not supported.
4. Click **Save** to submit the new preferred IP address.

Editing a Preferred IP Address

Change a preferred IP address as follows:

1. With the mouse, hover over the table row to be edited.
2. Click the pencil icon that appears near the right end of the row.
3. The IP address can be modified as needed.
4. Click **Apply** to make or **Revert** to reset the change made.

Deleting a Preferred IP Address

Delete a preferred IP address as follows:

1. With the mouse, hover over the row to be deleted.

2. Click the **x** that appears at the right end of the row.
3. Click **Delete** to remove or **Cancel** to keep.

To delete multiple preferred IP addresses at once:

1. With the mouse, hover over the row to be deleted.
2. Set the check box on the left end of each row to be deleted.
3. Click the **Delete** button in the toolbar at the top of the table.

Exporting Preferred IP Addresses

The preferred addresses you have created can be exported to a .csv file as follows:

1. Go to Administration > Feature Settings: Preferred IPs page.
2. Click **Export** at the right end of the toolbar at the top of the table.
3. The file `preferred-ips-export.csv` is downloaded to your local system. Additional exports use the same file name plus an index value, for example, `preferred-ips-export (2) .csv`.

Importing Preferred IP Addresses

You can import preferred IP addresses from other AppResponse systems as follows:

1. Go to Administration > Feature Settings: Preferred IPs page.
2. Click **Import** at the right end of the toolbar at the top of the table.
3. In the window that opens, click **Choose File** or click in the text box.
4. Select the .csv file to import and click **Open**.
5. Click **Import** to load or **Revert** to cancel.
6. The .csv file's contents are merged with the current preferred IPs.

Port Alias Configuration

Packet Analyzer Plus and AppResponse 11 use port aliases in display names.

The default ports and aliases are based on the IANA definitions. These TCP and UDP port aliases can be added to or revised to match your network traffic. For example, if your network uses a nonstandard port to carry SIP traffic, you can add that port with the TCP and/or UDP *sip* alias to the port aliases. If none of your SIP traffic runs on the default port, you can delete the port or change the alias to identify the TCP and/or UDP protocol that does use the port in your network.

AppResponse displays a name for unidentified network traffic from the *protocol/port number (port alias)* defined, for example, TCP/2753 (de-spot). If no port alias is defined just the protocol and port are used when displaying the name.

Default port alias names use lower case letters, numbers, and special characters. Auto-recognized traffic uses upper and lower case letters, numbers, and special characters. This convention eases traffic identification when viewing traffic in Insights and Navigator.

Use the Port Definitions page to:

- Assign a recognizable name (alias) to an individual TCP/UDP port.
- Edit or delete an existing port alias.

This section addresses the following:

- [“Configuring a Port Alias”](#)
- [“Editing a Port Alias”](#)
- [“Deleting a Port Alias”](#)

Configuring a Port Alias

A port alias can be used by one or more ports. A port can only have one TCP alias and/or one UDP alias defined.

Configure a port alias as follows:

1. Choose Definitions > Port Aliases to open the Port Alias Configuration page.
2. Click **Add** in the tool bar at the top of the table.
3. In the New Port Alias window, enter the following:
 - Port—A port number must be between 1 and 65535.
 - TCP alias—Enter a name if needed. Names can use letters, numbers, and special characters. By convention, alias name are in lower case.
 - UDP alias—Enter a name if needed. Names can use letters, numbers, and special characters. By convention, alias name are in lower case.
4. Click **Save** to store or click the **x** in the top right corner of the window to discard.

Editing a Port Alias

1. Choose Definitions > Port Aliases to open the Port Alias Configuration page.
2. With the mouse, hover over the port alias to be edited.
3. Click the pencil icon that appears near the right end of the row.
4. The contents of the port alias can be modified as needed.
5. Click **Save** to make or **Revert** to reset the change(s) made.

Deleting a Port Alias

To delete a port alias:

1. With the mouse, hover over the port alias to be deleted.
2. Click the **x** that appears at the right end of the row.

To delete multiple port aliases at once:

1. With the mouse, hover over a port alias to be deleted.
2. Set the check box to the left end of port alias to be deleted.
3. Click the **Delete** button in the toolbar at the top of the table.

Policies

Policies enable you to configure AppResponse to detect and alert you when logical network objects exhibit traffic or performance behavior that is noteworthy or otherwise merits examination. Some examples of logical network objects are an IP address, an IP conversation representing the interaction of two IP addresses over the network, a web server, a database server, etc. Policies enable you to specify conditions on the behavior of network objects (i.e., on metric values). When those conditions are met, the policies generate violations. You can review these violations in the web UI and, optionally, configure notifications so that external systems can be informed when these violations occur.

AppResponse furnishes dedicated packet analysis features that analyze traffic to detect the presence of specific types of network objects and calculate feature-specific metrics for each of those objects.

- See **“Application Stream Analysis (ASA) Metrics”** for the list of network objects that are tracked by the ASA module and the metrics it calculates for each object.
- See **“Web Transaction Analysis (WTA) Metrics”** for the list of network objects that are tracked by the WTA module and the metrics it calculates for each object.
- See **“Database Analysis (DBA) Metrics”** for the list of network objects that are tracked by the DBA module and the metrics it calculates for each object.
- See **“Unified Communications Analysis (UCA) Metrics”** for the list of network objects that are tracked by the UCA module and the metrics it calculates for each object.

Each feature analyzes network traffic, detects the presence of network objects in the traffic, calculates a set of feature-specific metrics for each object, and stores the network object and its corresponding metric information every minute. Policies allow you to specify conditions only on the 1-minute metric values that are calculated for network objects; therefore, a policy is always checking the most recent 1-minute value of a metric for an object against a user-specified or built-in policy condition.

AppResponse provides a number of **“Built-In Policies”** that track changes in common network behaviors used often by IT/network operations to track how well a network is doing its job. Most of the built-in policies are enabled by default.

AppResponse enables you to define your own policies, also. You can have up to 750 user-defined policies. The Policies page shows the number of active policies that are defined out of the maximum allowed 750.

Once a policy has been defined, you can edit it to place additional conditions on the traffic it monitors, to change the violation criteria, to add notification recipients, and so on. A policy is Enabled by default.

Note: If you’re migrating to AppResponse 11 from AppResponse 9, **“Importing and Exporting Policies”** is supported, as well.

Static Policies and Adaptive Policies

Policies support two types of metric comparisons: static and adaptive.

A *static policy* uses discrete trigger criteria for one or more metrics. When the value of a metric matches or exceeds a discrete threshold, an alert is sent to the recipients. All metrics support static policies. One example of a policy with a static condition is:

Host Group Denver should be in Minor violation state when the total throughput to Denver's IP addresses exceeds 25 Mbps, in a Major violation state when the total throughput exceeds 50 Mbps, and in Critical violation state when total throughput exceeds 75 Mbps.

This is a static policy because the violation state is determined by applying user-defined static thresholds for metric values, i.e., the latest current-minute metric value of Total Throughput for HG Denver is compared against the static threshold values for Minor (25 Mbps), Major (50 Mbps) and Critical (75 Mbps) configured by the user.

An *adaptive policy* uses relative trigger criteria for one or more metrics. When the value of a metric deviates by a specified factor from what is normal for that time period, an alert is sent to the recipients. Not all metrics support adaptive policies. One example of a policy with an adaptive condition is:

Web User Group San Francisco should be in Minor violation state when the average Page Time experienced by the users in San Francisco across all web apps deviates from normal by one standard deviation, in Major violation state when the deviation is two standard deviations, and in Critical state when the deviation is three standard deviations.

This is a adaptive policy because the violation state is determined by assessing the extent to which the current-minute metric value has changed from an autocomputed normal value. In other words, the current-minute metric value is compared to a autocomputed normal value that adapts over time.

Note: The Comparison Type cannot be changed after the policy definition has been completed.

Defining a Policy

1. Click Definitions > Policies to open the Policies page.
2. Click Add to open the Create New Policy wizard. The wizard provides four pages for defining the policy, listed in the pane at the left of the wizard. Complete each page in order:
 - **“General Properties”** - The name and description of the policy, as well as its comparison type (Static or Adaptive), and whether it is Enabled or not.
 - **“Alert On & Filtering Properties”** - The traffic objects or attributes the policy monitors. Each object you want the policy to monitor must exist before you create the policy. For example, entities such as Host Groups and Preferred Applications must be defined before you can include them in a policy definition.
 - **“Trigger Properties”** - Define the thresholds for triggering alerts. For static policies, these are discrete thresholds; for adaptive policies, they are relative thresholds.
 - **“Notification Properties”** - The person or system to be notified when a policy violation triggers an alert. This can be a notification recipient that you've defined previously, or an ordinary Email address.

The descriptions that follow describe each wizard page in detail.

General Properties

Return to **“Policies”** if you're looking for an overview of policies.

Specify the policy's General properties:

1. Type the policy name as you want it to appear throughout AppResponse 11. Every policy must have a unique name.
2. Optionally, type a brief, meaningful description of the policy. This can capture additional information that will help you and other users remember why the policy was created, and what the intent and rationale was behind the policy. Riverbed recommends capturing all pertinent info in a policy's description, e.g., a trouble ticket number if the policy was created to troubleshoot a specific problem, or the name of an IT/network operations project that the policy relates to.
3. Choose the Comparison Type: Static or Adaptive. Your choice will affect the options that are available on subsequent pages. The Comparison Type cannot be changed after the policy definition has been completed.
4. The policy is Enabled by default. Deselect the option if you do not want the policy to be in effect immediately.
5. Choose Next to continue to the Alert On & Filtering page.

Alert On & Filtering Properties

Return to **"Policies"** if you're looking for an overview of policies.

The Alert On & Filtering properties specify the objects that are monitored for the policy. Not all objects are supported for Adaptive policies, so the presentation of objects differs depending on whether you've chosen Static or Adaptive as the Comparison Type.

For static policies:

1. Click Add to open the Select Group dialog. Expand the hierarchical tree of filtering options as necessary to specify the order in which each filter is applied to the monitored traffic. The OK button becomes active once you've selected a group type.
2. The sequence of filters you chose is shown hierarchically. Specify the value of each group in the filtering path. Each row that has an edit icon (pencil) must be edited to specify members of the group before you can continue to the Trigger page to define the policy trigger. Click the pencil icon and specify the value for the group type. As you specify the criteria for each group type, the values you enter are displayed.

To replace the entire filtering path, click Replace near the top of the Create New Policy wizard. This re-opens the Select Group dialog, enabling you to specify a new filtering definition.

3. Click Next to continue to the Trigger page.

For adaptive policies:

1. The Alert On & Filtering page displays a dropdown, and prompts you to choose the type of object you want to monitor. Choose an object type, then provide additional information as you are prompted for it.

2. Once you've specified the particular object you want to monitor, click Next to continue to the Trigger page.

Trigger Properties

Return to **"Policies"** if you're looking for an overview of policies.

The Trigger page enables you to define the conditions in which an alert is sent for some traffic behavior on the object you specified in the Alert On & Filtering page. Triggers for static policies are defined in terms of discrete threshold values for one or more metrics. Triggers for adaptive policies are defined in terms of relative threshold values for one or more metrics. When an alert is sent, the corresponding trigger conditions are included in Email notifications, SNMP traps, and are shown in Alert Detail reports.

For any policy, you can compare up to three traffic metrics to alerting criteria to determine when an alert is triggered. One, two, or all three metric comparisons can be used to specify one, two, or three conditions. Possible combinations are:

- Use three metric comparisons to specify one condition. The results of all three comparisons must be true to trigger an alert. (The condition is the logical AND of all the metric comparisons that define it.)
- Use one metric comparison in each of three separate conditions. If the metric comparison in any of the three conditions is true, then that condition triggers an alert. (The policy uses the logical OR of all its conditions.)
- Use two metric comparisons in one condition and a third metric comparison in a second condition. An alert is triggered if either condition contains a metric comparison that is true. (This is logically the AND of two comparisons, OR'ed with a third comparison.)

To define the trigger for a static policy:

1. In the Add a metric comparison section, choose a metric from the dropdown list and specify the values necessary to trigger an alert. The list includes only traffic metrics that are applicable to the type of group you specified in the Alert On & Filtering page for the policy to monitor.
2. Select the type of threshold checking to perform and specify the values for the metric that will trigger alerts. For example, a volume or rate that is only slightly problematic should trigger a minor alert, so enter that value in the Minor box.
3. If you want to add another metric comparison that must be met in order for the condition to trigger an alert, click "Add a metric comparison" to add another row. The condition is true only when all the comparisons are true. That is, the alert condition is the logical AND of all its metric comparisons.
4. If you want to add another condition that also can trigger an alert, click "Add a condition" to add another condition row. Then, add a metric comparison to that condition. If either condition is true, it triggers an alert. That is, the policy uses the logical OR of its alert condition specifications.
5. Specify the number of times over a period of minutes that a violation must occur before it triggers an alert. Refer to **"Alert Levels"** for an example of how this setting affects alerting.

6. Choose from the existing “**Business Hour Profiles**” if you want to constrain the triggering of an alert to a specific recurring time interval. (Business hour profiles are used with static comparisons, not with adaptive comparisons.)
7. Click Next to continue to the Notification page.

To define the trigger for an adaptive policy:

1. In the Add a metric comparison section, choose a metric from the dropdown list and specify the values necessary to trigger an alert. This field is pre-populated with the metric you chose in the Alert On & Filtering page. The list includes only traffic metrics that are applicable to the type of group you specified in the Alert On & Filtering page for the policy to monitor. Specify Deviation factor values for the metric. These values, between 0.1 and 10, specify how many standard deviations from the mean the current measurement must be in order to trigger an alert at Minor/Major/Critical levels.
2. (Optional) Specify a minimum metric deviation value, in the metric’s units. This specifies a discrete minimum tolerance around the comparison window mean for the metric: measurements *within* the bounds of this value will not trigger alerts, regardless of the deviation factor values that are specified.
3. Review the river graph of the metric’s recent behavior. Specify the window of history to show (1 hour, 6 hours, 12 hours, or 1 day), and choose from the dropdown how far back from right now (the “lookback period”) you want to see that window (1 hour, 6 hours, 12 hours, 1 day, or 1 week). The graph will show that portion of the metric’s historical behavior, subject to its availability. In addition, the graph will show, in colored bands, the metric’s normal range and the deviation ranges you specified.

Note: The default average for a window of history is based 50% on the previous instance of that window, and 50% on the total historical average for that window. Changing the lookback period changes the portion used to calculate the historical average, and may cause a period of instability (unexpected alerts or missed alerts) until the new historical data is assimilated.

4. Specify the number of times over a period of minutes that a violation must occur before it triggers an alert. Refer to “**Alert Levels**” for an example of how this setting affects alerting.
5. Click Next to continue to the Notification page.

Alert Levels

The level of an alert reported when a policy is violated is determined by *conditions* and *metric comparisons*. A condition can include one, two, or three metric comparisons.

Conditions

A condition is true if all metric comparisons it contains are true. If a policy has two conditions and both are true, the policy generates an alert that is the higher of the two condition’s alert levels. For example, if one condition meets the criteria for a Minor alert and a second condition meets the criteria for a Major alert, the policy generates a Major alert.

If the policy has only one condition, then it generates an alert of the same level as that condition.

Metric Comparisons

A condition can contain one, two, or three metric comparisons. All the metric comparisons in the condition must evaluate to true for the condition to be true.

If the condition is true, its alert level is the level of the highest severity that is common to all its metric comparisons. This can be understood by asking “With what severity were the first metric comparison AND the second metric comparison violated?”

The alert level of the condition represents the highest severity at which the first metric comparison AND the second metric comparison were violated.

For example, assume that you want to monitor the load on a server. When it gets too high AND it is affecting the actual server response time, you want to be alerted. So you want to limit this policy to high server response time that is correlated with a high connection rate on the server. To do this you specify a condition that requires both metrics to exceed thresholds:

- Server Response Time
 - If it crosses 20, it is a Minor severity policy violation
 - If it crosses 40, it is a Major severity policy violation
 - If it crosses 60, it is a Critical severity policy violation
- Connection Request Rate
 - If it crosses 100, it is a Minor severity policy violation
 - If it crosses 500, it is a Major severity policy violation
 - If it crosses 1000, it is a Critical severity policy violation

Assume that the server response time is 50, which exceeds the threshold considered to be a Major severity. Assume that the connection request rate is 200, which exceeds the Minor threshold but not the Major threshold. That is, for server response time, both the Minor and Major thresholds have been exceeded. But for connection request rate, only the Minor threshold has been exceeded.

So while it is true that server response time AND connection request rate Minor severity thresholds have been exceeded, it is *not* true that both server response time AND connection request rate Major severity thresholds have been exceeded. Therefore, the severity of the condition is Minor.

Regardless of what may be going on with the server response time, the correlation this policy is monitoring for (high server response time AND high connection request rate) has been detected at a Minor level.

You might have another policy for monitoring all cases of high server response time, and that policy will alert you to a server response time problem. This policy alerts you to a level of correlation you are looking for. While this correlation is something you are studying, you do not want a relatively minor level of correlation to raise a Major alert in the operations center.

Notification Properties

Return to [“Policies”](#) if you’re looking for an overview of policies.

The Notification page specifies the recipient to notify when an alert occurs. Notifications can be sent by several different means, as specified by the recipient. You can define recipients using the Definitions > Recipients page if you anticipate that they will be reused frequently, or you can specify an ordinary Email address if that's more convenient.

To define the alert Notification:

1. Click Generate a separate alert for each violating entity to cause alerts for a collective object (such as Any App or Any Host) to be sent for each constituent object (such as each individual application or individual host), instead.
2. Choose Add Recipient to open a list of recipients that have been specified on the Definitions > Recipients page.
3. Select the check boxes in the entries for the recipients that are to receive notifications.
4. Choose Add Email if you want to specify one or more ordinary Email addresses to which to send notifications. You can click Test to send a message to the address to confirm that it's been configured as you expect.
5. Choose the alerting thresholds the recipient/address is monitoring, and for which they will receive notifications.
6. To notify a recipient/address during every minute that the alert is ongoing, click in the right side of the "Notify continuously" slider or use your mouse to click-drag the slider to the right side.
7. Choose Finish to exit the wizard and add the policy definition to the list on the Policies page.

When recipients are notified

All recipients are notified when an alert threshold they are monitoring is crossed in either direction. For example, a new Critical alert crosses Minor, Major, and Critical alerting thresholds, so all recipients will receive notifications that the threshold they are monitoring has been crossed.

Recipients are notified about the starting and stopping of the alert severity level they are monitoring. The policy violation may be more severe than the alert level, but recipients receive notifications about only the alert levels selected in the Notification step of the policy definition.

When the severity of a policy violation decreases below a monitored threshold, recipients monitoring that threshold are notified. For example, assume that Recipient A is monitoring only Critical alerts and Recipient B is monitoring both Critical and Major alerts. Assume that as network conditions improve, the policy violation severity drops below the Critical alert threshold but is still above the Major alert threshold. If no more Critical alerts occur within the specified time span, both Recipient A and Recipient B are notified that the Critical alert is no longer ongoing. This is because both recipients are monitoring Critical alerts. Now, assume that the same policy violation decreases in severity until it no longer exceeds the Major alert threshold. Recipient B is notified that the Major alert is no longer ongoing.

The Alert Event Over option sends a notification to all subscribed recipients up to and including the maximum alert level attained by the alert when it expires due to not having been updated. No additional updates are made to an expired alert, and subsequent violations of the policy will create a new alert. The Alert Event Over notification is sent to all recipients up to, and including, the maximum alert level attained by the alert. For example, if an alert starts at minor, changes after a time to major, subsequently returns to minor, then expires, only minor and major recipients will receive Alert Event Over notifications. Any recipients of critical alerts would not receive an Alert Event Over notification, since they never received an Alert Has Started notification.

There is a limit of 25 alerts/evaluation period imposed for all policies (user-defined policies and built-in policies). This limit prevents overly sensitive policies from flooding the alerting and notification systems. If a particular policy has more than 25 alerts in a single evaluation cycle, the alerts will be triaged by severity: more severe alerts will have priority over less severe ones.

Notification example

The product checks for policy violations once per minute. Assume that you specify that an alert is to be generated if a policy violation occurs more than twice during a 5-minute period. Assume that there are currently no policy violations. Alerting could proceed as in this example:

12:00 - No violations.

12:01 - No violations.

12:02 - No violations.

12:03 - A Minor violation occurs. No alert is generated, but the appliance waits to see if a second Minor violation will occur within 5 minutes of the first violation.

12:04 - No violations.

12:05 - No violations.

12:06 - A second Minor violation occurs. It has not been 5 minutes since the first policy violation occurred at 12:03, so the appliance recognizes a Minor alert and sends notifications (if configured) that a Minor alert has started.

12:07 - No new violations. If configured to continuously notify recipients, the appliance sends notifications that the Minor alert is ongoing.

12:08 - A Major violation occurs. This violates both the Minor criteria and the Major criteria. So the appliance sends notifications that a Major alert has started.

12:09 - No new violations. The appliance sends notifications to continuously notified recipients that the Major alert is ongoing.

12:10 - 12:12 - No new violations. The appliance continues to send notifications each minute that the Major alert is still ongoing and continues to wait for another alert to occur within 5 minutes of the latest alert.

12:13 - No new violations within the past 5 minutes. The appliance sends notifications that the Major and Minor alerts have ended.

Editing and Deleting Policies

On the Policies page, you can set a policy to be active or inactive with the slider switch in the Active column.

To edit a policy definition

1. Hover your mouse over an entry to display the edit icon (pencil).
2. Choose the edit icon and make your edits on the Edit Policy page. This page includes all the settings you configured in the wizard steps.
3. Choose Save to keep your edits or Revert to return to the previous specification.

To delete policies:

To delete an individual policy, hover your mouse over the entry for the policy and choose the delete (x) icon.

To delete multiple policies, select the check boxes at the beginning of the rows listing the policies and then choose Delete near the top of the page.

Built-In Policies

AppResponse provides a number of built-in, preconfigured policies that can be modified, but cannot be deleted.

For each built-in policy, you can:

- Enable/disable
- Configure notifications
- Configure the “**Business Hour Profiles**”
- Update the threshold values, but not the metrics being tracked
- Set the list of inclusions or exclusions. For example, the Network Packet Loss built-in policy allows the editing of client groups.

The Built-in Policy configuration page appears in a separate tab from the user-defined Policy configuration page, and the alerts generated by the built-in policies similarly will be separated from user-defined Policy alerts.

- Built-in Policies that use unlicensed data sources (the VoIP policies and the DB perf policy) will be visible, enabled, and configurable, but will not produce any alerts.
- Built-in policies generate one violation per alert; this is not user-configurable.
- Built-in policy alerts use corresponding Insights to enhance the Alert Detail information.

Currently, the following built-in policies are available:

Policy Name	Alert On	Default Activation
Foreign Country DNS Request	DNS request sent to a server in another country	Disabled
Large Number of DNS Errors	Sudden increase of DNS errors for specific server	Disabled
Large Number of DNS Timeouts	Sudden increase of DNS timeouts for a specific server	Disabled
Adaptive Threshold for Application-based Server Response Time	Any application showing abnormal Server Response Time in the last day.	Enabled
Adaptive Threshold for Host Group Throughput	Any Host Group showing abnormal Total Throughput in the last day.	Enabled
Web Server Errors (requires WTA module)	Any web server returning significant server errors.	Depends on license
Network Packet Loss	Any client groups experiencing significant retransmissions.	Disabled
Server Availability	Any server IP failing to accept inbound connections.	Enabled
Poor VoIP Call Quality (requires UCA module)	Any user group experiencing VoIP calls with low MOS-CQ.	Depends on license
Poor Video Call Quality (requires UCA module)	Any user group experiencing Video calls with low MOS-V.	Depends on license
Database Availability (requires DBA module)	Any DB server with rejected sessions.	Depends on license

Importing and Exporting Policies

User-defined policies can be exported and imported, enabling you to move them from one system to another. Built-in policies are features of the installed software, and cannot be exported or imported.

The Policies page tool bar provides an Export button near the left side of the page, and an Import button at the right side. The Export button becomes accessible when one or more user-defined policies are selected, and writes the selected policies to a single .json file.

AppResponse 9 policies can be imported using .csv files. AppResponse 11 policies can be imported using .json files, with multiple Insight definitions in a single .json file.

Note: Prior to importing policy definitions from AppResponse 9, you need to make sure that, first, you import host group and application definitions that had been exported from AppResponse 9.

The following operations occur during a policy import:

- Version check; an imported file cannot be from a version later than the system performing the import.
- Validate that all drilldowns are valid. Policies with invalid drilldowns will be removed, and an error displayed.
- Validate that all metrics are valid. Policies with invalid metrics will be removed, and a error displayed.
- Validate that all columns are valid. Invalid columns will be removed from the imported policy, and a warning displayed.
- If a policy specifies defined applications, Host Groups, web apps, VIFGs, page families, or web users, these are looked up by name. If the name is found, the correct ID is set in the relevant Insight. If the name is not found, the policy is not imported and an error is displayed.

When the import is complete, a dialog is displayed if there are any warnings or errors for any imported policies. Save errors, such as a duplicate name, are identified at save time and displayed in this dialog, also.

Traffic Analysis Filters

Traffic analysis filters are used by Packet Analyzer Plus when applying application views to traffic. The protocol filters web UI page lists applications and their IP protocol, server port(s), and server IP address(es). If these applications in your network do not use the same IP protocols, server port(s), or server IP address(es), the protocol filter definitions can be revised to match those used by your applications. This ensures that Packet Analyzer Plus views reliably report this application traffic in your network.

The filters are fixed and cannot be renamed or deleted. They can be disabled.

Note: The default filters work in most networks. Errors made when revising or disabling these filters can cause unreliable results when application views are applied in Packet Analyzer Plus.

If changes are made to these filters, they must be synchronized with any Packet Analyzer Plus using this AppResponse 11 system as a probe.

This section covers the following:

- [“Example Use Cases” on page 159](#)
- [“Editing Protocol Filters” on page 159](#)
- [“Adding a Definition to a Filter” on page 160](#)
- [“Synchronizing Changes with Packet Analyzer Plus” on page 161](#)

Example Use Cases

You use both standard and nonstandard IP protocols and ports to carry SIP traffic in your network. You can add the protocols and ports that carry SIP traffic in your network to the SIP filter. If none of your SIP traffic runs on the default protocols and ports, you can revise the default definition with the IP protocols and ports that you do use for SIP traffic. This ensures that Packet Analyzer Plus application views reliably report the SIP traffic on your network.

Specifying a server or servers in a filter definition can be used to report only application traffic of interest. For example, if you are not interested in external traffic for WEB, you could add the server IP addresses for your internal server(s) to the WEB filter and report only that traffic in the Packet Analyzer Plus web views.

Editing Protocol Filters

1. Go to Administration > General Traffic Settings: Traffic Analysis Filters, and click the tab for the set of protocols you want to work with.
2. With your mouse, hover over the application filter to be edited. Click the pencil icon that appears at the end of the row.
3. The Edit Traffic Filters dialog opens, showing the current filter definitions by protocol.
 - To delete an IP protocol, hover over the entry and click the x that appears at the end of the entry.
 - To revise an existing IP protocol entry, hover over the protocol and click the pencil icon on the right.

4. In the Edit Traffic Filters dialog, the existing IP protocol, server ports, and server IP addresses are displayed.
 - To change the existing IP protocol, select the new IP protocol from the drop-down list.
 - To delete a port or port range, click in the Server Ports box and click the **x** to the right of the entry.
 - To edit existing Server Ports, click in the Server Ports box and enter your changes. Existing ports can be edited by double-clicking in their box. New ports can be added one at a time or in a comma-separated list. Port ranges can be entered separated by a dash. A mix of ports and port ranges can be entered in a comma-separated list. Press the Enter key after each entry.
 - To add a Server IP address, click in the Server IP box and enter an address or a range of addresses, separated by commas. IPv4 and IPv6 addresses in standard or CIDR format can be used.
5. Click **Apply** to make the changes or **Revert** to discard them.
6. In the Edit Traffic Filters dialog, click **Save** to update the filter.

Adding a Definition to a Filter

1. Go to Administration > General Traffic Settings: Traffic Analysis Filters, and click the tab for the set of protocols you want to work with.
2. With your mouse, hover over the application filter to be revised.
3. In the Edit Traffic Filters dialog, click **Add**.
4. In the New Filter window select the new IP protocol to add from the drop-down list.
5. To add server ports, click in the Server Ports box.
 - Ports can be added one at a time or in a comma-separated list.
 - Port ranges can be entered separated by a dash.
 - A mix of ports and port ranges can be entered in a comma-separated list.
 - Press the Enter key after each entry.
6. To add server IP addresses, click in the Server IPs box.
 - Enter an IP address or a range of IP addresses, separated by commas.
 - IPv4 and IPv6 addresses in standard or CIDR format can be used.
 - Press the Enter key after each entry.
7. Click **Apply** to make the changes.
8. Click **Save** to update the filter.

Synchronizing Changes with Packet Analyzer Plus

If you make changes to the traffic analysis filters, they must be synchronized with Packet Analyzer Plus so application views correctly show your network traffic. For more information on synchronizing filters, see the *SteelCentral Packet Analyzer Plus User's Guide*.

Discovered Service Names

Click Definitions > Discovered Service Names to display the Discovered Service Names page. This page enables the auto-discovery of service names that correspond to web applications and protocols present on the network, which in turn enables you to define and manage corresponding URL applications. (The auto-discovery does not include public web application traffic, such as Google, Facebook, Amazon, etc.) The auto-discovery extracts the service names from HTTP CONNECT messages, Common Name (CN) field, and TLS Server Name Indication (SNI) extensions.

The Enable Auto-Discovery option is disabled by default. Select it and click Apply to make service discovery take effect.

The Discovered Service Names page provides the following tabs for working with discovered services and the corresponding URL applications:

- **Used (URL Apps) tab** – This tab lists the service names that AppResponse discovered from the supported sources and that have been associated with a defined URL application. Select an entry and click Edit URL App to display the Edit URL Application dialog and change the definition of the corresponding URL application.
- **Available tab** – This tab lists the service names that AppResponse discovered from the supported sources and that are not currently used in any URL application definitions. Traffic associated with these service names is not included in calculating L3/L4 traffic volume and TCP performance metrics (refer to “**Application Stream Analysis (ASA) Metrics**” for the complete list). You must include these service names in one or more URL application definitions to allow ASA metric calculation. Select an entry and click Define URL App to display the Define URL Application dialog and specify the definition of the corresponding URL application.
- **Ignored tab** – This tab lists the service names that AppResponse discovered from the supported sources that you have explicitly chosen to ignore, by clicking Ignore in the Available tab. Traffic associated with these service names is not included in calculating L3/L4 traffic volume and TCP performance metrics (refer to “**Application Stream Analysis (ASA) Metrics**” for the complete list). You must include these service names in one or more URL application definitions to allow ASA metric calculation.

The Edit URL App/Define URL App dialog is displayed by the corresponding controls in the Used tab and the Available tab. This dialog enables you to specify a meaningful name and description for the URL application associated with a discovered service. The URL is populated by the discovery process automatically; you can delete the auto-populated value and specify a new one, if necessary.

Insights

An Insight provides a one-page overview of the performance and status of applications and the network.

Drill down is available in some table and chart elements using right-click menu options, for example, the right-click menu can be used to show TCP connections in Navigator filtered, by the selected item.

You can use Navigator charts to build and share your own Insights. These Insights are listed on the Insights page and can be revised by loading them into the Navigator workspace. You control who can view and revise Insights that you create.

A *Saved Report* is one or more Navigator charts or Insights captured at a specific moment in time. Drill down is done using the right-click menu options for some chart elements. You control who can view Saved Reports that you create.

This section covers the following:

- [“Opening Insights” on page 164](#)
- [“Supported Insights” on page 165](#)
- [“Summary Insights” on page 166](#)
- [“Individual Insights” on page 167](#)
- [“Interactive Insights” on page 167](#)
- [“Editing an Insight’s Properties” on page 170](#)
- [“Using the Layout Editor to Modify a Custom Insight’s Content” on page 170](#)
- [“Deleting an Insight” on page 171](#)
- [“Viewing Alert Events” on page 173](#)
- [“Viewing Alert Event Details” on page 175](#)

Related topics:

- [“The Navigator Workspace” on page 192](#)

Opening Insights

You can open some Insights using a shortcut in the Insights menu or by selecting it from a list of all Insights.

1. Choose Insights on the AppResponse 11 menu bar.

2. View an Insight by either:
 - Selecting an Insight under the Summary, Transactions, or Individual headings in the drop-down menu.
 - Selecting More... or Launch/Manage in the drop-down menu.
3. If More... or Launch/Manage is selected, a table containing all of the available Insights is displayed. You can filter the table rows by owner, tag, or name. Filters can be saved and reloaded with a name that you specify. For more information see [“Alerts” on page 173](#).
4. Choose the Insight you wish to view.
5. If an Individual Insight is chosen, specify Inputs to identify the desired group or network element. To use the URL filter, you need to specify the exact URL, including “/” at the end, or the filter will not be valid.
6. Click **OK** to open the Insight.

Note: For HD Insights only, the Launch button is disabled until you specify a value for at least one of the criteria fields.

Specifying IP Addresses and Ports

For HD Insights, IP fields in inputs for time series widgets support the use of wildcards, ranges, and CIDR notation. IP addresses cannot start with a wildcard, and values cannot be specified after a wildcard (for example, 10.*.10 is not permitted). All parts of the IP address must be entered to be valid (for example, 10.10.* is not supported, and must be entered as 10.10.*.*). Ranges are entered with a hyphen and no spaces (for example, 10.10.10.0-10.10.10.255). Both IPv4 and IPv6 addresses are supported.

Similarly, for HD Insights, port fields in inputs for time series widgets support ranges. An example of a valid range is “2400-2800”.

Supported Insights

The built-in insights that are provided in the current release are listed below:

TCP/IP:

- All Traffic: Shows all traffic being monitored.
- Virtual Interface Groups: Shows top Virtual Interface Groups (VIFGs) and identifies host groups, apps, and IP conversations within them.
- Apps: Summary of applications.
- Host Groups: Summary of host groups.
- Servers: View servers.
- IPs: Shows load, network anomalies and performance of top hosts.
- Traffic Diagnostics: Shows load on monitoring interfaces, connections and web requests being processed, as well as flows exported to NetProfiler.

Web:

- Web User Groups: View web user groups.
- Web Apps: View web apps.
- Web Servers: View web servers.
- Web Users: View web users.

VoIP/Video:

- All UC Traffic: Shows all UC traffic being monitored.

Database:

- All DB Traffic: Shows all database traffic being monitored.
- DB Client Groups: View DB client groups.
- DB Servers: View DB servers.

SSL/TLS:

- SSL/TLS Handshakes: View SSL/TLS handshakes.
- SSL/TLS Certificates: View SSL/TLS certificates.

Citrix:

- Citrix Servers: Shows load, network anomalies and performance of a Citrix server.
- Citrix Users: View user experience of a Citrix user and troubleshoot back end issues.
- Citrix User Sessions: View Citrix user sessions.

DNS:

- DNS Servers: View DNS servers.
- DNS Server: View DNS server.
- DNS Transactions: View DNS transactions.

Alerts:

- Alert Events: View system and traffic alert events.

You can save a modified built-in Insight without any filters that you've applied. This is available in the Save Insight As dialog, as a checkbox under Insight mode in the Format section.

Summary Insights

A Summary Insight is an overview of status and performance information for a group, for example, traffic, applications, or TCP servers. A Summary Insight:

- cannot be changed.
- can be saved with a new name or as a duplicate.
 - If renamed or duplicated, it can be changed and saved as an Insight or a Saved Report.
 - Access to the new Insight can also be specified when it is saved.

Individual Insights

An Individual insight is an overview of status and performance information for a specific application or network traffic element for example, a Web Application, a Host Group, or a TCP client. Expand the Input tab in the top left-corner of an Individual Insight, if necessary, to see fields available to identify the application or network element of interest. When providing input to an Individual Insight:

- Required fields must have entries.
- Optional input fields are used to specify the exact item of interest.
 - Specify an input by clicking in the text box - in some cases, entries to choose from are displayed.
 - To use the URL filter, you need to specify the exact URL, including “/” at the end, or the filter will not be valid. Note also that wildcard characters (“*”) are not supported for URLs in Inputs.

An Individual Insight:

- cannot be changed.
- can be saved with a new name or as a duplicate.
 - If renamed or duplicated, it can be changed and saved as an Insight or a Saved Report.
 - Access to the new Insight can also be specified when it is saved.

Interactive Insights

Predefined Insights in AppResponse 11.1.0 and later can include interactivity. Selecting a time interval in a chart or a row in a table updates the charts and tables that follow to display the selected time interval or selected row.

Interactive Insights include:

- Time charts where you can select a peak to drill down into that time interval. Charts or tables to the right and below a selection are updated for the selected time interval.
- A table row selection fills in subsequent tables and charts with data for that row.
- Interactive insights for guided troubleshooting drill downs:
 - Bandwidth Hogs
 - Slow Apps
 - Slow Web Apps

These insights are designed to guide a user to the source of an issue in their network, based on the selection that is made. For example, the Bandwidth Hogs insight guides a user to identify what Host Groups, IP addresses, or Applications are using the bandwidth on a network.

Note: When the time interval is changed the guided charts and tables are cleared as the top tables and charts may be different in the new time interval.

Please note the following:

- Interactive insights cannot be created using Navigator. Interactivity only occurs in predefined insights.

- Changing a time interval can clear some charts or tables if they have no data for that time interval.
- Input criteria and group interactivity are not supported together in an insight.

Viewing Insights

All Insights have a toolbar in the top-right corner of the screen.

- **Time interval**—The time interval is used to calculate the data and metrics in the tables and charts in the Insight, with the time interval currently in effect shown between two arrows. Click an arrow to change the interval incrementally, or select a predefined current time interval (15m, 1h, 1d, 1w, 1m). Clicking the time interval itself displays a dialog that enables you to specify a custom interval or choose from existing **“Business Hour Profiles”**.
- **Auto-Update**—If enabled, an Insight can be used to monitor specific application or network performance. When enabled the Insight data in tables and charts is changed on an interval you specify in minutes. This is disabled by default.
- **Countdown Icon**—This icon indicates when the next Insight update will occur. It is displayed next to Auto-Update when it is enabled.
- **Update Interval**—Click the pyramid icon and specify the number of minutes between auto-updates.
- **Open Insight in New Tab**—Opens the current Insight in a new browser tab. In the new tab, drill downs can be done while preserving the original Insight in the previous tab. You can try a drill down and start over from the previous tab if the results aren't what you need.

Drill Downs

Right-click a group name or chart element - if drill down is supported a menu appears with available options. Options can include:

- **Add to Favorites**—Right-click a group name in a table row or select a chart element to add it to a new Favorite (with default name Favorites - x) or to add it to an existing Favorite. Select the data to add.
- **Add to Workspace**—Select to add a group to a new or a current chart or table in the workspace. Next, select the new chart or a current chart for the group.
- **Download Packets**—When packets are available, save packets as a PCAP trace file to your local system. If there is more than one capture job defined, choose the capture job with the packets from the displayed list.
- **Launch “Individual or Summary Insight”**—Launches the individual or summary Insight.
- **Launch SteelCentral Packet Analyzer Plus**—Sends packets (when packets are available) to Packet Analyzer Plus on the local system. Packet Analyzer Plus opens and adds a new probe if the AppResponse is not already a probe. The packets are sent and a default view is applied by Packet Analyzer Plus.
- **Search**—The selected item is searched in AppResponse and the results are displayed. Click links in the search results to view more detailed information on the selected item.

- **Show Individual Page Views**—The Individual Page Views group opens, filtered by the right-clicked group or chart element. The filter is shown in the table toolbar.
- **Show TCP Connections**—The TCP Connections group opens, filtered by the right-clicked group or chart element. The filter is shown in the table toolbar.
- **This Application**—Opens an Insight based on the group or chart element selected.

Launching and Managing Insights

To display a list of available Insights go to Insights > Actions: Launch/Manage.

The Insights are listed in a table with a selectable numbers of rows displayed (default 10). Predefined Insights have no Owner. Duplicate or new Insights are owned by selected roles.

The Insights toolbar appears at the top of the table. The tools available are:

- **Add**—Provides a link to Navigator where Insights can be built in the workspace and saved. Insights created in Navigator can also be loaded and edited later in Navigator.
- **Delete**—Removes selected Insights from the table. If a predefined Insight is selected the Delete icon is not active.
- **Duplicate**—A window opens with the name Duplicate *<Insight name>* for the selected Insight.
 - Access can be chosen for a predefined Insight duplicate.
 - Access and Read-Only or Read/Write privileges can be assigned by role for all other Insights.
- **Add Tags**—Specify a comma separated list of tags to add to an Insight. Tags cannot be added to predefined Insights.
- **Export**—Custom Insights can be exported to a .json file so they can be imported to other AppResponse 11 systems; multiple Insights can be written to a single .json file. Built-in Insights cannot be exported.
- **Import** —Click this to select a .json file and read in one or more custom Insights. Refer to [“Importing Custom Insights”](#) for details.
- **Filter Bar**—Multiple filters can be applied to the list of Insights. A green background indicates an applied filter in the filter bar. Click the funnel icon to select the type of filter and choose its values:
 - By owner displays a list of owners for selection.
 - By tag displays a list of all current tags for selection.
 - By name matches the text specified with Insight names.
 - Tags is a shortcut to selection by tag used when applying multiple filters.
 - All Shared is a shortcut to by owner used when applying multiple filters.
 - Click **Apply** to use the revised filter.
- **Editing a filter**
 - A filter type appears with a green background when that filter type is an applied filter. To edit the applied filter, click the desired filter type with a green background. The applied filter is displayed and can be edited.

- To change the filter click in the text box (Name) or change selections in a list (Tags or Owner/Shared).
- Click apply to use the revised filter.
- Removing filters
 - To remove a single filter, click the **x** in the upper-right corner of the green box.
 - To remove all filters, click the **x** in the black box at the end of the filter bar.

Editing an Insight's Properties

Insights with owners can be edited by roles with read/write access. Built-in Insights (no owners) cannot be edited.

1. With the mouse, hover over the Insight to be edited.
2. Click the pencil icon at the end of the row.
3. The Name and Description fields can be modified as needed. If the name is changed the Insight is saved with the new name, replacing the current name.
4. Tags are a comma-separated list. New tags can be added and existing tags can be modified or deleted.
5. Define a schedule for the insight by clicking the “+” in the Schedules column to display the Create New Schedule wizard.
6. Select the access to the Insight.
 - Public or Private access allows the Insight to be used by anyone or only yourself.
 - Shared access is granted by role. You select read-only or read/write access for each role.
7. Click Apply to complete and save the Insight.

Using the Layout Editor to Modify a Custom Insight's Content

The layout of custom Insights can be changed at any time, using the Layout Editor. Layouts include the individual metrics that are displayed in the Insight, the type of widget used to display them, their arrangement on the Insight page, and the time parameters that control which data are displayed at one time. Insight layouts cannot be changed for the built-in Insights that are provided with AppResponse 11.

The Layout Editor is launched automatically when you begin creation of a custom Insight. Access the Layout Editor later by clicking the wrench icon in the tool bar at the upper right of the Insight. The Add Widget dialog provides the following sets of controls on separate tabs:

- Grouping: Select the metrics you want to include.
- Visualization: For each metric, specify the type of widget and pagination.
- Time: Specify the time properties for the metrics.
- Meta: Specify the Title, Description, and Tags the Insight will use.

Adaptive Mode and Static Mode

Choose Adaptive or Static from the Layout dropdown menu in the Edit Layout page. Adaptive mode provides you with full control over the set of widgets in the Insight, enabling you to add, remove, reorder, move, and resize them. Static mode is more restrictive, enabling you to move and resize the existing set of widgets in the Insight.

Deleting an Insight

Insights with owners can be deleted by roles with read/write access. Predefined Insights (no owners) cannot be deleted.

1. With the mouse, hover over the Insight to be deleted.
2. Click the **x** at the end of the row.

Importing Custom Insights

The following operations occur when a custom Insight is imported:

- Version check; an imported file cannot be from a version later than the system performing the import.
- Validate that all drilldowns are valid. Insights with invalid drilldowns will be removed, and an error displayed.
- Validate that all metrics are valid. Insights with invalid metrics will be removed, and an error displayed.
- Validate that all columns are valid. Invalid columns will be removed from the imported Insight, and a warning displayed.
- If an Insight specifies defined applications, Host Groups, web apps, VIFGs, page families, or web users, these are looked up by name. If the name is found, the correct ID is set in the relevant Insight. If the name is not found, the policy is not imported and an error is displayed.

At the conclusion of the import, a dialog is displayed if there are any warnings or errors on any imported Insights. Save errors, such as a duplicate name, are caught at save time and displayed in this dialog.

Schedules

Most insights can be scheduled to run at specific times, or at specific intervals, to generate saved reports. The few insights that cannot be scheduled make use of interactive components that are not included in the scheduling definition. Each insight can have multiple schedules defined for it, and each schedule is a parent of the saved reports that are generated as a result.

Click Insights > Actions:Schedules to display the Schedules page for defining and managing saved report schedules. This list can be sorted using a number of its column headings. Click Add on the Schedules page to display the Create New Schedule wizard, which will guide you through the steps for defining a schedule. Alternatively, if the Insights page is displayed, you can display the Create New Schedule wizard simply by clicking the “+” in the Schedules column for a listed insight. If you have an insight definition open for editing, you can click the calendar icon at the upper right of that page to display the Create New Schedule wizard.

1. Type a meaningful name for the schedule.
2. Choose the type of insight to which the schedule applies.
3. Type a descriptive explanation for the schedule.
4. Add any tags that you want to be associated with the schedule.
5. The schedule is active by default, but you can toggle the schedule to be inactive, if you don't want it to execute.
6. Specify any inputs that are needed for the specified insight type. Some insights don't require any inputs; others require you to supply relevant information such as IP addresses. You can choose to inherit the default inputs from the associated insight, or you can choose to specify custom inputs. If the inputs are customized, they lose their inheritance relationship with the insight.
7. Define the timing of the schedule (Recurrence); whether the saved report will be generated once only, or at recurring intervals, as well as when the schedule must start and finish. The time that the schedule will execute next is displayed below these controls.
8. Specify the “window,” the duration of time that the scheduled saved report will encompass (Time Frame). The next time the schedule will execute is shown, along with the particular span of time that will be saved report when it does. The window can look forward or backward from the scheduled run time, so check this carefully to ensure that you've specified the correct time span. Note that you can specify an existing business hour profile to use, or click the link to define a new one. Non-business hours will be grayed out in time series charts.
9. Specify one or more Email recipients for the saved report. These can be recipients that have been defined previously in AppResponse 11, or ordinary Email addresses. You can click Test Email to send a message to the address to confirm that it's been configured as you expect. In addition, type the name of the saved report's PDF file.
10. Specify whether the resulting saved report is to be public, shared with users with particular roles, or private.

Existing schedules can be edited to change their definitions, and can be deleted if desired. A schedule's activation status can be toggled through the schedule definition itself, or using the Active column on the Schedules page.

Completed saved reports are available on the Saved Reports page. Each scheduled saved report can be clicked on to be explored, and is available as a PDF for convenient distribution.

Viewing Saved Reports

When viewing a saved report:

- the time interval of the saved report is fixed.
- drill downs for groups and chart elements are done using the right-click menu, if a drill down is available.
- tables and charts cannot be changed or deleted.
- the saved report cannot be saved; however, the most recent instance of a scheduled saved report is available as a PDF document that can be downloaded and shared.
- the list of saved reports can be sorted by saved report name, schedule name, insight name, owner, or creation date.

Alerts

In AppResponse 11 when an event on your network violates a policy you configured, an alert is triggered. You can view alerts and their details using the Alerts submenu under Insights in the web UI.

Two alert Insights are available:

- **Alert Events**—A list by alert ID of all or selected policies that took place in the time interval chosen or specified.
- **Alert Event Details**—An event summary for a specified alert ID. This includes the policy, severity, duration, and policy trigger conditions.

This section covers the following topics:

“Viewing Alert Events”

“Viewing Alert Event Details”

Note: Disabling alerts suspends the alert mechanism. When alerts are disabled, AppResponse 11 continues tracking trigger criteria, as it does when alerts are enabled, but abstains from sending an alert unless or until alerting is re-enabled. If alerting is re-enabled, alerts are sent according to the trigger criteria that were tracked while alerting was suspended.

Viewing Alert Events

You can choose or specify a time interval and view alerts for all policies or a selected policy in that time interval.

To view alert events:

1. Go to Insights > Alerts: Alert Events
2. On the Inputs tab, specify the following:
 - **Policy Type**—AppResponse 11 supports Traffic policies only.
 - **Name**—To view alerts for all policies, leave this field blank. To view alerts for a specific policy, click in the text box and select the policy from the displayed list or enter the policy name.

3. Set or clear the Show Ongoing Only check box to see only ongoing alerts.
4. Click **Launch**. A table listing the alerts by alert ID is displayed.

To display other alerts you can:

- change the time interval.
- click the expand icon next to Inputs at the top of the page and repeat steps 2 through 4 above.

Note: There is an Alert Events tab provided in the Host Groups, IPs, and Server IPs Insights, enabling you to view relevant alert events without leaving those Insights.

Alert Events Table

Based on the inputs provided, AppResponse 11 displays a list of alerts by alert ID. The table can be modified in the following ways:

- The table can be sorted using any column heading by clicking the up or down arrowhead icons to the right of a column heading.
- To change the columns that are displayed, click the More icon, then click Open Column Chooser. This displays the Column Chooser dialog, enabling you to modify the set of columns shown in the table.
- The number of rows displayed can be set in the bottom-right corner of a large table.
- To change a table's time interval, use the table toolbar in the upper-right corner of the page.
 - Select a predefined current time interval (15m, 1h, 1d, 1w, 1m) or click the pencil or in the displayed time interval to specify the time interval in units of one minute or greater.
- To display the table on a single page, hover over the top-right corner of the table and click the settings icon (gear).
 - In the Edit Widget window, click Appearance in the left column, then clear the Enable Pagination check box.
- To add a title to the table, hover over the top-right corner of the table and click the settings icon (gear).
 - In the Edit Widget window, click Appearance in the left column, then specify a title in the Widget Title text box.
- To view the Alert Event Details for a table row, click the ID in the first column. The Alert Event Details page for that alert ID then opens.

Monitoring Alerts Using the Alert Events Page

The table toolbar has a check box to enable or disable Auto-Update of the table's contents. The update cycle (in minutes) can be set by clicking the expand icon to the right of Auto-Update. Specify the desired update cycle in minutes, then press Enter. A countdown icon appears to the right of Auto-Update when it is enabled, indicating the status of the next update.

Saving an Alert Events Page

An Alert Events page can be saved as an Insight in two different formats:

- **Insight**—Insights you create can be revised and renamed in the Navigator workspace.
- **Saved Report**—A Saved Report is a one-time image of a chart's contents.

To save an Alert Events page:

1. Click the disk icon at the end of the table toolbar to open the Save Insight as window.
2. The Name and Description fields can be modified as needed. If the name is already used by an Insight a new name must be used.
3. Tags are a comma-separated list. New tags can be added and existing tags can be modified or deleted.
4. Select the access to the Insight.
 - Public or Private access allows the Insight to be used by anyone or only yourself.
 - Shared access is granted by role. You select read-only or read/write access for each role.
5. Select the format to be saved in.
 - Insight
 - Saved Report
6. Click **OK** to save or **Revert** to discard your changes. To cancel, click the **X** in the top-right corner of the window.

Viewing Alert Event Details

An alert ID number is used to select the event details to view. Alert IDs are displayed in the first column of the Alert Events table. If you click an alert ID in an Alert Events table, the Alert Event Details for that ID are then displayed. Note that for host groups and IP addresses associated with an alert, right-clicking gives you the option of accessing captured packets, using the Download Packets (for IP addresses) and Packet Download Preview (for Host Groups) commands.

To view alert event details:

1. Go to Insights > Alerts: Alert Event Details
2. On the Inputs tab, enter the alert ID you wish to view.
3. Click **Run**.

An event summary is displayed with the following information:

- **ID [#]**—A number assigned by AppResponse 11.
- **Policy**—The name of the policy that was violated.
- **Policy Type**—AppResponse 11 supports Traffic policies only.
- **Severity**—An icon for one of the three trigger conditions.
- **Severity Value [#]**— A number from 1 (low) to 100 (high),

- **Start Time**—Date and time of the first violation of the policy.
- **Duration [min]**—Time in minutes until the policy violation stopped.
- **Conditions**—Trigger conditions set in the policy.

The Alert Detail Insight Groups With Violations table includes a Group column for all alerts, including relevant AppResponse 11 tag data.

Saving an Alert Event Details Page

An Alert Events page can be saved as an Insight in two different formats:

- **Insight**—Insights you create can be revised and renamed in the Navigator workspace.
- **Saved Report**—A Saved Report is a one-time image of a chart's contents.

To save an Alert Event Details page:

1. Click the disk icon at the end of the table toolbar to open the Save Insight as window.
2. The Name and Description fields can be modified as needed. If the name is already used by an Insight a new name must be used.
3. Tags are a comma-separated list. New tags can be added and existing tags can be modified or deleted.
4. Select the access to the Insight.
 - Public or Private access allows the Insight to be used by anyone or only yourself.
 - Shared access is granted by role. You select read-only or read/write access for each role.
5. Select the format to be saved in.
 - Insight
 - Saved Report
6. Click **OK** to save or **Revert** to discard your changes. To cancel, click the **X** in the top-right corner of the window.

Alert Event Details Table

Based on the alert ID provided, AppResponse 11 displays a list of groups with policy violations. The table can be modified in the following ways:

- The table can be sorted using any column heading, except the first, by clicking the icon to the right of a heading.
- The number of rows displayed can be set in the bottom-right corner of a large table.
- To display the entire table on a single page, hover over the top-right corner of the table and click the settings icon (gear) that appears.
 - In the Edit Widget window, click Appearance in the left column, then clear the Enable Pagination check box.

- To add a title to the table, hover over the top-right corner of the table and click the settings icon (gear) that appears.
 - In the Edit Widget window, click Appearance in the left column, then specify a title in the Widget Title text box.

Insight PDF Downloads

Clicking Reports > Downloads displays the Insight PDF Downloads page, showing the following information for each PDF that has been downloaded for any Insights:

- Name
- Created
- Status
- Total Size
- Owner

Select a PDF and click Delete if you want to remove it for any reason. PDFs expire 24 hours after being generated.

Downloads

Choosing Administration > System Status: Downloads displays the Downloads page for accessing packet traces and PDFs of insights that you have downloaded.

The permissions necessary to see the Downloads page mirror those of the Capture Jobs page: at least Read-Only access to System configuration and Job configuration. To view the Packet Traces tab on the Downloads page, and to download packet traces, it is also necessary to have at least Read-Only access to Network packets.

The Downloads page provides these controls:

- Packet Traces tab – This displays the following information for each packet download:
 - Size Available For Downloads
 - Size Used For Downloads
 - Creation Time
 - Download Time Range
 - Filters
 - Status – This can be one of:
 - Initializing – The packet trace export is being created.
 - Running – The packet trace is in progress.
 - Ready – The packet trace is available, but has not been downloaded, yet. If the packet trace was larger than the configured Size Available For Downloads, the status will be Truncated, rather than Ready.
 - Streaming – The packet capture export is in the process of being downloaded to a user's browser.
 - Downloaded – The packet trace has been downloaded.
 - No Data – The packet trace contains no packets. This is distinct from the Error state in that nothing unexpected happened during generation of the packet trace.
 - Error – A problem occurred with the generation of the packet trace, causing it to be malformed.
 - Total Size – This displays the total size of the download. If the download is in progress, the total estimated size will be shown, along with the percentage of the download that is complete
- Insight PDF Downloads tab – This displays the following information for each PDF that has been downloaded for any Insights:
 - Name
 - Created
 - Status
 - Total Size
 - Owner

Note that Insight PDFs expire six hours after creation.

Traffic Diagnostics Insight

The Traffic Diagnostics Insight comprises these tabs:

- “General”
- “Flow Export”
- “ASA Module”
- “WTA Module”
- “DBA Module”
- “UCA Module”
- “CXA Module”

General

The General tab displays this data:

- Packet Rate
- Throughput
- Duplicate Packet Rate
- Connection Rate
- Monitoring Interface Hardware Drops
- Monitoring Interface Software Drops
- Analysis Packet Drops
- Capture Packet Drops

Flow Export

The Flow Export tab displays this data:

- Flow Rate to NetProfiler
- Rejected Flow Rate by NetProfiler

ASA Module

The ASA Module tab displays this data:

- Traffic to App Match Rate
- Traffic to HG Match Rate
- Unique HG Apps Match Rate
- IP Flow Write Rate

WTA Module

The WTA Module tab displays this data:

- Web Request Rate
- Individual Page Views
- New SSL Handshake Rate

DBA Module

The DBA Module tab displays this data:

- DB Transaction Write Rate
- Summarized DB Query Rate
- New DB Session Rate

UCA Module

The UCA Module tab displays this data:

- RTP packet Rate
- Call Rate
- Audio Channel Rate
- Video Channel Rate

CXA Module

The CXA Module tab displays this data:

- Management Interface Throughput –
- Reporting Agents –
- Reported Connections –
- Reported Flows –
- Discarded Connections (Agent Collector) – The number of flows discarded because the output queue is full.
- Discarded Connections (Agent Processor) – The number of flows discarded because the output queue is full.
 - Connections discarded (full queue) – number of flows discarded because the output queue is full.
 - Connections discarded (invalid report) – number of reports (agent bundles) discarded because the report is not valid (for example an unsupported format).
 - Connections discarded (invalid session) – number of sessions (within reports) discarded because the session is not valid (for example an empty session).

- Connections discarded (invalid): number of flows (within sessions) discarded because the connection is not valid (for example a null socket = IP=0, port=0)
- Discarded Connections (Flow Collector) – The number of flows discarded because the output queue is full.
- Discarded Connections (Flow Processor) – The number of flows discarded because the output queue is full.
 - Flows discarded (out of order) – number of discarded flows that are out of order.
 - Flows discarded (exceeding limit) – number of discarded flows that exceed maximum limit (internal limit based on model).
 - Flows discarded (full queue) – number of flows discarded because the output queue is full.
- Discarded Connections (Correlator) –
 - Report connections discarded (late arrival) – number of agent flows discarded for late arrival.
 - Report connections discarded (early arrival) – number of agent flows discarded for early arrival.
 - Report connections discarded (unmatched) – number of agent flows discarded for being unmatched (we were unable to match the agent flows with the probe flows).
 - End-to-end transactional flows discarded – number of end to end Citrix transaction flows discarded because output queue is full.
 - End-to-end summary flows discarded – number of end to end Citrix rollup flows because output queue is full.
 - Flows discarded (late arrival) – number of probe flows (from packets) discarded for late arrival.
 - Flows discarded (early arrival): – number of probe flows (from packets) discarded for early arrival.
 - Flows discarded (duplicate) – number of duplicate flows discarded.

SSL/TLS Insights

Click Insights > SSL/TLS: SSL/TLS Handshakes or SSL/TLS Certificates to display a corresponding Insight reporting the SSL/TLS activity observed by AppResponse 11. These are useful for investigating issues such as questions about the certificates being seen in network traffic, and for investigating failed or slow handshakes.

Note: Refer to “[SSL Decryption](#)” for instructions on enabling SSL/TLS for AppResponse 11.

For each SSL/TLS Insight, there is first an Input page, enabling you to constrain the set of handshakes or certificates that you want to view. If you click Launch without specifying any details, the resulting Insight will show the complete, unconstrained set of handshake/certificate activity. Note that for fields marked with a Search icon (magnifying glass), clicking on the icon can display a pulldown menu of known possible entries for that field.

Each Insight provides a summary of high level statistics for the activity, plus a set of tabs that enable you to view the displayed activity in terms of a particular characteristic such as Client IPs, SSL/TLS Version, Certificate Status, and Cipher Suite, among many others. In the SSL/TLS Handshakes Insight, right-clicking on a handshake enables you to download packets for it.

Note: Be conscious of the following behaviors:

- Certificate info is not extracted for TLS 1.3.
- TLS renegotiations are only if the session is decrypted.
- Certificate serial numbers are displayed in hexadecimal signed format (per OpenSSL convention):
 - Positive numbers (normal case) = 0xABABABABABABABABABABABAB
 - Negative numbers = -0xABABABABABABABABABABABAB

When converting from decimal to hexadecimal, be sure to use the signed version:

- Convert decimal unsigned to decimal .
- Convert signed decimal to hexadecimal.

DNS Insights

Three DNS-specific Insights are available, under Insights > DNS. These isolate pertinent DNS metrics and eliminate any need for manual packet analysis when investigating DNS-related issues.

- **DNS Servers** – This Insight summarizes DNS traffic across all visible DNS servers, including:
 - Response Time – The time elapsed from when a request was issued to when its response is received.
 - Response Time (P95) – The response time in the 95th percentile of queries.
 - DNS Timeouts – The number of queries that have timed out.
 - All Errors – Queries that had any unsuccessful error code.
 - DNS Servers – The number of DNS servers visible.
 - All DNS Traffic – A time series chart for all visible DNS servers. By default, the number of DNS timeouts is graphed.
 - Slowest DNS Servers table – A table of visible DNS servers with the worst response times.
 - DNS Servers With Errors table – A table of DNS servers with the most errors.
 - DNS Servers With Timeouts table – A table of DNS servers with the most timeouts.
- **DNS Server** – This Insight shows data for a specified DNS server:
 - Server IP Address – The IP address of the specified DNS server.
 - Response Time – The time elapsed from when a request was issued to when its response is received.
 - Response Time (P95) – The response time in the 95th percentile of queries.
 - DNS Timeouts – The number of queries that have timed out.
 - All Errors – Queries that had any unsuccessful error code.
 - DNS Clients – The number of DNS clients visible.
 - DNS Requests & Responses – Listed in a table.
 - Response Time True Plot – A time chart of the response times.
 - DNS Timeouts – The number of queries that have timed out.
 - DNS Errors – The number of times a DNS packet is malformed or abnormal in some way.
 - DNS Queries By Location – This lists the locations from which DNS queries originate.
 - Top Queried Domains – This lists the most queried domains.
 - OpCodes – This lists the DNS op codes issued to the server.
 - Query Types – This lists the query types.
- **DNS Transactions** – This Insight shows data for DNS transactions that match specified filter criteria:
 - Response Time – The time elapsed from when a request was issued to when its response is received.
 - Response Time (P95) – The response time in the 95th percentile of queries.

- DNS Timeouts – The number of queries that have timed out.
- All Errors – Queries that had any unsuccessful error code.
- DNS Servers – The number of DNS servers visible.
- DNS Errors – These are shown in a pie chart.
- DNS Response Time – This is shown in a time series chart.
- DNS Transactions tab – This shows the slowest DNS transactions.
- DNS Timeouts tab – This shows DNS timeouts and timed out DNS queries.
- Query Names tab – This shows the top query names and the corresponding DNS response times.
- Client Groups tab – This shows the top DNS client groups and the corresponding DNS response times.
- Client IPs tab – This shows the top DNS client IP addresses and the corresponding DNS response times.
- Server IPs tab – This shows the top DNS server IP addresses and the corresponding DNS response times.
- OpCodes tab – This shows the top op codes issued to the server and the corresponding DNS response times.
- Query Types tab – This shows the top query types and the corresponding DNS response times.
- GeoMap tab – This shows DNS requests and response times by location.

Navigator

Navigating Groups and Selecting Favorites

The Navigator enables you to view aggregated groups of traffic data and metrics built by AppResponse 11 from network traffic, application stream analysis, web transaction analysis and database analysis. You can create custom groups known as “**Favorites**” by selecting individual groups from all available AppResponse11 groups, table rows, and chart elements.

- A selected group is displayed in a table, the top table, with default metrics displayed in columns.
- A default chart appears below the top table in the workspace.
- Drill down using row expansion to see related subgroups of data and metrics.
- Build and share charts and tables in the workspace, which also can be saved and shared as Insights or Saved Reports.
- Right-click menus provide additional options for the top table and workspace data.

Favorites can assist you:

- in troubleshooting.
- in quickly building and sharing custom Insights or Saved Reports.

Note: If you want to view traffic data that you archived from an AppResponse 9.6.x appliance, open the archive VM in another browser window. You cannot access the archive VM from within AppResponse 11.

Important: Version 11.7.0 introduces a significant change in the handling of drilldown groups for the ASA feature. Refer to “[ASA Drilldown Changes Introduced in Version 11.7.0](#)” for details.

This section provides information on the following:

- “[Viewing a Group in Navigator](#)” on page 190
- “[The Navigator Top Table](#)” on page 190
- “[The Navigator Workspace](#)” on page 192
- “[Favorites](#)” on page 196
- “[Using Right-Click Menu Options in Tables and Charts](#)” on page 197
- “[Drill-downs](#)” on page 198

Viewing a Group in Navigator

To open a group using the Navigator drop-down list in the AppResponse 11 menu bar

1. Select a group by either:
 - Choosing Navigator in the menu bar and selecting a group under Application Stream Analysis, Web Transaction Analysis, or Database Analysis from the drop-down list.
 - Choosing More....
If you chose More... the Navigator page opens and displays all of the available groups including Advanced groups and Favorites in a navigation pane. Select a group from the list in the navigation pane.
2. The selected group appears in the top table, next to the navigation pane.
 - The top table is sorted by the default Top By: metric, displayed above the table.
 - In the workspace below the top table, AppResponse 11 displays a default chart, typically a time-series chart.
 - Once a group is opened the default chart and any new charts that you create remain in the workspace.

Clicking a new group in the navigation pane opens that group in the top table. This new top table data can be added to an existing chart or table and can be used to create new charts or tables in the workspace. This capability enables custom Insights to be built using the Navigator workspace.

Note: Groups marked with the "HD" icon provide access to all associated traffic, regardless of whether it is TCP or UDP.

Note: To maintain any existing charts with their data, lock each chart or table to preserve their data *before* clicking a group in the navigation pane. For more information see [“Adding Top Table Rows to a New or Existing Chart or Table” on page 193](#) in this section.

Charts in the workspace are kept until a new group is opened using Navigator in the AppResponse 11 menu bar. When a different group is selected in the navigation pane, the data in existing charts and tables is replaced by data from the newly opened group, unless the chart or table is locked. For more information see [“Adding Top Table Rows to a New or Existing Chart or Table” on page 193](#) in this section.

You can remove added charts or tables by:

- Choosing **Revert to Default Chart** from the workspace toolbar.
- Hovering over the top right corner of a chart or table and clicking **x**.

The workspace charts can be saved as an Insight or a Saved Report by clicking the Save button in the workspace toolbar. See [“Save Insight” under “The Navigator Workspace” on page 192](#) for more information.

The Navigator Top Table

You can configure the top table’s contents when viewing a group as follows:

- Select a current time interval or specify a time interval of interest. The Navigator time interval is used to calculate the data and metrics in the top table rows and workspace charts and tables.
- View the selected group organized by a default topping metric or one that you choose.
- Select the table columns (metrics) and their order.
- Sort the a table by a column you select.
- Expand a table row to drill down using data from subgroups related to the group.

The Top Table Toolbar

The tools available are determined by the content in the top table. The standard tools are described below:

- **Limit**—Specifies the number of top-level rows displayed in the top table.
- **Top By**—Select the metric used to order the top table rows, from highest to lowest metric value, in the specified time interval.
- **Time interval**— The current date and time are shown against a green background. Select a predefined current time interval (15m, 1h, 1d, 1w, 1m) or click the pencil or in the displayed time interval to specify the time interval in units of one minute or greater. The Navigator time interval is used to calculate the data and metrics in the top table rows and workspace charts.
- **Create New Favorite**—Click the star icon to create a new Favorite. For more information, see [“Favorites” on page 196](#).
- **Column Chooser**—Click the columns icon in the top right corner of the top table.
 - The Column Chooser window opens, displaying the set of available columns and the set of selected columns. The available columns are grouped by metric type.
 - Typing in the text panel above the available columns filters the list of column names that are shown, based on which column names contain a match for the text you entered.
 - Clicking the Filter button enables you to specify one or more modifiers to associate with the displayed available columns, such as a unit, a direction, or some other characteristic.
 - To move a column name from one set to the other, select it and click the appropriate arrow button to move it.
 - Re-order a column in the selected columns set by clicking the handle at its left and dragging and dropping the column to a new place in the list.
 - Click the pencil icon (Edit) for a selected column to specify its units.
 - For some columns, you have the option of displaying the data as either a number or a bar. Some columns support the display of stacked bars.
 - Click the Reset to Defaults button to revert the set of selected columns to the system defaults.
- **Information**—Click the “i” icon to display a pop-up Information window summarizing the selected group.

Additional tools are available in the top table toolbar when a Favorite is selected in Navigator:

- **Add**—Enables selection of a group from all available AppResponse groups to add to the Favorite.

- **Delete**—Removes a selected group from the Favorite.
- **Trash Can**—Deletes the Favorite.

The Navigator Workspace

The workspace is the area below the top table. Use the workspace to display top table data in charts and tables that you select. A workspace can be saved and shared as an Insight or a Saved Report. Selecting a group in Navigator opens a default chart, typically a time-series chart, in the workspace.

Note: The workspace also uses the Navigator time interval for charts or tables. Changing the Navigator time interval recalculates the table rows as well as the workspace charts and tables.

The Workspace Toolbar

The following widgets and tools, from left to right, are available in the workspace toolbar. Hover your mouse over an icon to see a description of what it does:

- **Revert to Default Chart**—Replaces the current workspace with the default chart for the group in the top table. Any changes or additions to the current workspace not saved are lost.
- **Load Insight icon**—Choose an existing custom Insight to display in the workspace. Built-in Insights are not loaded this way.
- **Save Insight**—The workspace can be saved as an Insight in two different formats:
 - **Insight**—Insights you create also can be revised and renamed in the Navigator workspace.
 - **Saved Report**—A Saved Report is a one-time image of a chart's contents.
- **Top Check Box**—Selects what group data in the top table is displayed in a new chart or table.
 - **Checked**—A chart or table shows only the topped table rows. The charts and tables that support topped data are available for use.
 - **Unchecked (default)**—A chart or table shows only the selected table rows. All supported charts and tables for the group are available.
- **Chart icons**—The type of group in the top table determines the chart icons displayed. Other chart options may be available when a different type of group is selected. Charts may include time-series charts, multi-metric time series charts, pie charts, bar charts, TruePlot (scatter) charts, waterfall charts, grid tables, sparkline charts, and flip charts.
- **Workspace format**—Click an icon to choose how charts are displayed in the workspace. The default is a tabbed folder. The choices are:
 - in a tabbed folder, one chart or table per tab.
 - one chart or table per line.
 - two charts or tables per line.
 - three charts or tables per line.

Controlling Chart and Table Updates

A chart or table can be unlocked (default) or locked to control when the chart or table is updated.

- If unlocked, new selections in the top table are automatically added to a chart or table.
 - If a top table row selection is cleared, the data is removed from unlocked charts or table.
- If a chart or table is locked, new selections in the top table are ignored while unlocked charts and tables are updated.

Locking or Unlocking a chart or table

1. Hover over the top-right corner of a chart or table to see the lock icon.
2. Click the lock icon to lock or unlock the chart or table.

Adding top table data to an unlocked chart or table

1. Hover over a top table row and click its selection box.
2. Click the selection box of additional top table rows to add them to the chart.

Adding top table data to a locked chart or table

1. Select the row or rows to add.
2. Click the grab icon at the beginning of a row to drag the rows into an open chart.
3. Drop the rows over **Append** or **Replace** to add to or replace the existing chart data.

Adding Top Table Rows to a New or Existing Chart or Table

Table row data can be added as a new chart or table or the data can be added to multiple existing charts and tables, both unlocked and locked.

Creating a new chart or table in the workspace

1. Right-click on the group name of a top table row to open a pop-up menu of options.
2. Choose Add to Workspace.
3. Select the radio button next to New Chart/Table.
4. Choose a chart or table from the list presented.
5. Click OK to add the chart to the workspace or Cancel to close the window.

A new chart or table is added to the workspace with the selected table row data.

Adding to an existing chart or table in the workspace

1. Right-click on the group name of a top table row to open a pop-up menu of options.

2. Choose Add to Workspace.
3. Select the radio button next to Current Chart/Table.
4. Select Show Locked to include existing charts or tables that are locked in the list.
5. Select the charts and tables where the data is to be added.
 - To select multiple charts or tables, hold the CTRL-key down when selecting.

The table row data is added to the selected existing charts or tables.

Using Settings to Select Chart Data and Appearance

The top table rows displayed by a chart when it opens are set by default. Hover over the top-right corner of a chart to see the settings icon. The settings icon opens an edit widget window where you can select and edit existing data (groups). You also can choose or modify their appearance.

Selecting or Editing Data

Use the Data screens to choose from all of the group data and metrics available in AppResponse 11.

1. Click the settings icon in the top right corner of the chart.
2. Choose **Data** in the left column of the Edit Widget window. The groups and their paths in the current chart are displayed beneath the Add button.
 - To edit an existing group hover over the row and click the pencil icon that appears.
 - To delete an existing group hover over the row and click the 'x' that appears.
3. Under Widget Type
 - Select Top Groups to use the top group in a group you add. You specify the Top By metric and the number of rows (the limit).
 - Select Specific Groups to add one or more groups.
4. Click **Add**.
5. The Select/Filter Group window opens. Click **Add**.
6. Select the group or subgroup that you wish to add from the list. Make your selection and click **OK**. If a label group containing no data is selected, the OK button at the bottom of the list is disabled.
7. The Select Filter/Group window returns, now showing the path to the group you selected.
8. Click each pencil icon under Value to enter the filter value(s) needed to identify the group you want to select.
 - For applications, first choose the application type from the drop-down list.
To specify an application by protocol and port, begin by typing the protocol in the filter box and select it from the list that appears. Next, enter the port number.

To specify other applications, choose the application type and begin typing the application name in the filter box. A list of applications matching the name appears below the filter box. If you don't see the application on the list, type additional characters in the filter box. Select the application you want to add.

9. When finished, click **OK** to save the changes, **Cancel** to discard them.

Selecting or Modifying Appearance

Use the Appearance screen to specify how chart or table data is displayed, for example, the chart title, a legend, and the scale for the chart.

1. Click the settings icon in the top right corner of the chart or table.
2. Choose **Appearance** in the left column of the Edit Widget window. A table of the available settings for the chart or table is displayed.
3. Enter and choose the settings you want for the chart's appearance.
4. Click OK to view the revised chart in the workspace.

Adding a Correlation Chart For Comparing Two Metrics

When working in the Navigator or when creating a custom Insight, you can add a Correlation Chart to plot and compare two metrics of your choosing.

To add a correlation chart:

1. Click the Add Correlation Chart widget button in a Navigator pane tool bar.
2. A new Correlation Chart pane appears.
3. In the new Correlation Chart pane, click Change Widget Settings to display the Edit Widget dialog.
4. Select the metric and corresponding unit to display on the chart's X-axis and Y-axis.
5. Specify any other options that will define the chart, such as legend location, scale, etc.
6. Click OK to finish defining the correlation chart.

Filtering Using Tags

You can filter the contents of Navigator tables based on a number of tag types:

- Host groups
- Apps
- Host (IP)
- Host pairs (IP pairs)

Use the Apply Filter dialog to select one or more of these tags as filters; clicking the Filter Drilldowns checkbox will filter all the rows displayed in the tree table. The filtering of records applies only to groups/drilldowns that are taggable; for resources that cannot be tagged, all the relevant records are displayed.

In charting widgets, tag information is displayed in the tooltip.

Favorites

Favorites are user-selected groups that can be assembled from all available AppResponse 11 data groups. A data group can be added to a Favorite from a top table row selection or a chart element. Favorites can be used in troubleshooting workflows and building custom Insights.

A Favorite can be saved and revised. A group and all of its subgroups are saved, along with any open charts. Each saved Favorite is listed under Favorites in the Navigator navigation pane, and is listed in the Manage Favorites page.

Creating a Favorite

You can create a Favorite using any of these methods:

- Select a group in the top table and click the star icon in the upper right corner of the top table toolbar to display the Create New Favorite dialog. Using this method, you can specify:
 - the name of the group (required).
 - a description (optional).
 - any tag (optional). Use a comma-separated list for multiple tags.
 - access by others: public (read-only), shared, or private. For shared files, read-only or read/write access can be assigned by role.
- Right-click a group name in a table or an element in a chart and choose Add to Existing Favorites or Create New Favorite. Using this method, you can specify:
 - if a new Favorite is created or if the selected group is added to an existing Favorite, chosen from a list. New Favorites are assigned a standard name with a sequence number, (Favorites-*x*).
 - what data in a group is added to the new or existing group.
- Click Navigator > Actions:New Favorites in the menu bar to display the New Favorite page. Click Add to display the Select Group dialog and begin picking groups for inclusion in the new Favorite.
- Click Navigator > Actions:Manage Favorites in the menu bar to display the Favorites page, listing all existing favorites. Click Add on the Favorites page to display the New Favorites dialog and begin defining a favorite.

Adding or Deleting Groups in a Favorite

One way to add or delete groups from a Favorite is to open the Favorite in Navigator.

1. Click Navigator and choose More...

2. In the navigation pane under Favorites, choose the Favorite you want to change.
3. The top table toolbar has two icons on the left-hand side: Add and Delete.
 - Clicking Add opens the Select Filter/Group screen. Click add here and all AppResponse 11 groups are available for selection.
 - To remove a group, select the table row and click Delete.
4. Click the Save icon to the right of the time interval.
5. Select Save or Save As to save

An alternative way to add a group to a Favorite uses the right-click menu.

1. Right-click a group name in a table row or a chart element.
2. Select Add to Existing Favorites or Create New Favorite to display the corresponding dialog.
3. Select the existing Favorite to which to add, or type the name of the new Favorite.
4. Choose the group you want to add to the Favorite and click OK.

Deleting a Favorite

1. Select the Favorite in the navigation pane to display it in the top table.
2. Click Delete to select one or more groups to remove from the Favorite.

Using Right-Click Menu Options in Tables and Charts

Use the right-click menu options for group names in a table and selections in a chart. Right-click options, depending on the item clicked, can include:

- **Add to Existing Favorites**—Right-click a group name in a table row or select a chart element to add it to add it to an existing Favorite. Select the data to add.
- **Create New Favorite**—Right-click a group name in a table row or select a chart element to use it to create a new Favorite. Select the data to add.
- **Add to Workspace**—Right-click a group name in a table row or select a chart element to add it to an existing chart or create a new chart in the workspace.
- **(Open Insight)**—Opens an Insight based on the type of item right-clicked.
- **Download packets**—When packets are available, display the Packet Export dialog to save packets as a PCAP trace file to your local system (refer to [“Downloading Packets From a Capture Job”](#) for a detailed description). If there is more than one capture job defined, choose the capture job with the packets from the displayed list.
If a sweep (click-drag) is made in a time-series chart, right-clicking a chart item in the sweep downloads only packets in the selected time interval.
- **Launch Browser**— When a URL is selected a browser window may opened if you approve.
- **Launch ‘Name’**—An individual or group Insight is displayed for the selected item.

- **Launch SteelCentral Packet Analyzer Plus**—Sends packets (when packets are available) to Packet Analyzer Plus on the local system. Packet Analyzer Plus opens and adds a new probe if the AppResponse is not already a probe. The packets are sent and a default view is applied by Packet Analyzer Plus.
If a sweep (click-drag) is made in a time-series chart, right-clicking a chart item in the sweep sends only packets in the selected time interval to Packet Analyzer Plus.
- **Show Conversations**—The IP Conversations group opens, filtered by the right-clicked group. The filter is shown in the table toolbar.
- **Show Individual Page Views**—The Individual Page Views group opens, filtered by the right-clicked group. The filter is shown in the table toolbar.
Note that, when downloading packets for an individual SSL page view, handshake packets will be downloaded, as well. This can result in the download of objects in addition to those associated only with the specified page.
- **Show TCP Connections**—The TCP Connections group opens, filtered by the right-clicked group. The filter is shown in the table toolbar.
- **Chart**—Opens an Insight based on the type of chart element selected.
- **View Definition**—Edit the definition of the selected object.
- **Use In Definition**—Create a new object definition or use the selected item in an existing object definition.
- **Launch SteelCentral Transaction Analyzer**—Choose Trace Explorer, Tree View, or App Doctor.
- **Search**—Display the Search Results page.

Drill-downs

Expanding a row in a group displays associated subgroups and their data and metrics. Symmetrical groups provide multiple paths to the same data, for example, you can start with an application and drill down to related TCP Server Groups or you can start with a TCP Server Group and drill down to the applications.

1. Choose a group in the navigation pane.
2. Expand a row in the top table to see associated subgroups.
3. Continue to drill down until you find a subgroup of interest.
 - Use a right-click menu choice for further investigation, if available.
4. Open a chart in the workspace to display the top table entries of interest.
5. Click a chart element or click and drag to select a time interval in the chart and right-click chart elements of interest.
6. From the right-click menu, choose the next step in your analysis.

Right-click Options

Right-click a group name or chart element - if drill down is supported a menu appears with available options. Options can include:

- **Add to Existing Favorites**—Right-click a group name in a table row or select a chart element to add it to add it to an existing Favorite. Select the data to add.
- **Create New Favorite**—Right-click a group name in a table row or select a chart element to use it to create a new Favorite. Select the data to add.
- **Add to Workspace**—Select to add a group to a new or a current chart or table in the workspace. Next, select the new chart or a current chart for the group.
- **Download Packets**—When packets are available, save packets as a PCAP trace file to your local system. If there is more than one capture job defined, choose the capture job with the packets from the displayed list.
- **Launch “Individual or Summary Insight”**—Launches the individual or summary Insight.
- **Launch SteelCentral Packet Analyzer Plus**—Sends packets (when packets are available) to Packet Analyzer Plus on the local system. Packet Analyzer Plus opens and adds a new probe if the AppResponse is not already a probe. The packets are sent and a default view is applied by Packet Analyzer Plus.
- **Search**—The selected item is searched in AppResponse and the results are displayed. Click links in the search results to view more detailed information on the selected item.
- **Show Individual Page Views**—The Individual Page Views group opens, filtered by the right-clicked group or chart element. The filter is shown in the table toolbar.
- **Show TCP Connections**—The TCP Connections group opens, filtered by the right-clicked group or chart element. The filter is shown in the table toolbar.
- **This Application**—Opens an Insight based on the group or chart element selected.
- **View Definition**—Open the configuration page and Edit dialog for the selected object type and instance.
- **Chart**—Display a dedicated chart to examine values for the selected object. Depending on the object, a variety of chart types are available, including:
 - Time Series
 - Response Time Composition
 - Pie
 - Bar
 - Sparklines
 - Multi-Metric Time
 - Grid Table
 - Flip Table
- **View Definition**—Edit the definition of the selected object.

- **Use In Definition**—Create a new object definition or use the selected item in an existing object definition.
- **Launch SteelCentral Transaction Analyzer**—Choose Trace Explorer, Tree View, or App Doctor.
- **Search**—Display the Search Results page.

GeoMap Chart

The GeoMap chart widget is available in Navigator for some WTA and CXA views, enabling you to show geographical origins for some data. The GeoMap chart is a choropleth map, enabling you to display specified data using a color gradient on a map.

There is a GeoMap icon in the tool bar.

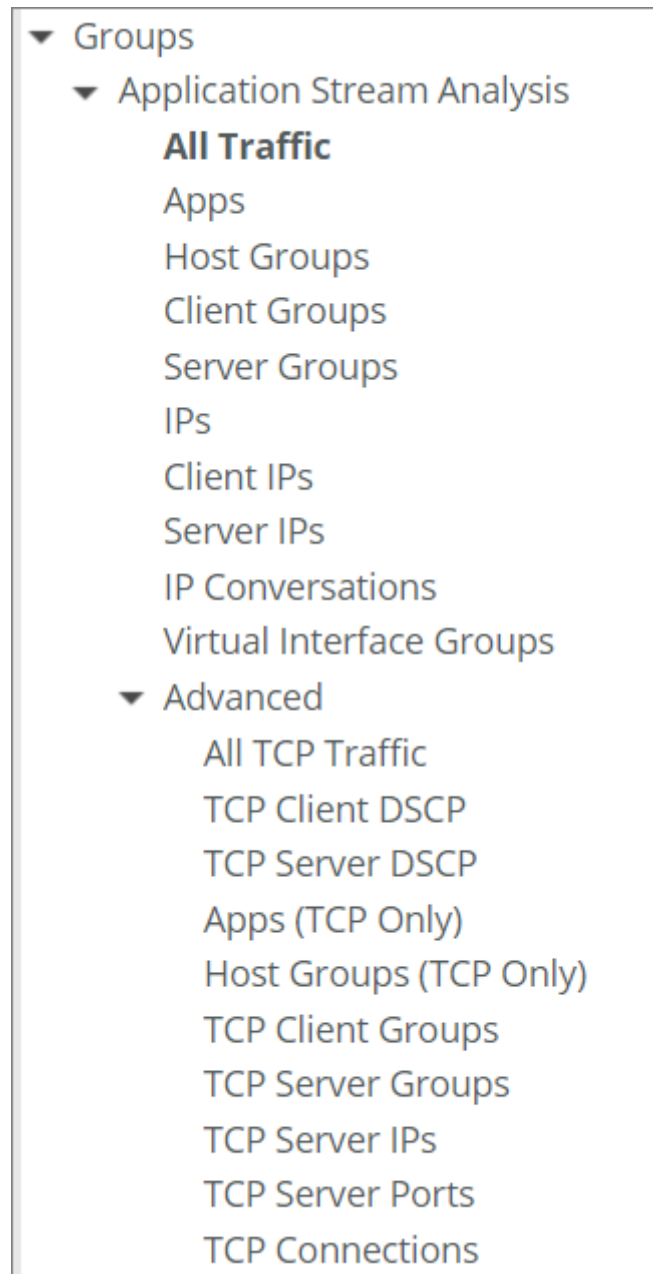
You can customize the GeoMap widget using the Edit Widget dialog. Along with the standard widget settings, the GeoMap widget supports the following settings:

- **Color column and unit**—The column to use to color the map and its associated unit.
- **Auxiliary columns**—The columns to display in the tooltip. When the user specifies auxiliary columns, they will be displayed in the tooltips above the map.
- **Scale Type**—Absolute or Relative. The user can specify whether they want to specify an absolute min and max value for the gradient or whether they want to have the gradient computed between the color columns min and max value.
- **Thresholds**—The minimum and maximum value for the absolute gradient.
- **Gradient Colors**—The colors to use for the gradient.

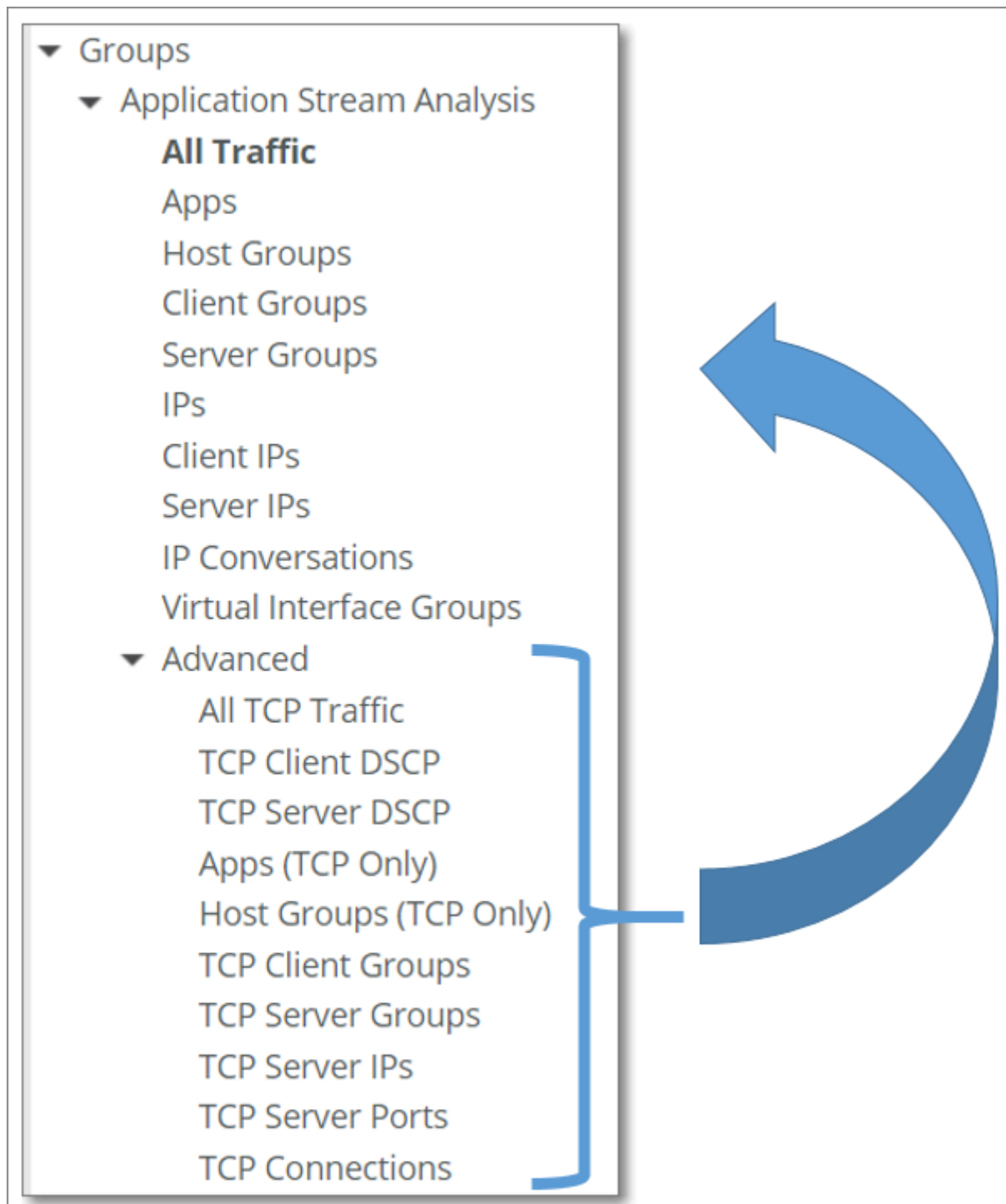
ASA Drilldown Changes Introduced in Version 11.7.0

This topic explains an important change in the drilldown start groups available for the ASA feature in the Navigator.

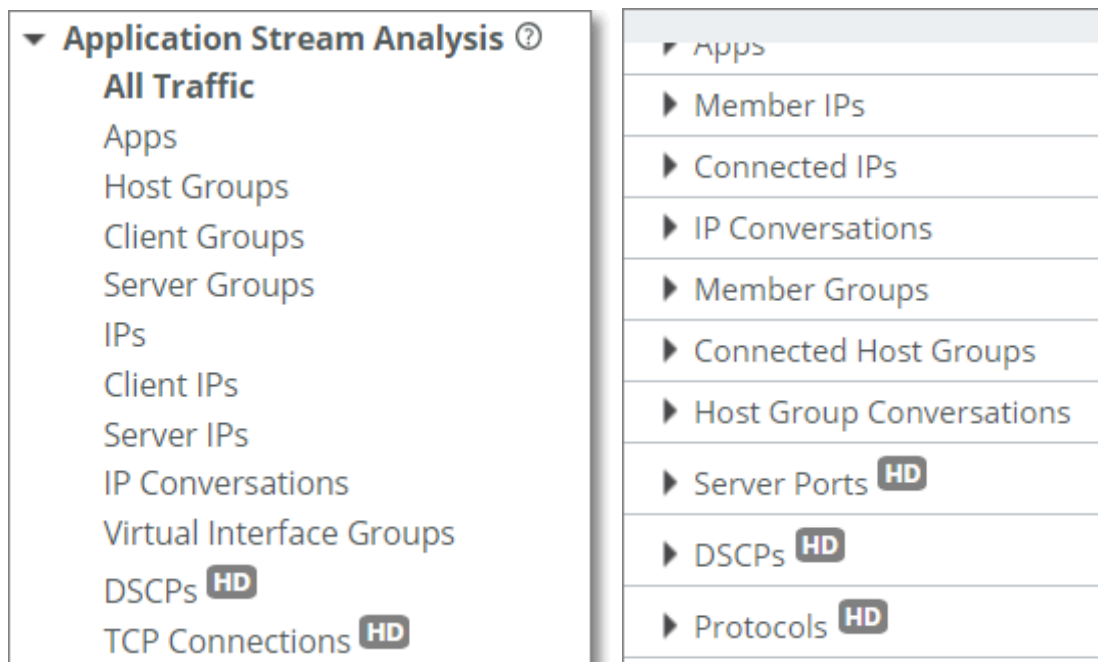
Prior to Version 11.7.0, drilldown start groups for ASA in Navigator were available in the following manner:



As of Version 11.7.0, the drilldown start groups that were available under Advanced have been merged with the regular (non-Advanced) groups:

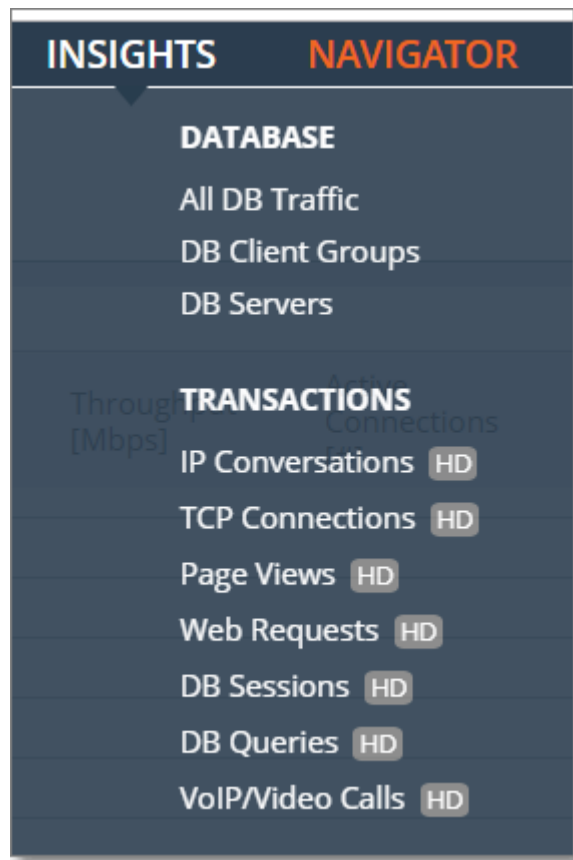


The unified drilldown start group “tree” in Version 11.7.0 is what you see in the left pane of the Navigator. Note that groups that used to be present under Advanced now are tagged with the “HD” icon (indicating High Definition) to indicate that the metrics for these groups are derived on-demand from un-topped transaction data.



As shown above, the former Advanced drilldown start groups mostly have become drilldown groups for Apps, Host Groups, Client Groups, and Server Groups, as shown at right, above.

Beginning in Version 11.7.0, all transaction data-based Insights also are visually tagged with the “HD” icon wherever they show up in the UI, like in the menu shown below:



Transaction Searches

Click Transactions in the menu bar to search for individual transactions of several types: page views, web requests, DB queries, DNS transactions, and TLS handshakes. Right-click on a search result to display a pop-up menu with relevant commands for the result. You can right-click on a result in either the scatter plot or the results list.

For each transaction search type, you can specify a constraint in the criteria builder panel, then click Search. Click in the panel to show autocomplete suggestions as you type; for some elements, such as a name or IP address, you may need to type what you want without assistance from the system. Note that multiple constraints are supported only with the "AND" operator, not with the "OR" operator. The context-based widgets in the Refine Results By pane at the left provide a convenient means of filtering the search results, based on one or more characteristics.

Note: Searchable transaction data is collected only after updating to Version 11.11.0 and later. Following the update, searching for transaction data in a time period prior to that update (prior to the collection of searchable data) will not return results.

Web Transaction Analysis

Page Analysis Configuration

You enable and set up Web Transaction Analysis Module (WTA) on the Administration > Feature Settings: Web Page Analysis UI page.

Data Collection Options

Option	Notes
Enable Page Analysis	<p>When enabled, the appliance collects web page analysis data for the specified ports and IP addresses.</p> <p>Before you enable Page Analysis, mask out all private parameter values in any HTTPS traffic that might get decoded, as described in “Information Privacy” on page 217.</p> <p>WARNING—There is no way to mask private data after it is saved on an appliance. For this reason, you must specify all sensitive parameters <i>before you enable Page Analysis</i>.</p>
Ports	Collect data for the specified ports only.
Server IP Addresses	<p>Collect data for a subset of IP addresses or select check box for all IP addresses.</p> <p>Note—Collecting web page data can be highly resource-intensive, especially on very large networks with a lot of web traffic. To minimize the performance impact on the appliance, it is good practice to limit Page Analysis to ports and hosts of interest only.</p>
Default Slow Page Threshold	<p>The appliance uses this threshold, in seconds, to determine metrics such as Slow Pages and Slow Page Rate.</p> <p>Range: 1 - 600; default is 5 seconds.</p>
Enable SSL Decoding	<p>When this option is selected, AppResponse 11 decodes web-over-SSL traffic on the specified ports and server IP addresses. SSL keys are managed at Administration > System Settings: “SSL Decryption,”</p>
“Enable SOAP Processing”	
“Advanced Options”	
Unique User Definition	Configure the parameters used to identify a unique user.
GeoMap Private Data	Import a CSV file to map private IP addresses to locations.

Enable SOAP Processing

This option is useful for analyzing SOAP transactions. When this option is enabled, the appliance does the following:

- Translates every discrete SOAP transaction into a separate Page View (without SOAP processing enabled, a page view might include two or more SOAP transactions)
- Includes the SOAP method in the URLs shown for page families and individual page views in the Page Analysis insights (for example,
`http://webapp.com/TradeProcess/Process.aspx [method:ProcessTrade]`)

Note the following:

- This option requires additional computing resources and might slow down performance on the appliance.
- Normally, you should enable this option only if your appliance is monitoring back-end SOAP traffic and not front-end browser traffic.
- You cannot include SOAP methods in URLs when you define web applications.

Advanced Options

AppResponse 11 can provide a close approximation to the number of unique users of web applications.

Unique User Definition

Users are identified using the user and session tracking configurations. The precision of the count is estimated as the number of unique IDs grows larger. For example, if there are thousands of unique IDs, the count would not be the exact number as when only a single unique ID is tracked.

When selecting a unique user definition, keep in mind the following:

- The default unique user definition settings provides the most granularity when tracking unique users of web applications.
- You can remove the User-agent to combine all pages from the same computer instead of splitting by them by browser.
- You can switch from Originating IP to Client IP to group user pages when someone is using the same account on multiple computers behind a common client IP address.

AppResponse 11 creates two metrics with unique users:

- **Unique Users**—A unique user is defined under Advanced Settings and identified from the user and session tracking configuration.
- **Affected Unique Users**—A user is deemed 'affected' for a page if at least one of the web applications associated with that page is identified as slow.

The following AppResponse 11 insights include unique users:

- Individual: Web App
- Summary Web Apps
- Summary: Page Views

- Individual Web User Group
- Summary: Web User Groups

GeoMap Private Data

If you want to collect geographic information on private network IPs, you can import a private GeoMap CSV file with the mapping information. Do this by clicking the Import Configuration button under Advanced Options in the Page Analysis Configuration page Data Collection Options tab. There are buttons for exporting and deleting the GeoMap configuration, also.

Following is an example CSV file; the format is: IP Address Range, Continent Code, Country Code, Region Code, Latitude, Longitude (Latitude and Longitude are optional).

```
version:1
3ffe::0200:ff:fe00:7,NA,US,MD,39.4370002746582,-76.78179931640625
3ffe::300:ff:fe00:9c,EU,RU,TUL,55,73.4000015258789
10.38.25.116,NA,US,MD,34.5,23.3
10.128.0.0-10.128.3.3,AS,IN,KA,23.4,12.3
```

IP address ranges can be specified for both IPv4 and IPv6, and can be specified in the following ways:

- Single address (192.168.1.1)
- Range using "-" (192.168.1.1-192.168.1.10)
- Range using CIDR (192.168.1.0/24)

GeoMap location codes use the continent, country, and subdivision identifiers defined in ISO 3166-2. Refer to https://en.wikipedia.org/wiki/ISO_3166-2 for a list of supported country codes that also provides access to the relevant subdivision information for each country.

Installing a WTA Configuration from an Upgraded AppResponse 9.6.x Appliance

Customers using a 2200, 3300, or 3800 appliance or a VMon or v2000 virtual appliance with WTA can evaluate their WTA configuration by running an admin CLI command. The output of this command includes a determination of whether the 9.6.2 WTA configuration uses any custom configurations. If there are no custom configurations, the WTA configuration can be done using the AppResponse 11.1.0 (or later) Web UI at Administration > Web Transaction Analysis: *Page Analysis* or *Information Privacy* or *User Session Tracking*.

If a custom WTA configuration is found, you can create a diagnostics bundle that you include when you file a support case for AR9-->AR11 WTA Transition Assistance with Riverbed Support. WTA engineers will analyze the diagnostics bundle and send you a configuration file that is an equivalent or close-to-equivalent translation of the AppResponse 9.6.2 WTA configuration. For more information, see the AppResponse 9.6.2 release notes.

Importing a WTA Configuration File

1. Go to Administration > Analysis: Page Analysis in the AppResponse 11 web UI.
2. Click **Import** in the top-right corner of the page header.

3. Specify or choose the name of the Riverbed Support configuration file in the window that opens.
4. Click **Import**.
5. WTA is configured on AppResponse 11.

Page Analysis Rules: Customize How WTA Constructs Page Views

Custom Page Analysis rules enable you to customize how WTA processes specific types of web objects. A Page Analysis rule includes a web-object filter and the set of actions to perform on objects that match this filter. Examples of actions you can specify include:

- Exclude matching objects from WTA
- Include matching objects in one and only one Page View
- Start a new Page View when a matching object is observed

This section discusses the following:

- [“Custom Page Family Rule Settings” on page 213](#)

Custom Page Analysis Rule Settings

To create or edit Page Analysis rules, go to Administration > Web Transaction Analysis: Page Analysis. Then go to Custom Page Analysis Rules.

Setting	Notes
Name	
Enable Rule	
Page Match Criteria	Define a web-object filter so the rule is applied only to objects that match the selected criteria (URL Patterns, Content Values, and/or Advanced).
URL Patterns	<p>Apply the rule only to objects that match a URL pattern in the list. For example:</p> <p><code>www.riverbed.com/*</code> matches both</p> <ul style="list-style-type: none"> ■ <code>http://www.riverbed.com/*</code> and ■ <code>https://www.riverbed.com/*</code> <p>Include the protocol prefix (<code>http://</code>, <code>https://</code>, or <code>http*://</code>) only if you specifically want to match only http or only https. For example:</p> <p><code>http://*popup-ad-click.com/*</code></p> <p><code>https://*redir.adap.tv/redir*</code></p> <p><code>http*://*redir.adap.tv/redir*</code></p>
Content Values	Apply the rule only to objects with matching name/values in the URL or HTTP/HTTPS payload data.
Advanced	
Settings	Criteria for grouping individual “Content Values” pages into families. You can group pages by “Truncated URL” and/or .
Stop processing object after this rule is applied	<p>If you have multiple Page Analysis rules enabled, the appliance will apply each rule to the object (from first rule in the list to last) until</p> <ol style="list-style-type: none"> 1. It applies a rule with this option selected, or 2. All enabled rules are applied. <p>If you enable multiple rules at the same time, an object might match multiple rules and be included in multiple Page Views. If multiple rules are applied, a subsequent rule might override actions applied as a result of a previous rule.</p>

Setting	Notes
Drop Object	If an object matches this rule, exclude it from WTA analysis.
Additional Actions:	
Start new page with this object	This setting is useful for web objects that correspond to web pages but do not have commonly recognized web-page file types or extensions (*.html, *.jsp, *.asp, and so on). In this case, define the URL patterns, content values, and/or advanced options to filter on these nonstandard web page objects. Make sure that the rule filters <i>on the page objects themselves</i> and not simply on objects that might be included in these pages.
Allow pages that start with an unobserved redirect	<p>These options are useful when you want to track certain types of web objects that WTA ignores by default. Depending on your web traffic and monitoring goals, you might want to enable one or more of these actions for all pages, or only for pages of interest.</p> <p>One possible workflow you might be use is to</p> <ul style="list-style-type: none"> ■ Enable one or more of these actions on all pages. ■ Monitor the WTA results for instances of "unobserved-redirect," "zero-length content," and/or "unrecognized-file-type" pages. ■ If these pages are cluttering up your WTA results, apply the actions only to web pages that meet specific page rules (as defined by URL patterns, content, and/or advanced filtering).
Allow pages that start with zero-length content	
Allow pages that start with an unrecognized content type	
Get originating ID from this IP header field	This setting is useful for web traffic where the originating IP is in a header field other than X-Forwarded-For.
For web pages that have missing or incomplete responses	<p>By default, WTA ignores any page view in which the page response (*.html, *.jsp, *.asp, etc.) is missing or incomplete. You can select one of the following actions to override this behavior:</p> <ul style="list-style-type: none"> ■ Do not record page—Ignore every page in which any response for any object is missing or incomplete ■ Do not record missing/incomplete objects—Track pages with missing/incomplete responses but do not track these objects ■ Record missing/incomplete objects—Track pages with missing or incomplete responses and track these objects

Page Family Rules: Customize How WTA Constructs Page Families

Custom Page Family rules enable you to customize how WTA combines Page Views into Page Families. A Page Family rule includes a page-view filter and the set of rules to group matching Page Views. You can define Page Family rules to

- Define user-friendly names (such as “Dropbox Notifier Service” or “Windows Update”) instead of long strings derived from the page URLs.
- Truncate the URL strings included in Page Family names
- Include specific URL parameters, SOAP values, and other types of Page View content in Page Family names

This section discusses the following:

- [“Custom Page Family Rule Settings” on page 213](#)

- [“Recommendations for Page Family Rules” on page 213](#)
- [“Custom WTA Metrics/Columns” on page 216](#)

Custom Page Family Rule Settings

You can specify the rules AppResponse 11 uses to create page families in Custom Page Family Rules at Administration > Web Transaction Analysis: Page Analysis. You can define up to 500 Page Family rules. For each page view it observes, WTA does the following:

- Iterates through the list of Page Family rules on the appliance.
- If it finds a matching rule, it assigns the view to the corresponding Page Family.
- If no matching rule is found, it assigns to a Page Family based on the page URL (default behavior).

For best results, read and observe the following recommendations for page family rules.

Recommendations for Page Family Rules

- The order in which the rules are listed can determine the Page Family to which a specific individual page view is assigned. If a specific page view matches multiple rules, it is assigned to the first (topmost) rule listed in the Custom Page Family Rules table - the first matching rule wins.

Important: When using match or replace URL Parameters in Advanced Options under Truncated URL, if there are two Page Family Rules defined using the "All Pages" Page Match Criteria, only the first (topmost) such page family rule is used, as any web page matches "All Pages." If you have multiple match or replace rules that you want to perform you can just put them on separate lines in the same rule in the Advanced Options section.

- In general, it is good practice to include more specific rules higher in the list and more general, all-inclusive rules lower in the list. Otherwise you might find that all views are assigned to the general rule ("US logins") rather than to more targeted rules ("New York logins") lower in the list.
- Define or edit your Page Family rule based on criteria that makes sense to you.
- Riverbed recommends a layered approach to defining Page Family rules:
 - Define your Web Apps to group pages into high-level groups.
 - Navigate through your page tables and drill down into individual pages.
 - Examine the URLs of important individual page views and see how you might want to further group them into families.
- Any changes to your Page Family rules are applied only to page views observed *after you save your changes*; older views are not affected.

Setting	Notes
Name	Assign a name that describes or helps in organizing the rules. The name has no bearing on how the rule functions or what the rule does.
Enable Rule	
Page Match Criteria	Apply the page family rule only to pages that match the following criteria. Leave these fields blank to apply the rule to all pages. For more details on Page Match Criteria, see the three sections on Page Match Criteria under "Web" in the Administration > Definitions: Applications Help.

Setting	Notes
URL Patterns	<p>Apply the rule only to pages that match a URL pattern in the list. Each entry should include the protocol prefix (<code>http://</code>, <code>https://</code>, or <code>http*://</code>). Examples include:</p> <pre>https://*mycompany.com/*calendar*</pre> <pre>http://www.example.com/*.aspx</pre>
Content Values	Apply the rule only to pages with matching name/values in the URL or in the HTTP/HTTPS headers or payloads.
Advanced	
Group Pages By	Criteria for grouping Page Views into Page Families. You can group pages by “Truncated URL” and/or “Content Values” .
Truncated URL	<p>Group page views into families based on Truncated URLs.</p> <p>These settings define the URL characters used to truncate family names that appear in the UI. The appliance truncates at or after the first matching character, thus resulting in the shortest URL.</p> <p>By default, the appliance truncates each URL at the question mark (?) that separates the resource path from the parameters, or at the 7th slash in the full URL (including the protocol), whichever comes first.</p> <p>Your goal is to define your truncated URLs and/or content values to group matching page views into useful categories. For example, you might want to group page views by region or by transaction type if the web app includes URL patterns such as region or trxttype.</p> <p>Note—You might need to refine your truncated URL and/or content values in an iterative manner to get the results you want. The workflow is as follows:</p> <ul style="list-style-type: none"> ■ Define your truncated URLs and/or content values. ■ Collect web traffic for 15 minutes or more. ■ Examine the results. ■ Refine your definitions and repeat the process until you get the results you want. <p>For more information, see “Content Values” on page 210.</p>
Minimum Length	<p>If a Page Family name (URL + added content values) is truncated at the maximum 150 characters, this option ensures that at least x characters of the URL are retained.</p> <p>If the length of the length of the Truncated URL portion PLUS the Content Values portion is bigger than 150, the Truncated URL portion is further reduced to make it all fit into 150 characters. However, the Truncated URL portion <i>WILL NOT</i> get reduced beyond what's specified by the Minimum Length. And if the Truncated URL shortened to its minimum length PLUS the Content Values portion is <i>STILL</i> longer than 150 characters, then the Content Values portion will get shortened to make it all fit into 150 characters.</p>
Truncate at character_____	<p>Truncate all characters at or after a custom character. If the appliance is configured to truncate at the semicolon(;), the result is</p> <pre>http://www.example.com/a;bcd... (URL stem)</pre> <pre>http://www.example.com/a... (page family name)</pre>

Setting	Notes
Truncate at ___ slashes	<p>Truncate all characters after the first instance of the <i>n</i>th slash (includes <code>http://</code>). The <i>n</i>th slash is not truncated. For example, if the appliance is configured to truncate at the fourth slash, the result is:</p> <pre>http://www.example.com/a/b/c/d/e... (URL stem) http://www.example.com/a/... (page family name)</pre>
Advanced Options	<p>Use Advanced Options to match and replace strings within the page family name.</p> <ul style="list-style-type: none"> ■ Uses this format: "match" => "replace" ■ Multiple match/replacements can be entered by putting them on separate lines. <p>You also can use regular expressions, with \N denoting a back-reference. For example, the following entry in the Advanced Options section:</p> <ul style="list-style-type: none"> – replaces all instances of "riverbed" with "rvbd" – replaces all instances of "company" with "co" – swaps the first and second portions of the path section of the URL: <pre>"riverbed" => "rvbd" "company" => "co" "http://([^\/*]+)/([^\/*]+)/([^\/*]+)/(.*)" => "http://\1/\3/\2/\4"</pre>
Content Values	<p>Group page views into families based on page content. The appliance uses each entry in this table to construct Page Family names. The more content values you include in this table, the more page families you will get.</p> <p>The content values you select should correspond to the page matching rule and group pages into useful categories. For example, you might want to group a trading app into "buy" and "sell" page views based on a parameter named <code>trx_type</code>.</p> <p>Each entry has the following attributes:</p> <ul style="list-style-type: none"> ■ Display label (optional)—A label for the content value that be inserted into the Page Family Name preceding the value taken from the page. ■ Content—Content type: SOAP value, URL parameter, etc. ■ Location—The page location where the content is located. The available options depend on the selected content type. ■ Parameter Name—The parameter or value taken from the page. If you specify Custom RegEx for the content type, enter the RegEx here. <p>Important—The more content values you include in this table, the more page families you will get.</p> <p>For more information, see “Truncated URL” on page 214.</p>
Prepended Display Label	<p>A prefix string to insert before the content values in the Page Family name.</p> <p>If you want to specify a simple Page Family name, with no content list or URL parameters (such as “East Coast sales”), specify the name in this field with Truncated URL unchecked and no Content Values defined.</p>
Delimiter Character	The delimiter to use between content values in the Page Family name.

Custom WTA Metrics/Columns

You can create custom metrics in WTA tables to show data of interest for matching Page Views: SOAP values, URL parameters, and so on.

Custom Page Column Settings

Setting	Notes
Name	The name that appears in the column heading. Try to specify a short but descriptive name.
Status	A Page Column rule must be active for the custom column to appear in a table.
Page Match Criteria	You can display the custom column for all Page Views, or only for Page Views that match specific criteria. If a table or other view has no matching Page Views, the custom column is hidden.
URL Patterns	
Content Values	A matching Page View must include matching name/values in its URL or HTTP/HTTPS payload data.
Advanced	
Column Value Definition	The value to display for each Page View in this column.
Content	Value type: SOAP value, URL parameter, form value, or HTTP header value
Location	Value location (depends on the value type).
Parameter	The parameter (key) that corresponds to the value you want to display.

Page Match Criteria

A *Page Match Criterion* is a set of filters used to match

- Web objects to applications (Advanced Web Applications).
- Web objects to pages (Page Analysis Rules).
- Web pages to Page Families (Page Family Rules).

A Page Match Criterion can include one or more of the following filters:

- URL patterns

Filter web objects or pages with URLs that match one or more of the specified patterns. Each entry should include the protocol prefix (`http://`, `https://`, or `http*://`). Examples include:

```
https://*mycompany.com/*calendar*
```

```
http://www.example.com/*.aspx
```

- Content Values

Filter objects or pages that contain one or more of the following content values in the specified locations. Each entry has the following attributes:

- Display label (*optional*)—A label for the content value to be inserted into the Page Family Name preceding the value taken from the page.

- Content—Content type: SOAP value, URL parameter, etc.
 - Location—The page location where the content is located. The available options depend on the selected content type.
 - Parameter Name—The parameter or value taken from the page. If you specify Custom RegEx for the content type, enter the RegEx here.
- URL patterns

Filter web objects or pages with URLs that match one or more of the specified patterns. Each entry should include the protocol prefix (`http://`, `https://`, or `http*://`). Examples include:

```
https://*mycompany.com/*calendar*
```

```
http://www.example.com/*.aspx
```

Information Privacy

You can configure AppResponse 11 to prevent private data in observed web traffic—URLs, cookies, POST data—from being saved in the metric database or displayed in the user interface. Examples of private data include passwords, personal identification such as Social Security numbers, and other internal information.

This section discusses the following:

- [“Information Privacy Definition Settings”](#)
- [“Important Notes and Warnings about Information Privacy and WTA” on page 217](#)
- [“Task: Define Private Information to Filter from WTA Data” on page 218](#)
- [“Defining Keys Using Regular Expressions” on page 221](#)

Information Privacy Definition Settings

Setting	Notes
Key	<p>The <code>[key]</code> string in the <code>[key] = [value]</code> pairs that contain the private information to exclude.</p> <p>For information about how to find the key string, see “Information Privacy Definition Settings” on page 217.</p>
Description	
Status	If the definition is not enabled, private information for the specified key will not be hidden.
IP Addresses	<p>To reduce unnecessary load on the appliance, it is good practice to apply the privacy definition only to server IP addresses and ports for the web application of interest.</p> <p>For information about how to find this information, see “Information Privacy Definition Settings” on page 217.</p>
Ports	
URLs	

Important Notes and Warnings about Information Privacy and WTA

Note the following:

- **WARNING**—This functionality does not hide private data after it has been observed by the appliance. For this reason, you must specify the private data to mask out before you enable web page analysis or SSL decoding.
- **WARNING**—This Information Privacy functionality applies to Web Transaction Analysis data only. You cannot use this functionality to hide sensitive information in packet data captured over unencrypted connections.

If you want to use Web Transaction Analysis and capture packets but cannot do both over an encrypted connection, Riverbed recommends that you configure the appliance using one of the following methods:

Capture in "headers-only" mode, as described in XREF.

Set the Packet Size Limit to no higher than 128, as described in XREF.

- AppResponse 11 assumes that private data fields are embedded in the web traffic as key-value pairs separated by the '=' character (for example, `username=jsmith` and `sessionID=1131`).

If a web application uses different conventions for transferring values, you must define the keys using regular expressions as described in *Defining Keys Using Regular Expressions*. Note that to use this method, you must have a working knowledge of regular expressions and the exact data formats used by the web application of interest.

Task: Define Private Information to Filter from WTA Data

The following items describe the general workflow:

1. For each web application of interest, create a list of HTTP parameter fields that contain private data you want to mask out. Examples of private data include
 - Passwords
 - Social Security numbers
 - External usernames

Note—The best source for obtaining this information is from the web developers or other staff who develop, maintain, and/or troubleshoot the web application directly. If this is not an option for you, the following steps provide additional guidelines for obtaining this information on your own.

2. If you cannot obtain the data key, server, and URL information from someone in your organization, use tcpdump, Wireshark, or another program to capture one or more page views that contain at least one instance of each data field that you want to mask out.

Capture the web traffic as follows:

- Go to the login page for the web application.
- Start the capture.
- Log in as a user who can enter and submit the data fields you want to mask out (password, Social Security number, and so on).
- Wait until the "login-succeeded" page downloads completely.
- Navigate to a web page that prompts you for the data field(s) of interest.

Note—Pages such as "Update Profile" or "New Profile" are likely candidates for entering and submitting this type of information.

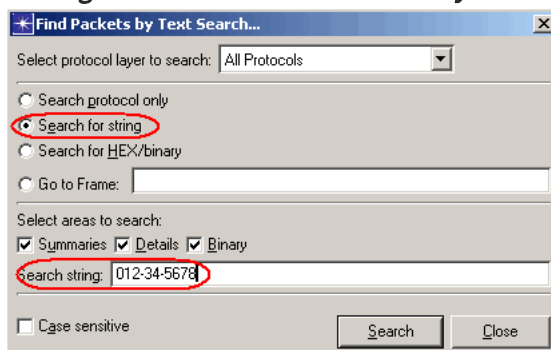
- When prompted, specify the requested information. If necessary, write down the values that you specify so you can search for these values in the trace.
 - Submit the information to the web server (for example, by clicking OK or Submit).
 - Stop the capture.
 - Open the resulting trace file in Wireshark or in the Trace Explorer window of Transaction Analyzer.
3. Go to Administration > Web Transaction Analysis: Information Privacy.
 4. Click Add to create a new Information Privacy definition.
 5. Specify the Key, IP Address(es), Port(s), and URL(s) in which the private information will be found.

Note—The best source for obtaining this information is from the web developers or other staff who develop, maintain, and/or troubleshoot the web application directly. If this is not an option for you, the following sections describe how to find this information if the trace file you created in step 2.

Key

Using the Find Packets operation in Wireshark or Transaction Analyzer, search for packets that contain the `[value]` string that you submitted for the data field of interest (password, Social Security number, etc.). Make sure that you search the text/string/ASCII data rather than the binary/HEX data.

Finding Packets with a Social Security Number (Example)



For each packet that contains the `[value]` string, parse the HTTP contents of that packet to locate the corresponding `[key]` string. This best places to look are in the `POST` data (most likely) or the URL parameter of a `GET` request (less likely, but possible).

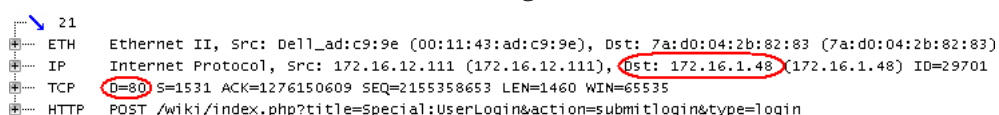
Servers > Ports

Servers > IP Addresses

Examine the `POST` message for the web page that contains the `[key] = [value]` string of interest.

- The port number is in the TCP header > destination port.
- The IP address is in the IP header > destination IP.

Server Port and IP address in POST Message



Note—If the web application uses multiple servers, you might need to specify multiple server ports/IP addresses.

URLs

When you specify the host and path, your goal is to enter one or more regular expressions that match all page views that might include the specific `[key]=[value]` string. The following are some example hostnames/paths:

`inet.acme.com` and `*/profile*` (“Any page view whose URL includes the host string `inet.acme.com` and a path with the parameter string `profile`”)

`myprofile.acme.com` and `*` (“Any page view whose URL includes the host string `myprofile.acme.com`”)

`www.webstore.com` and `/purchase/*` (“Any page view whose URL includes the host string `www.webstore.com` and a parameter string that starts with `/purchase/`”)

6. Repeat **Step 4** and **Step 5** for each additional parameter you want to mask out.

7. Review all your entries in the Information Privacy definitions, then click Apply or OK.

Note—AppResponse does not mask out private data after it is stored on an appliance. For this reason, it is good practice to review all Information Privacy profiles for all private key strings before you enable Web Transaction Analysis or SSL decoding.

8. If the data fields you want to mask out are included in URLs, you can use the following steps to verify that the Information Privacy profile you specified works as intended:
 - Go to the Administration > System > Pages web page and enable (turn on) the “Enable Page Analysis” option.
 - Go to the login page of the web application and log in (if you are already logged in, log out and then log back in).
 - Repeat the web session you performed in **Step 2** to generate the trace file.
 - Go back to Administration > System > Pages and disable (turn off) the “Enable Page Analysis” option.
 - Set the project time to focus on the web session you just performed.
 - Open the Individual Page Views insight (Insights > Page Analysis > Individual Page Views).
 - Select the Top Page Analysis Groups tab and select Web Application in the pull-down menu (top left).
 - In the Group table (top left), select the web application you are verifying.
The Top Individual Page Views table (bottom) shows the top page views for the web application.
 - In the Top Individual Page Views table, resize the Individual Page column so that you can see the entire URL. The sensitive parameter strings should appear masked.
9. If the parameter values of interest appear unmasked in the URLs, repeat step 2. through step 9. until you get the results you expect.

Defining Keys Using Regular Expressions

AppResponse can automatically find keys that are encoded in the application/x-www-form-urlencoded format: key=value pairs separated by ampersands—for example, key1=value1&key2=value2.

If a web application uses a different encoding format, you can enter regular expressions to find the username, session ID, and other keys. This requires the following:

- A working knowledge of regular expressions
- A knowledge of the exact key-encoding format used by the application you want to monitor. Information about non-urlencoded formats is outside the scope of AppResponse documentation.

You can specify regular expressions in the following fields only:

- Administration > Web Transaction Analysis: Information Privacy .> Key
- Administration > Web Transaction Analysis: User Session Tracking > Name of User Key field
- Administration > Web Transaction Analysis: User Session Tracking > Name of Session Key field

Required Format

To find a non-urlencoded key, you must enter a regular expression in the following format:

1. [regex] - This tag tells the appliance that you are defining a regular expression rather than a key string.
2. A regular expression that tells the appliance how to find the matching string
3. A parenthesized expression that tells the appliance how to find the key within the matching string

For example, suppose a web app defines usernames in the format

```
username:jsmith,password:XXXXXXX
```

In this case, you would do the following:

1. Go to Administration > Web Transaction Analysis: User Session Tracking > User Session Tracking.
2. In the Name of User Key field, enter **[regex]username: ([^,]*)**

This says: find the string `username: [all-chars-until-the-next-comma]`

The appliance finds the matching string: `username:jsmith`

The appliance uses the parenthesized expression `([^,]*)` to find the `username: jsmith`

User Session Tracking

You can configure WTA to track individual users and the page views for each user. To set up user tracking, you need to create a User Session Tracking definition for each web application of interest. Each definition specifies a set of related web pages and the key strings that the web client and web server use to track individual sessions.

This section discusses the following:

- “Important Notes”

- [“Use the Session Tag for User Name if User Name Not Found”](#)
- [“Discover User Tracking Information from a Packet Trace File”](#)
- [“Define User Session Tracking for a Web Application”](#)

Important Notes

Note the following:

- WTA assumes that usernames and session IDs are embedded in the web traffic as key-value pairs separated by the '=' character (for example, `username=jsmith` and `sessionID=1131`).

If a web application uses different conventions for transferring usernames and session ID strings, you must define the keys using regular expressions as described in [“Defining Keys Using Regular Expressions” on page 221](#). To use this method, you must have a working knowledge of regular expressions and the data formats used by the web application of interest.
- Do not use any of the following characters in a User Session Tracking definition, unless you are defining a regular expression as described in [Defining Keys Using Regular Expressions](#):
 - . (period)
 - + (plus sign)
 - * (asterisk)
 - ? (question mark)
 - () (parentheses)
 - { } (brackets)
 - [] (square brackets)
 - ^ (caret)
 - \$ (dollar sign)
 - \ (backslash)
 - *
- Collecting user data can be highly resource-intensive, especially on large networks with a lot of web traffic. Therefore, it is good practice to collect user data only for Page Families of interest.

Use the Session Tag for User Name if User Name Not Found

A User Session Tracking Definition contains a check box to enable using the session ID if a User ID is not found. When enabled, a hash of the retrieved session ID is used for the user name by default. To use the raw session ID for the user name the session Prefix must be specified as [raw].

To use a raw session ID as the user name, do the following:

1. Go to Administration > Web Transaction Analysis: User Session Tracking.
2. Click **Add** or hover over an existing User Session Tracking Definition’s description and click the pencil icon on the right to edit the definition.

3. Select **Active** for the definition Status.
4. Enter the **User key** and the **Session Key**.
5. Select **Cookie** under Search Locations for both User Key and Session Key.
6. Select **Use session IDs as User IDs if User ID is not found**.
7. Enter [raw] as the **Prefix**.
8. Enter Server Port(s).
9. Enter Server IP(s).
10. Click **Save** to make your changes or **Revert** to dismiss them. If Save is not active, check that there are valid entries for each field.

Discover User Tracking Information from a Packet Trace File

1. Capture a login of the web application in a packet trace file:
 - If the application login exchanges passwords or other sensitive information, verify that is configured to mask out this information.
For more information, see XREF.
 - If the application login is SSL-encrypted, set up SSL Decoding_XREF.
For more information, see Enable SSL Decoding.
 - Using tcpdump or Transaction Analyzer, capture the login sequence as follows:
Go to the login page for the web application.
Start the capture.
Enter the username/password and log in.
Wait until the "login-succeeded" page downloads completely.
If the web application uses separate servers for logins and for content, download a few more pages so that you can capture data for the different servers used by the application.
Stop the capture.
2. Open the resulting packet trace file in the Transaction Analyzer Transaction Analyzer or Wireshark.
3. You can find the correct information for the definition by analyzing the decoded HTTP trace data in Wireshark or Transaction Analyzer. The following sections describe how to determine the correct settings for
 - **“Login Page” Ports and IP addresses**
 - **“Login Page” URL Patterns**
 - **“User Session Tracking Definition Settings”**

“Login Page” Ports and IP addresses

Examine the POST message for the client login.

- The port number is in the TCP header > destination port.
- The IP address is in the IP header > destination IP.

If the web application uses multiple login servers, you might need to specify multiple server IPs.

“Login Page” URL Patterns

Examine the POST message for the client login. Look for the string in the URL path that is unique to the login-submitted page—that is, the page that indicates to the user that the login was successful. A useful technique is to compare the “pre-login” and “post-login” URLs to determine the string that is unique to the latter. For example, suppose a web application uses the following pre- and post-login URLs:

```
https://myapp.acme.com/index.php?title=Special:UserLogin
```

```
https://myapp.acme.com/index.php?title=Special:UserLogin&action=Submitlogin
```

In this case, `Submitlogin` is the string that marks a page as coming from the login server. In this case, you would specify the URL pattern as

```
myapp.acme.com/*SubmitLogin*
```

“Associated Pages” URL Patterns

If the web application uses the same server (or set of servers) for logins and other types of transactions, you can use the same URLs and servers for Associated Pages as you did for Login Pages.

If the application uses separate login servers, you will need to use the same workflow that you used for the login pages:

- Capture one or more associated page views using tcpdump or Transaction Analyzer.
- Examine the POST message(s) for the TCP port and IP address for the web server.
- Examine the POST message(s) to the URL host and path.

When you specify the host and path, your goal is to enter a regular expression that matches all page views of interest for the web application of interest (and no other web applications that you are tracking in AppResponse 11). The following are some example URL patterns:

- `inet.acme.com/*calendar*` (“Any page view whose URL includes the host string `inet.acme.com` and a path with the parameter string `calendar`”)
- `calendar.acme.com*` (“Any page view whose URL includes the host string `calendar.acme.com`”)
- `www.webstore.com*/shopchart/*` (“Any page view whose URL includes the host string `www.webstore.com` and a parameter string that starts with `/shopchart/`”)

Define User Session Tracking for a Web Application

A User Session Tracking definition specifies a set of related web pages and the key strings that the web client and web server use to track individual sessions. Each definition corresponds to one web application. AppResponse 11 requires this definition to track individual users and the page views for each user.

Figure 9-1. “User Session Tracking Definition Settings”

New User Session Tracking Definition

Name:

Description:

Status:

☒ Active ☐ Inactive

User Key:

Search Locations:

☒ URL

☐ Cookie

☒ POST Data

☐ Header

Session Key:

Search Locations:

☒ URL

☒ Cookie

☐ POST Data

☐ Header

☐ Use session IDs as User IDs if User ID is not found. Prefix:

session

Login Page

Server Ports:

Comma separated ports

Server IPs:

Comma separated IPs

URL Patterns:

Add Url

Associated Pages

☒ Use Login Page Server Ports, IPs, and URL Patterns

Save

User Session Tracking Definition Settings

Setting	Notes
Name	Identifies the web application and associated pages.
Description	
Status	To enable user tracking, select Active . To disable, select Inactive .
User Key	The key name used to track the username (for example, user in key=value pair user=jsmith) and the HTTP/HTTPS locations to search. This field is required for WTA to identify usernames in web traffic.
Session Key	The session ID used to track the session ID (for example, sessionID in key=value pair sessionID=12345). This field is required for WTA to identify session IDs in web traffic.
Use session IDs as User IDs if User ID is not found. Prefix:	<p>This option is useful to track users when the appliance did not observe the initial login sequence for a session. This can occur because</p> <ul style="list-style-type: none"> ■ A web application uses an authentication server whose traffic is not monitored by the appliance. ■ The login occurred before WTA was enabled. <p>When this option is enabled, WTA creates User names with the label <code>[prefix]+[session_tag]</code>. The session tag is a unique, auto-generated tag (not the session ID). Note—If the prefix includes a non-alphanumeric character, enclose the argument string in single quotes (example: <code>'FinTrx\$Session'</code>).</p>

Setting	Notes
Login Page	<p>The login pages where users enter usernames.</p> <ul style="list-style-type: none"> ■ Ports—Port number(s) used by these login pages ■ IP addresses—The IP address(es) for all hosts that serve these login pages ■ URL Patterns—A set of strings or regular expressions to identify the login pages. Specify the following: <ul style="list-style-type: none"> ■ 1+ strings/patterns for the hostname/domain (examples: <code>www.acme.com</code> and <code>*.google.com</code>). <p>Do not include a port number in this field, even if the web application normally includes one in its URL—for example, enter only <code>www.mywebapp.com</code> and not <code>www.mywebapp.com:8010</code>.</p> ■ 1+ strings patterns for the login page (examples: <code>*/identification.aspx</code> and <code>*AUTH_Login*</code>)
Associated Pages	<p>Web pages that use Session IDs based on the key specified under the Parameters Tab. To identify users that downloaded these pages, WTA parses the traffic for session IDs and matches an individual session to a username.</p> <ul style="list-style-type: none"> ■ Ports—Port number(s) used by associated pages ■ IP addresses—The IP address(es) for all hosts that serve these associated pages ■ URL Patterns—A set of strings or regular expressions to identify associated pages. Specify the following: <ul style="list-style-type: none"> ■ 1+ strings/patterns for the hostname/domain (examples: <code>www.acme.com</code> and <code>*.google.com</code>). <p>Do not include a port number in this field, even if the web application includes one in its URL—for example, enter <code>www.mywebapp.com</code> and not <code>www.mywebapp.com:8010</code>.</p> ■ 1+ strings patterns for the login page (examples: <code>*/identification.aspx</code> and <code>*AUTH_Login*</code>)

Database Analysis

The Database Analysis module provides performance metrics for SQL statements. The module decodes Layer 7 SQL statements issued across the network to supported relational database servers. With these metrics you can analyze and evaluate how applications are performing in your network. For example, when an application is slow, is the problem in the network, the web server, the application server, or the relational database? While it isn't unusual for the database to be the culprit, identifying and fixing a problem often requires detailed information about the SQL statements being used.

In addition to decoding the network traffic and isolating the SQL statements and their performance, AppResponse 11 also does a full parse of every SQL statement. It normalizes the statements across SQL dialects, enabling SQL statements to be standardized. In this process literals are masked out allowing the performance of a particular SQL statement to be compared over time, even when the statements originally looked different due to differing literals. For example, when the SQL statement "select customer_name where customer_id = 12345" is parsed, the literal "12345" is masked out (replaced by "L1"). This provides the additional benefits of hiding potentially sensitive information, such as SSNs or passwords, and improving AppResponse 11 performance and use of storage.

The Layer 7 protocols for the following relational database servers are supported:

- IBM DB2 LUW 8.0 through 9.7
- IBM DB2 on AS/400
- IBM Informix 7.30 through 12.10
- Microsoft SQL Server 2005, 2008, 2012, 2014, and 2019
- MySQL 5.0 through 5.5
- Oracle 8.1.7 through 12c
- PostgreSQL 9.5 and higher
- Sybase ASE 11.9.2 through 15.7
- Teradata V2R5.0 through 15.10

The following topics are discussed in this section:

- [“Configuring DB Analysis” on page 229](#)
- [“Using Insights to View and Analyze Database Metrics” on page 230](#)
- [“Using Navigator to Explore and Create Insights” on page 230](#)

Configuring DB Analysis

DB Analysis is enabled by default. All supported database servers are auto-detected and monitored. The web UI page, found at Administration > Database Analysis: DB Analysis, has an Enable check box and displays the current status. See [“Database Analysis” on page 228](#) for an overview and a list of topics.

Disabling database analysis

1. Go to Administration > Feature Settings: DBA Module.
2. To disable database analysis, clear the check box next to Enabled.
3. Click **Apply** to make the change or **Revert** to discard it.
4. If applied, the current status is now Capture Disabled.

Enabling database analysis

1. Go to Administration > Feature Settings: DBA Module.
2. To enable database analysis, select the check box next to Enabled.
3. Click **Apply** to make the change or **Revert** to discard it.
4. If applied, the current status is now Capture Enabled.

Configuring Database Analysis Filters

Click Administration > General Traffic Settings: Traffic Analysis Filters, then click the Database Analysis tab to configure database analysis traffic filters. These filters are visible also (but not editable) in the Filters tab of the Database Analysis page displayed by clicking Administration > Feature Settings: DBA Module.

The database analysis results will include only traffic that matches the filters that are enabled at the time of data capture. The filters do not affect data that has been captured already, and at least one filter must be enabled to process database traffic.

Click the Edit icon next to a filter entry to display the Edit Traffic Filters dialog for modifying an existing definition or creating a new one by clicking Add. Each filter is enabled by default. The filter definition parameters are:

- Protocol – Specify the protocol used by the database analysis traffic. Currently, this must be TCP.
- Server Ports – Specify individual ports or a range of ports associated with the database analysis traffic.
- Server IPs – Specify individual IP addresses or a range of addresses associated with the database analysis traffic.

Using Insights to View and Analyze Database Metrics

In the web UI menu bar, go to Insights and choose a DB summary or individual insight. For more information about insights, see [“Insights” on page 164](#).

Using Inputs to select or specify Insight contents

Predefined AppResponse 11 insights have an Input drop-down menu on the far left. Open the drop-down menu to specify or select database metrics to use in the insight. When finished, click **Launch**. The Inputs vary by the Insight selected. They enable you to specify the metrics of interest used in the insight

For example, go to Insights > Summary: DB Queries. and open the drop-down menu. Click in the DB Client Group text box. Click your selection from displayed list of available choices. When no choices are displayed specify the desired item, for example, for “DB Client IP” enter a valid IPv4 or IPv6 address.

Using Navigator to Explore and Create Insights

For more information on using Navigator to drill down and analyze database metrics, see [“Navigator” on page 189](#).

UC Analysis

Unified communications analysis (UCA) is an optional module for AppResponse 11 that enables you to view aggregated or individual VoIP call information in the web UI. The UCA module requires a separate license in order to be active and accessible; no VoIP data will be handled or displayed unless the UCA module license is active.

To access the UC Analysis module controls, choose Administration > Feature Settings:UCA Module.

The UC Analysis screen appears, divided into three tabs:

- **Enable/Disable tab** - Enable or disable the UCA module. Note that even if this option is enabled, the UCA module won't function without a valid license.
 - **Enable UC Analysis**
 - **Infer Call From RTP** - When this option is enabled, RTP streams will be shown as calls in the Individual Calls table, even if there is no signaling associated with them.
 - **Decode Encrypted Signaling** - When this option is enabled, any time encrypted signaling is encountered and a matching key has been added under Administration > System Settings: Traffic Decryption, the VoIP module will be able to decrypt the signaling and show the decrypted calls.
 - **Apply/Revert** - Execute changes to the Enable UC Analysis settings, or return to the previous settings.
- **Signaling tab** - This tab displays the ports that are mapped currently for the available signaling protocols. Changes to these port mappings can be made under Administration > Analyses: Module Traffic Filters. The default signaling protocols supported are H323, SIP, and SKINNY.
- **Call Quality tab** - This tab enables you to specify quality thresholds for the **“AppResponse 11 supports the following CODECS for unified communications analysis in the current version:”**. These thresholds are used to show what percentage of time for a call is spent at poor, fair, good, or excellent quality. The thresholds represent the minimum MOS score associated with that quality level. For example, setting the fair threshold to 2 means that any MOS score below 2 will be classified as poor and MOS scores above 2 will be classified as fair.
 - **Add/Delete** - Manage the set of available codecs.
 - **Codec: Status, and MOS scores for Fair/Good/Excellent**

CXA Module

Click Administration > Feature Settings:CXA Module to display the CXA Module page. This page provides the Enabled checkbox to activate/deactivate the CXA module. (It is enabled by default.) Click Apply to finalize or Revert to undo a change to the module activation.

In addition, the page provides controls for handling GeoMap private configuration data for supporting the GeoMap widgets available for various CXA drilldowns. You can import or export GeoMap private configuration using a CSV or JSON file, or you can delete the current configuration. The CXA module uses ISO country codes and MaxMind region codes that are valid as of April 2019.

The Citrix Analysis (CXA) module is an optional feature module for SteelCentral AppResponse appliances, delivering end-to-end network performance monitoring of Citrix activity in your network. When the CXA module is enabled and AppResponse 11 is communicating with SteelCentral Agents for Aternity SaaS, three AppResponse 11 Insights enable you to view Citrix-related performance data: Citrix Servers, Citrix Users, and Citrix User Sessions. **Refer to the *AppResponse Release 11 Citrix Analysis (CXA) Module Installation and Configuration Guide* for information about how to begin using the CXA module.**

Command-Line Interface

Most system operations can be done using the Administration tab in the AppResponse 11 menu bar in the web UI. The web UI is the recommended way of managing AppResponse 11 when possible. In version 11.0, storage unit management is done only through the CLI.

Command-Line Interface Operation

The AppResponse command-line interface (CLI) is accessed using SSH to the AppResponse 11 IP address, using the default username and password (admin/admin). AppResponse 11 running on a VMware virtual machine can also access it using the VM console by logging in as admin.

Different CLI commands are available in different CLI modes. Each mode has a unique command-line prompt. When entering CLI commands, the use of two special characters can provide information, options, and auto-completion of commands.

- Use the "?" key for an explanation of available CLI commands.
- Use the Tab key to show the next entries on a command line.
- Use the Tab key to auto-complete a CLI entry.

Here is an example CLI session, from login to exit. Text in < > demonstrate how special keys can be used.

```
login as: admin
host's password: admin
Last login: Thu Nov  3 15:02:52 2016 from 10.18.41.255
host > <?>
enable  Enter enable mode
exit    Exit config mode or logout
no      Negate or clear certain configuration options
show    Display system configuration or statistics
host > enable
host # <?>
configure  Enter configuration mode
disable    Leave enable mode
exit       Exit config mode or logout
no         Negate or clear certain configuration options
show       Display system configuration or statistics
host # con<Tab> terminal
host (config) # <?>
exit       Exit config mode or logout
interface  Configure network interfaces
ip         Configure IP settings
no         Negate or clear certain configuration options
reboot     Reboot the system immediately
show       Display system configuration or statistics
shutdown   Shut down the system immediately
```

```
storage    Configure storage settings
user       Add/Modify a user account
wizard     Run the configuration wizard
host (config) # exit
host # exit
```

Supported CODECS

AppResponse 11 supports the following CODECS for unified communications analysis in the current version:

Audio

- MPEG1
- MPEG2
- MPEG3
- MPEG2AAC
- AC3
- MPEG4AAC
- MPEG4LDAAC
- MPEG4HEAAC
- WMAP
- MPEG4HEAACv2
- MPEG4LCAAC
- AMRWBPlus
- AudioVorbis

Video

- Motion JPEG
- MPEG-1
- MPEG-2
- ITU-T H.261
- ITU-T H.263
- ITU-T H.263+
- ITU-T H.264/MPEG-4 AVC

- MPEG-4 ASP
- VC-1 SMTPE 421M (Microsoft)
- VP6 (On2 TrueMotion)
- ITU-T H.264 SVC
- VP8 (On2 Technologies/Google)
- VP9 (Google)
- ITU-T H.265

Voice

- G.711 64k u-law
- G.711 64k u-law with PLC
- G.723.1 (5.3kbit/s)
- G.723.1 (6.3kbit/s)
- G.728 (16 kbit/s)
- G.729 (8.0 kbit/s)
- G.729A, AB (8.0 kbit/s)
- GSM 6.10 (full rate)
- GSM 6.20 (half rate)
- GSM 6.30 (enhanced full rate)
- Lucent/elemedia SX7300/8300
- Lucent/elemedia SX9600
- G.711 64k A-law
- G.711 64k A-law with PLC
- G.726 ADPCM (16 kbit/s)
- G.726 ADPCM (24 kbit/s)
- G.726 ADPCM (32 kbit/s)
- G.726 ADPCM (40 kbit/s)
- GIPS Enhanced G.711 u-law
- GIPS Enhanced G.711 A-law
- GIPS iLBC
- GIPS iSAC
- GIPS iPCM-wb
- G.729E (8.0 kbit/s)
- G.729E (11.8 kbit/s)

- Wideband Linear PCM
- Wideband Linear PCM with PLC
- G.722 (64 kbit/s)
- G.722 (56 kbit/s)
- G.722 (48 kbit/s)
- Siren7/G.722.1 (32 kbit/s)
- Siren7/G.722.1 (24 kbit/s)
- AMR-WB/G.722.2 (23.85 kbit/s)
- AMR-WB/G.722.2 (23.05 kbit/s)
- AMR-WB/G.722.2 (19.85 kbit/s)
- AMR-WB/G.722.2 (18.25 kbit/s)
- AMR-WB/G.722.2 (15.85 kbit/s)
- AMR-WB/G.722.2 (14.25 kbit/s)
- AMR-WB/G.722.2 (12.65 kbit/s)
- AMR-WB/G.722.2 (8.85 kbit/s)
- AMR-WB/G.722.2 (6.6 kbit/s)
- QCELP (8 kbit/s)
- QCELP (13 kbit/s)
- EVRC-A (4.0-8.3 kbit/s)
- SMV (3.67-7.95 kbit/s)
- AMR-NB (12.2 kbit/s)
- AMR-NB (10.2 kbit/s)
- AMR-NB (7.95 kbit/s)
- AMR-NB (7.4 kbit/s)
- AMR-NB (6.7 kbit)
- AMR-NB (5.9 kbit/s)
- AMR-NB (5.15 kbit/s)
- AMR-NB (4.75 kbit/s)
- iLBC (13.3 kbit/s)
- iLBC (15.2 kbit/s)
- G.711 56k u-law
- G.711 56k u-law with PLC
- G.711 56k A-law
- G.711 56k A-law with PLC

- G.723.1 Annex C (0.7-14.3 kbit/s)
- Speex Narrowband (2.15 kbit/s)
- Speex Narrowband (5.95 kbit/s)
- Speex Narrowband (8 kbit/s)
- Speex Narrowband (11 kbit/s)
- Speex Narrowband (15 kbit/s)
- Speex Narrowband (18.2 kbit/s)
- Speex Narrowband (24.6 kbit/s)
- Speex Narrowband (3.95 kbit/s)
- Speex Wideband (12.8 kbit/s)
- Speex Wideband (16.8 kbit/s)
- Speex Wideband (20.6 kbit/s)
- Speex Wideband (23.8 kbit/s)
- Speex Wideband (27.8 kbit/s)
- Speex Wideband (34.2 kbit/s)
- Speex Wideband (42.2 kbit/s)
- BV16 (BroadVoice 16kbit/s)
- BV32 (BroadVoice 32 kbit/s)
- IS-54 (7.95 kbit/s)
- Japanese PDC (6.7 kbits)
- AMBE2Plus (2.4 kbit/s)
- AMBE2Plus (3.2 kbit/s)
- AMBE2Plus (4 kbit/s)
- AMBE2Plus (4.8 kbit/s)
- EVRC-B (4.0-8.3 kbit/s)
- MS RTAudio (Microsoft Real Time Audio Wideband)
- MS RTAudio (Microsoft Real Time Audio Narrowband)
- MS RTAudio (Microsoft Real Time Audio Wideband with Redundancy)
- MS RTAudio (Microsoft Real Time Audio Narrowband with Redundancy)
- G.729 with GIPS PLC
- SILK Narrowband
- SILK Narrowband with FEC
- SILK Mediumband
- SILK Mediumband with FEC

- SILK Wideband
- SILK Wideband with FEC
- SILK Super Wideband
- SILK Super Wideband with FEC
- EVRC Wideband
- EVRC Narrowband-Wideband
- AMR Wideband Plus
- Siren7/G.722.1 (16 kbit/sec)
- Siren14/G.722.1C (24 kbit/sec)
- Siren14/G.722.1C (32 kbit/sec)
- Siren14/G.722.1C (48 kbit/sec)
- Siren14/G.722.1C with LPR (24 kbit/sec)
- Siren14/G.722.1C with LPR (32 kbit/sec)
- Siren14/G.722.1C with LPR (48 kbit/sec)
- Siren22 (32 kbit/sec)
- Siren22 (48 kbit/sec)
- Siren22 (64 kbit/sec)
- Siren22 with LPR (32 kbit/sec)
- Siren22 with LPR (64 kbit/sec)
- Siren22 with LPR (64 kbit/sec)
- G.719 (32 kbit/sec)
- G.719 (48 kbit/sec)
- G.719 (64 kbit/sec)
- Opus SILK Narrowband
- Opus SILK Narrowband with FEC
- Opus SILK Mediumband
- Opus SILK Mediumband with FEC
- Opus SILK Wideband
- Opus SILK Wideband with FEC
- Opus Hybrid Super Wideband
- Opus Hybrid Super Wideband with FEC
- Opus Hybrid Fullband
- Opus Hybrid Fullband with FEC
- Opus CELT Narrowband

- Opus CELT Wideband
- Opus CELT Super Wideband
- Opus CELT Fullband
- Enhanced Voice Services (EVS) Narrowband
- EVS Narrowband with FEC
- EVS Wideband
- EVS Wideband with FEC
- EVS Super Wideband
- EVS Super Wideband with FEC
- EVS Fullband
- EVS Fullband with FEC
- L16 Narrowband
- L16 Narrowband with PLC
- L16 Wideband
- L16 Wideband with PLC
- L16 Super Wideband
- L16 Super Wideband with PLC
- L16 Fullband
- L16 Fullband with PLC

AppResponse 11 Metric Descriptions

AppResponse 11 metrics provide insight into the behavior of individual IP addresses or the aggregate behavior of groups. Metrics include performance and utilization data captured by AppResponse 11 directly from network traffic in real time, as well as information derived from traceroutes, BGP, DNS, and a WHOIS database in the appliance.

Use AppResponse 11's Navigator to view aggregated groups of traffic data and metrics built by AppResponse 11 from network traffic, application stream analysis, web transaction analysis and database analysis.

AppResponse 11 captures or calculates metrics for these modules:

- "Application Stream Analysis (ASA) Metrics"
- "Citrix Analysis (CXA) Metrics"
- "Database Analysis (DBA) Metrics"
- "Unified Communications Analysis (UCA) Metrics"
- "Web Transaction Analysis (WTA) Metrics"

Common Concepts In Metrics

Metrics are always calculated for one minute intervals. Subsequently, those one minute intervals are aggregated into longer intervals, such as five minutes and one hour. Most widgets in the AppResponse 11 user interface (charts and tables), will autoselect the granularity of interval to display based on the volume of data available.

Unless noted explicitly otherwise, metrics displayed in tables are weighted averages, weighted by the number of measurements of that metric. Specific values, or maximum or minimum values, are displayed only when noted as such.

Application Stream Analysis (ASA) Metrics

The ASA metrics that are collected or calculated are:

Metric	Description
Outbound Utilization	The percent utilization of bandwidth configured for the associated Host Group in the outbound direction.
Inbound Utilization	The percent utilization of bandwidth configured for the associated Host Group in the inbound direction.
Active Connections	The number of TCP connections that exchanged data in the applicable time interval. TCP connections that were open but did not exchange data are not counted.
Connection Request Rate	The rate at which TCP SYNs were seen in the applicable time interval.
Connection Requests	The number of TCP SYNs, excluding any retransmitted SYNs, that were seen in the applicable time interval.
Connection Setup Time	The time it took for the TCP three-way handshake (connection open) to complete.
Data Transfer Time	The average time required to successfully transfer client-to-server Request and server-to-client Response data segments that were seen in the applicable time interval.
Response Data Transfer Time	The average time required to successfully transfer all server-to-client Response data segments that were seen in the applicable time interval.
Request Data Transfer Time	The average time required to successfully transfer all client-to-server Request data segments that were seen in the applicable time interval.
Server Hostname	The DNS-resolved name of the TCP server host.
Client Hostname	The DNS-resolved name of the TCP client host.
Connections Failed Rate	The rate at which the system saw TCP connections that did not successfully complete the three-way handshake (connection open), e.g., it saw SYNs, but did not see the corresponding/expected SYN-ACKs.
Connections Failed	The number of TCP connections that did not successfully complete the three-way handshake (connection open) , e.g., the system saw SYNs, but did not see the corresponding/expected SYN-ACKs. Number of SYNs – Connections established.
Server IP Address	The IP address of the TCP server host.
Client IP Address	The IP address of the TCP client host.
Connections Opened	The number of established TCP connections, independent of the number of successful three-way handshakes seen.
Connections Opened Rate	The rate at which the system saw TCP connections that successfully completed the three-way handshake (connection open).

Metric	Description
Traffic Per Request	The average number of bytes that were carried in the client-to-server Requests that were seen in the applicable time interval. Byte counts are based on powers of 10, not powers of 2, e.g., 1 kB is 1,000 bytes, not 1,024 bytes.
Traffic Per Response	The average number of bytes that were carried in server-to-client Responses that were seen in the applicable time interval. Byte counts are based on powers of 10, not powers of 2, e.g., 1 kB is 1,000 bytes, not 1,024 bytes.
Packets Per Request	The average number of packets that were required to successfully transfer a contiguous chunk of client-to-server Request bytes. This is an indication of how big client-to-server Requests were. This includes non-payload control packets such as SYN, ACK, FIN, RST, keep alives, etc.
Packets Per Response	The average number of packets that were required to successfully transfer a contiguous chunk of server-to-client Response bytes. This is an indication of how big server-to-client Requests were. This includes non-payload control packets such as SYN, ACK, FIN, RST, keep alives, etc.
Payload Transfer Time	The sum of the average Request and average Response Payload Transfer Times that were measured in the applicable time interval.
Request Payload Transfer Time	The average estimate of the time it would have taken to successfully transfer a contiguous chunk of Request bytes if there were no retransmissions. In other words, the time taken up by retransmissions, if present, is not accounted for in this metric.
Response Payload Transfer Time	The average estimate of the time it would have taken to successfully transfer a contiguous chunk of Response bytes if there were no retransmissions. In other words, the time taken up by retransmissions, if present, is not accounted for in this metric.
Server Reset Rate	The rate at which server-to-client RSTs were seen in the applicable time interval.
Server TCP Resets	The number of server-to-client RSTs that were seen in the applicable time interval.
Client TCP Resets	The number of client-to-server RSTs that were seen in the applicable time interval.
Client Reset Rate	The rate at which client-to-server RSTs were seen in the applicable time interval.
Reset Rate	The sum of the average rates of client-to-server and server-to-client RSTs that were seen in the applicable time interval.
Resets	The sum of the number of client-to-server and server-to-client RSTs that were seen in the applicable time interval.
Response Retrans Delay	An estimate of the average additional time that retransmissions contributed to the successful transfer of server-to-client Responses.
Request Retrans Delay	An estimate of the average additional time that retransmissions contributed to the successful transfer of client-to-server Requests.

Metric	Description
Retrans Delay	The sum of the average additional times that retransmissions of client-to-server Requests and server-to-client Responses contributed to the successful transfer of those Request and Responses.
% Retrans	The ratio of all retransmission segments seen to the total number of client-to-server and server-to-client segments that were seen.
% Response Retrans	The ratio of retransmitted segments to the total number of segments that were seen in the server-to-client direction.
% Request Retrans	The ratio of retransmitted segments to the total number of segments that were seen in the client-to-server direction.
Response Retrans Traffic	The number of server-to-client bytes that were retransmitted in the applicable time interval. Byte counts are based on powers of 10, not powers of 2, e.g., 1 kB is 1,000 bytes, not 1,024 bytes.
Retrans Traffic	The sum of the server-to-client and client-to-server bytes that were retransmitted in the applicable time interval. Byte counts are based on powers of 10, not powers of 2, e.g., 1 kB is 1,000 bytes, not 1,024 bytes.
Request Retrans Throughput	The rate, in bits per second, required to transmit all the client-to-server Request bytes that were retransmitted.
Response Retrans Throughput	The rate, in bits per second, required to transmit all server-to-client Response bytes that were retransmitted.
Retrans Throughput	The rate, in bits per second, of the sum of the client-to-server and server-to-client bytes that were retransmitted.
Request Retrans Traffic	The client-to-server Request bytes that were retransmitted.
Response Retrans	The percentage of server-to-client Response packets retransmitted relative to the total number of packets used to transmit the Response.
Retrans	The percentage of total Request and Response packets retransmitted relative to the total number of packets used to transmit the Request and Response.
Request Retrans Rate	The rate, in packets per second, of the packets retransmitted for the Request from client-to-server. This includes non-payload control packets such as SYN, ACK, FIN, RST, keep alives, etc.
Response Retrans Rate	The rate, in packets per second, of the packets retransmitted for the Response from the server-to-client. This includes non-payload control packets such as SYN, ACK, FIN, RST, keep alives, etc.
Retrans Rate	The rate, in packets per second, of the total packets retransmitted for the Request and Response. This includes non-payload control packets such as SYN, ACK, FIN, RST, keep alives, etc.
Request Retrans	The percentage of client-to-server Request packets retransmitted relative to the total number of packets used to transmit the Request.

Metric	Description
Round Trip Time	<p>This metric is an estimate of how quickly the network between the client and server would transport bits in both directions if the client and server were infinitely fast, and took no time to respond to Responses and Requests.</p> <p>As of AppResponse 11 Version 11.10.0, Round Trip Time (RTT) comprises two distinct metrics: RTT (self) and RTT (others). RTT (self) is the round trip time as the traffic passes the AppResponse 11 system both from and to the originating IP address or host group. (This is similar to the RTT inbound metric that was used in AppResponse 9.) RTT (others) is the round trip time from when the traffic passes the AppResponse 11 system to when it arrives at another network element, such as an IP address or host group. (This is similar to the RTT outbound metric that was used in AppResponse 9.) RTT, undifferentiated as either (self) or (others), is the sum of the two constituent RTTs: $RTT = RTT (self) + RTT (others)$.</p> <p>See “Round Trip Time” for an illustration.</p>
Server Response Time	<p>An estimate of the average amount of time TCP servers took to send Responses to the immediately preceding client-to-server Requests they received. This is an approximate and directional measure of how much time the server takes to perform data processing before it has data to send back to the TCP clients it is communicating with.</p>
Server Turn Rate	<p>The per second rate at which Server Turns were seen at the TCP servers that communicated with TCP clients in the applicable time interval.</p>
Server Turns	<p>The number of data direction turns that were seen at the TCP servers in the applicable time interval. A "data direction turn" is when a Request seen in one direction is immediately followed by a Response from the server in the other direction. (It is common for a Request/Response to be transferred by TCP using multiple TCP segments/packets.)</p>
User Response Time	<p>The overall responsiveness that the application/process experiences in its use of TCP to transfer and process the Requests and Responses that the application/process created. This metric is calculated as the sum of: (a) The amount of time it took to setup the TCP connections that map to the selected group/object (Connection Setup Time); (b) The amount of time it took to transfer all the Request bytes from client to server ignoring delays due to any retransmissions (Request Payload Transfer Time); (c) The amount of time it took to transfer all the Response bytes from server to client ignoring delays due to any retransmissions (Response Payload Transfer Time); (d) The amount of (processing) time it took the server to send responses to the requests it received from the client (Server Response Time); and (e) The amount of time taken up by retransmissions, if any (Retransmission Delay).</p>
Packet Traffic	<p>The total number of packets that were seen by the system in both the outbound and inbound directions for the selected group/object. This includes non-payload control packets such as SYN, ACK, FIN, RST, keep alives, etc.</p>

Metric	Description
Outbound Packet Throughput	The total per second packet rate of the packets that were sent by the individual IP hosts in the selected group/object to other individual IP hosts in other groups/objects. This includes non-payload control packets such as SYN, ACK, FIN, RST, keep alives, etc.
Inbound Packet Throughput	The total per second packet rate of the packets that were received by the individual IP hosts in the selected group/object from other individual IP hosts in other groups/objects. This includes non-payload control packets such as SYN, ACK, FIN, RST, keep alives, etc.
Outbound Packet Traffic	The total number of packets sent by the individual IP hosts in the selected groups/objects to IP hosts in other groups/objects. This includes non-payload control packets such as SYN, ACK, FIN, RST, keep alives, etc.
Packet Throughput	The total per second packet rate that was seen by the system in both the inbound and outbound directions involving the individual IP hosts in the selected group/object. This includes non-payload control packets such as SYN, ACK, FIN, RST, keep alives, etc.
Inbound Packet Traffic	The total number of packets received by the individual IP hosts in the selected group/object's from the IP hosts in other groups/objects. This includes non-payload control packets such as SYN, ACK, FIN, RST, keep alives, etc.
Outbound Throughput	The per second bit rate of the bytes sent by the individual IP hosts in the selected group/object's to IP hosts in other groups/objects.
Inbound Throughput	The per second bit rate of the bytes received by the individual IP hosts in the selected group/object's to IP hosts in other groups/objects.
Inbound Traffic	The total number of bytes that were received by the individual IP hosts in the selected group/object's to IP hosts in other groups/objects. Byte counts are based on powers of 10, not powers of 2, e.g., 1 kB is 1,000 bytes, not 1,024 bytes.
Outbound Traffic	The total number of bytes that were sent by the individual IP hosts in the selected group/object's to IP hosts in other groups/objects. Byte counts are based on powers of 10, not powers of 2, e.g., 1 kB is 1,000 bytes, not 1,024 bytes.
Throughput	The total per second bit rate that was seen by the system in both the inbound and outbound directions for the selected group/object.
Traffic	The total number of bytes that were seen by the system in both the outbound and inbound directions for the selected group/object. Byte counts are based on powers of 10, not powers of 2, e.g., 1 kB is 1,000 bytes, not 1,024 bytes.
Control Retrans	The number of control packets being retransmitted.
Control Retrans Rate	The rate of control packets being retransmitted.
% Control Retrans	The percentage of control packets that were retransmitted (SYN, SYN-ACK). This is $100 * (\text{number of retrans control packets}) / (\text{number of total control packets})$, where total control packets are the control packets plus the retrans control packets.

Metric	Description
Control Packets	The number of control packets (SYNs, SYN ACKs).
Control Packet Rate	The rate of control packets (SYNs, SYN ACKs).
Out-of-Order TCP Segments	The percentage of total Request and Response packets received out of order relative to the total number of packets used to transmit the Request and Response.
Out-of-Order TCP Client Segments	The percentage of client-to-server Request packets received out of order relative to the total number of packets used to transmit the Request.
Out-of-Order TCP Server Segments	The percentage of server-to-client Response packets received out of order relative to the total number of packets used to transmit the Response.
Out-of-Order TCP Segment Rate	The rate, in packets per second, of the total packets received out of order for the Request and Response.
Out-of-Order TCP Client Segment Rate	The rate, in packets per second, of the packets received out of order for the Request from client-to-server.
Out-of-Order TCP Server Segment Rate	The rate, in packets per second, of the packets received out of order for the Response from the server-to-client.
Out-of-Order TCP Traffic	The sum of the server-to-client and client-to-server bytes that were received out of order in the applicable time interval. Byte counts are based on powers of 10, not powers of 2, e.g., 1 kB is 1,000 bytes, not 1,024 bytes.
Out-of-Order TCP Client Traffic	The number of client-to-server bytes that were received out of order in the applicable time interval. Byte counts are based on powers of 10, not powers of 2, e.g., 1 kB is 1,000 bytes, not 1,024 bytes.
Out-of-Order TCP Server Traffic	The number of server-to-client bytes that were received out of order in the applicable time interval. Byte counts are based on powers of 10, not powers of 2, e.g., 1 kB is 1,000 bytes, not 1,024 bytes.
Out-of-Order TCP Throughput	The rate, in bits per second, of the sum of the client-to-server and server-to-client bytes that were received out of order.
Out-of-Order TCP Client Throughput	The rate, in bits per second, required to transmit all client-to-server Request bytes that were received out of order.
Out-of-Order TCP Server Throughput	The rate, in bits per second, required to transmit all server-to-client Response bytes that were received out of order.
Client TCP Receive Window	The client-to-server TCP Window value that were seen in the applicable time interval.
Server TCP Receive Window	The server-to-client TCP Window value that were seen in the applicable time interval.
Zero Window TCP Segments	The sum of the number of client-to-server and server-to-client Zero Window segments that were seen in the applicable time interval.
Zero Window TCP Client Segments	The number of client-to-server Zero Window segments that were seen in the applicable time interval.

Metric	Description
Zero Window TCP Server Segments	The number of server-to-client Zero Window segments that were seen in the applicable time interval.
Zero Window TCP Segment Rate	The sum of the average rates of client-to-server and server-to-client Zero Window segments that were seen in the applicable time interval.
Zero Window TCP Client Segment Rate	The rate at which client-to-server Zero Window segments were seen in the applicable time interval.
Zero Window TCP Server Segment Rate	The rate at which server-to-client Zero Window segments were seen in the applicable time interval.
Connection Open Mode	Indicates how the TCP connection started: 3WH-Full 3WH-Partial Pre-Existing Open Other
Connection Close Mode	Indicates how the TCP connection was closed: By-Fin By RST Other
MSS	The Advertised TCP MSS value provided by the endpoints in the TCP options.
Option Wind. Scaling	Indicates if the TCP Windows Scaling Option is used.
Option SACK	Indicates if the TCP Selective Ack Option is used.
Option - Fast Open	Indicates if the TCP Fast Open Option is used.
TCP In-Flight Data (bytes)	The amount of data sent from the TCP source, but not yet acknowledged by the destination.

Citrix Analysis (CXA) Metrics

The CXA metrics that are collected or calculated are:

Metric	Description
Transaction Metrics	
Published App/Desktop	Application name (derived from the process, example: Firefox).
Citrix Client	End user host address (DNS name if resolved, else IP).
Citrix Client Country	Country name associated with the client IP (example: "United States of America").
Citrix Client Host Group IDs	Host Group IDs associated with the end user IP.
Citrix Client Host Groups	Host Groups associated with the end user IP.
Citrix Client Hosts	Number of end user IPs associated with current Citrix session.
Citrix Client IP	End user IP.
Citrix Client Region	Region name associated with the end user IP (example: "Maryland").
Citrix Server	Citrix server host address (DNS name if resolved, else IP).
Citrix Server Country	Country name associated with the server IP (example: "United States of America").
Citrix Server Host Group IDs	Host Group IDs associated with the Citrix Server IP.
Citrix Server Host Groups	Host Groups associated with the Citrix Server IP.

Metric	Description
Citrix Server IP	Citrix Server IP actively being used.
Citrix Server Region	Region name associated with the server IP (example: "Maryland").
Citrix Servers	Number of Citrix Server IPs associated with current Citrix session.
Citrix Session Duration	Citrix session duration. It is computed by subtracting the end time from the start time.
Citrix Session End Time	Citrix session end time.
Citrix Session ID	Citrix session unique ID (computed internally, assigning different IDs when end user sessions move from one host or client IP to another).
Citrix Session Start Time	Citrix session start time.
Citrix Sessions Finished	Number of Citrix sessions finished.
Citrix Sessions Started	Number of Citrix sessions started.
Unique Citrix Sessions	Number of unique Citrix sessions (computed based on Citrix Session ID).
ICA/CGP Compression Ratio	This is a bi-directional measurement (Client to Server and Server to Client). The ratio is computed by dividing the total payload bytes sent/received after compression by the total payload bytes sent/received before compression (since the last reboot). Ratio = "ICA/CGP Traffic" / "ICA/CGP Uncompressed Traffic". It is an average computed from samples collected on remote agents.
ICA/CGP Request Compression Ratio	Client (end user) to Server (Citrix Server) ICA/CGP compression ratio. The ratio is computed by dividing the total payload bytes received after compression by the total payload bytes received before compression (since the last reboot). Ratio = "ICA/CGP Request Traffic" /
ICA/CGP Uncompressed Request Traffic	Client (end user) to Server (Citrix Server) ICA/CGP uncompressed traffic. It is the total payload bytes received before compression. It is an average computed from samples collected on remote agents.
ICA/CGP Request Throughput	Client (end user) to Server (Citrix Server) ICA/CGP throughput. It is an average computed from samples collected on remote agents.
ICA/CGP Request Traffic	Client (end user) to Server (Citrix Server) ICA/CGP traffic. It is the total payload bytes sent after compression. It is an average computed from samples collected on remote agents.
ICA/CGP Response Compression Ratio	Server (Citrix Server) to Client (end user) ICA/CGP compression ratio. The ratio is computed by dividing the total payload bytes sent after compression by the total payload bytes sent before compression (since the last reboot). Ratio = "ICA/CGP Response Traffic" / "ICA/CGP Uncompressed Response Traffic". It is an average computed from samples collected on remote agents.
ICA/CGP Response Throughput	Server (Citrix Server) to Client (end user) ICA/CGP throughput. It is an average computed from samples collected on remote agents.
ICA/CGP Response Traffic	Server (Citrix Server) to Client (end user) ICA/CGP traffic. It is the total payload bytes sent after compression. It is an average computed from samples collected on remote agents.

Metric	Description
ICA/CGP Round Trip Time	This is a bi-directional measurement (Client to Server and Server to Client). It is an average computed from samples collected on remote agents.
ICA/CGP Throughput	This is a bi-directional measurement (Client to Server and Server to Client). It is an average computed from samples collected on remote agents.
ICA/CGP Traffic	This is a bi-directional measurement (Client to Server and Server to Client). It is the total payload bytes sent/received after compression. It is an average computed from samples collected on remote agents.
ICA/CGP Uncompressed Response Traffic	Server (Citrix Server) to Client (end user) ICA/CGP uncompressed traffic. It is the total payload bytes sent before compression. It is an average computed from samples collected on remote agents.
ICA/CGP Uncompressed Traffic	This is a bi-directional measurement (Client to Server and Server to Client). It is the total payload bytes sent/received before compression. It is an average computed from samples collected on remote agents.
Roll-up Metrics	
Published App/Desktop	Application name (example: Firefox).
Citrix Server	Citrix server host address (DNS name if resolved, else IP).
Citrix Server Country	Country name associated with the server IP (example: "United States of America").
Citrix Server Host Group IDs	Host Group IDs associated with the Citrix Server IP.
Citrix Server Host Groups	Host Groups associated with the Citrix Server IP.
Citrix Server IP	Citrix Server IP actively being used.
Citrix Server Region	Region name associated with the server IP (example: "Maryland").
Citrix Session Duration	Citrix session duration. It is computed by subtracting the end time from the start time.
Citrix Sessions Finished	Number of Citrix sessions finished.
Citrix Sessions Started	Number of Citrix sessions started.
ICA/CGP Compression Ratio	This is a bi-directional measurement (Client to Server and Server to Client). The ratio is computed by dividing the total payload bytes sent/received after compression by the total payload bytes sent/received before compression (since the last reboot). Ratio = "ICA/CGP Traffic" / "ICA/CGP Uncompressed Traffic". It is an average computed from samples collected on remote agents
ICA/CGP Request Compression Ratio	Client (end user) to Server (Citrix Server) ICA/CGP compression ratio. The ratio is computed by dividing the total payload bytes received after compression by the total payload bytes received before compression (since the last reboot). Ratio = "ICA/CGP Request Traffic" /
ICA/CGP Uncompressed Request Traffic	Client (end user) to Server (Citrix Server) ICA/CGP uncompressed traffic. It is the total payload bytes received before compression. It is an average computed from samples collected on remote agents.

Metric	Description
ICA/CGP Request Throughput	Client (end user) to Server (Citrix Server) ICA/CGP throughput. It is an average computed from samples collected on remote agents.
ICA/CGP Request Traffic	Client (end user) to Server (Citrix Server) ICA/CGP traffic. It is the total payload bytes sent after compression. It is an average computed from samples collected on remote agents.
ICA/CGP Response Compression Ratio	Server (Citrix Server) to Client (end user) ICA/CGP compression ratio. The ratio is computed by dividing the total payload bytes sent after compression by the total payload bytes sent before compression (since the last reboot). Ratio = "ICA/CGP Response Traffic" / "ICA/CGP Uncompressed Response Traffic". It is an average computed from samples collected on remote agents.
ICA/CGP Response Throughput	Server (Citrix Server) to Client (end user) ICA/CGP throughput. It is an average computed from samples collected on remote agents.
ICA/CGP Response Traffic	Server (Citrix Server) to Client (end user) ICA/CGP traffic. It is the total payload bytes sent after compression. It is an average computed from samples collected on remote agents.
ICA/CGP Round Trip Time	This is a bi-directional measurement (Client to Server and Server to Client). It is an average computed from samples collected on remote agents.
ICA/CGP Throughput	This is a bi-directional measurement (Client to Server and Server to Client). It is an average computed from samples collected on remote agents.
ICA/CGP Traffic	This is a bi-directional measurement (Client to Server and Server to Client). It is the total payload bytes sent/received after compression. It is an average computed from samples collected on remote agents.
CA/CGP Uncompressed Response Traffic	Server (Citrix Server) to Client (end user) ICA/CGP uncompressed traffic. It is the total payload bytes sent before compression. It is an average computed from samples collected on remote agents.
IICA/CGP Uncompressed Traffic	This is a bi-directional measurement (Client to Server and Server to Client). It is the total payload bytes sent/received before compression. It is an average computed from samples collected on remote agents.
Traffic Diagnostics	
<i>Discarded Connections (Flow Collector)</i>	
Flows discarded (full queue)	Number of flows discarded because the output queue is full.
<i>Discarded Connections (Flow Processor)</i>	
Flows discarded (out of order)	Number of discarded flows that are out of order.
Flows discarded (exceeding limit)	Number of discarded flows that exceed maximum limit (internal limit based on model).
Flows discarded (full queue)	Number of flows discarded because the output queue is full.
<i>Discarded Connections (Correlator)</i>	

Metric	Description
Report connections discarded (late arrival)	Number of agent flows discarded for late arrival.
Report connections discarded (early arrival)	Number of agent flows discarded for early arrival.
Report connections discarded (unmatched)	Number of agent flows discarded for being unmatched (we were unable to match the agent flows with the probe flows).
End-to-end transactional flows discarded	Number of end to end Citrix transaction flows discarded because output queue is full.
End-to-end summary flows discarded	Number of end to end Citrix roll-up flows because output queue is full.
Flows discarded (late arrival)	Number of probe flows (from packets) discarded for late arrival.
Flows discarded (early arrival)	Number of probe flows (from packets) discarded for early arrival.
Flows discarded (duplicate)	Number of duplicate flows discarded.
<i>Discarded Connections (Agent Processor)</i>	
Connections discarded (full queue)	Number of flows discarded because the output queue is full.
<i>Discarded Connections (Agent Processor)</i>	
Connections discarded (full queue)	Number of flows discarded because the output queue is full.
Connections discarded (invalid report)	Number of reports (agent bundles) discarded because the report is not valid (for example an unsupported format).
Connections discarded (invalid session)	Number of sessions (within reports) discarded because the session is not valid (for example an empty session).
Connections discarded (invalid)	Number of flows (within sessions) discarded because the connection is not valid (for example a null socket = IP=0, port=0)

Database Analysis (DBA) Metrics

The DBA metrics that are collected or calculated are:

Metric	Description
DB Sessions Busy (Max)	The maximum number of DB sessions that had some query/response activity over the applicable time period.
DB Sessions Busy	The average number of DB sessions that had some query/response activity over 1-minute buckets.
Concurrent DB Sessions (Max)	The maximum number of open DB sessions that were present (regardless of query/response activity) over time.
Concurrent DB Sessions	The average number of open DB sessions that were present (regardless of query/response activity).
DB Session Event Duration	The total number of minutes the DB session was active this period.

Metric	Description
DB Sessions Idle (Max)	The maximum number of DB sessions that had non-zero idle time in the applicable time period.
DB Sessions Idle	The average number of DB sessions that had non-zero idle time over 1-minute buckets.
DB Instance	The user-configured name of the DB instance associated with the selected group.
Client Process Name	The name of the process in the workstation/server that represents the user side of a DB session. The availability of this information varies by DB vendor.
DB Session Busy Time	This is the total time of all DB sessions that were active (meaning that a query was ongoing) over the observation interval. If you have 2 DB sessions, one lasting 2 min. with 1 min. activity, and another lasting 5 min. with 2 min. activity, you will see 3 min. for this value.
Duration Logged In	This is the total time of all DB sessions that were logged in over the observation interval. If you have 2 DB sessions, one lasting 2 min., and another lasting 5 min., you will see 7 min. for this value.
DB Sessions Detected After Login	The number of DB sessions for which no login was observed, but that were inferred as being DB sessions.
DB Session ID	A session ID, usually auto-assigned by DBMS.
DB Session Idle Time	This is the total time of all DB sessions that were idle (meaning that no query was ongoing), rather than busy over the observation interval. If you have 2 DB sessions, one lasting 2 min. with 1 min. idle, and another lasting 5 min. with 2 min. idle, you will see 3 min. for this value.
DB Sessions Discarded Due To Shutdown	This is the number of sessions discarded due to an AR11 shutdown, not a DBMS shutdown. When AR11 is shutdown, the sessions that were active before the shutdown are discarded when the AR11 comes back up.
New DB Session Logins	The number of new DB sessions that were seen in the applicable time interval that had a login sequence in the beginning.
DB Session Logouts	The number of DB sessions that ended with a detected logout sequence.
DB Sessions Refused	The number of DB session logins that were unsuccessful because the DBMS refused to create sessions, e.g., because of a bad password.
DB Sessions Discarded Due To Inactivity	The number of DB sessions that did not have any query activity or a logout sequence and are presumed to have ended.
DB Sessions Finished	The total number of DB sessions that ended for any reason. This is the sum of DB sessions that ended because of logout, refusal, or inactivity timeout.
New DB Sessions	The total number of new DB sessions that involved a login sequence and new ones that were detected after a login sequence that was not observed. This is the sum of "New DB Session Logins" and "DB Sessions Detected After Login".
DB Type	The DB type (e.g., Oracle).

Metric	Description
DB Username	The username that was used to login when creating the DB session.
Client Username	The user name used to log into the client system (e.g., Windows workstation/laptop), making queries and receiving responses.
Data Transfer Time (Max)	The maximum time it took to transfer a contiguous chunk of query response data, i.e, from the first row to the last row. This time includes any data transfer time observed at the TCP layer in addition to the processing time it took the DB server to send the full response. This is the maximum transfer time for any given DB query in the group over the observation interval.
Data Transfer Time	This is the time it took to transfer the data returned in the selected query, including the transfer time for the request, e.g., the UPDATE command.
Data Transfer Time	This is the average time it took to transfer the data returned in the selected query, including the transfer time for the request, e.g., the UPDATE command.
Transaction Time	The average of the sums of relevant Data Transfer Time + Server Response Time metric values for all queries relevant to the selected group. This is the average transaction time of a DB query from first byte sent to the last byte received.
Transaction Time	The sum of relevant Data Transfer Time + Server Response Time metric values for all query instances relevant to the selected query. This is the transaction time of the selected DB query from the first byte sent to the last byte received.
Transaction Time (Max)	The maximum duration of the query from the request to the last packet of the response message. This is the longest query that has been observed within the group during the observation window.
Packets Per Response (Max)	The maximum number of packets in any DB response sent by DB servers. This represents the largest DB response in terms of packets.
Request Packet Rate	The packet rate of DB requests sent to DB servers.
Packets per Request (Max)	The maximum number of packets in any DB request sent to DB servers. This represents the largest DB request in terms of packets that has been observed in the group.
Response Packets	The total number of packets sent in the DB response by the DB server for the DB query (this applies to a single DB query, not an aggregate).
Request Packets	The total number of packets sent in the DB request to the DB server for the DB query (this applies to a single DB query, not an aggregate).
Packets per Request	The average number of packets in a DB request sent to DB servers.
Packets per Response	The average number of packets in a DB response sent by DB servers.
Request Packet Traffic	The total number of packets sent as DB requests to DB servers.
Response Packet Rate	The packet rate of DB responses sent by DB servers.
Response Packet Traffic	The total number of packets sent as DB responses by DB servers.
Finished Query Rate	The rate of DB queries that have been completed in the time interval.

Metric	Description
Queries Finished	The number of DB queries that have been completed in the time interval.
Queries Started	The number of DB queries that started in the time interval.
Queries Unfinished	The number of DB queries that are unfinished in the time interval. An unfinished DB query is a DB query has started either before or during the time interval, but has not yet completed at the end of the time interval.
Query Command	The DB query operation (e.g., SELECT, UPDATE, DROP, etc.)
Query End Time	The end time of an individual DB query.
Query Return Code	The DB query return code. For each DB query, the DB server returns a code in the DB response indicating whether the query was successful or not.
Query Serial Number	The unique query identifier.
Query Start Time	The start time of an individual query.
Query Status	The status of a query. The status can be one of "C" (=Completed), "I" (=Indeterminate), "R" (=Rejected).
Query Text	This is the SQL clause sent to the DB server to perform an operation.
Repetition Count	The number of times a single DB query repeated within a very short time (<1sec).
Affected Rows	Total number of rows affected by DB queries, either returned, modified, added or removed.
Affected Rows per Query	The average number of rows affected by a DB query over all the DB queries, either returned, modified, added, or removed.
Affected Rows per Query (Max)	The maximum number of rows affected by a DB query over all the DB queries, either returned, modified, added, or removed. This represents the largest number of rows that has been affected by a DB query in the group.
Affected Rows	The number of rows affected by an individual DB query.
Server Response Time (Max)	The maximum server response time across all DB queries. This represents the largest server response time experienced by any DB query in the group.
Server Response Time	The average server response time of DB queries in the group.
Server Response Time	The server response time experienced by the individual query.
Response Size (Max)	The maximum number of application bytes in a DB response sent by DB servers. This represents the largest DB response in terms of bytes.
Response Throughput	The application throughput of DB response traffic sent by DB servers.
Response Traffic	The number of application bytes sent by the DB Server in an individual DB query.
Request Traffic	The total number of bytes sent in DB requests sent to DB servers. This adds up the number of bytes from all DB requests in the group.

Metric	Description
Request Size (Max)	The maximum number of application bytes in a DB request sent to a DB server across all DB queries. This represents the largest number of bytes sent in a DB request by any DB query in the group.
Request Throughput	The application throughput of DB request traffic sent to DB servers.
Request Size	The average number of application bytes in DB requests sent to DB servers.
Response Traffic	The total number of application bytes sent in DB responses sent by DB servers. This adds up the number of bytes from all DB responses in the group.
Response Size	The average number of application bytes in DB responses sent by DB servers.
Request Traffic	The number of application bytes sent to the DB server in an individual DB query.
Server Hostname	The DNS-resolved name of the TCP server host.
Client Hostname	The DNS-resolved name of the TCP client host.
End Time	The TCP flow end time.
Server IP Address	The IP address of the TCP server host.
Client IP Address	The IP address of the TCP client host.
Server Port	The server TCP port.
Client Port	The client TCP port.
Start Time	The TCP flow start time.

Unified Communications Analysis (UCA) Metrics

AppResponse 11 UCA uses Telchemy's VQmon technology (<https://www.telchemy.com/vqmon.php>) to analyze and monitor the quality of audio and video media streams. Refer to **"Analysis Using VQmon"** for additional detail.

The UCA metrics that are collected or calculated are:

Metric	Description
Burst Duration	The maximum duration of packet loss burst for a single channel.
Bursts	The number of occurrences of packet loss burst for the channel.
Channel Duration	The duration of the RTP channel.
MOS-CQ (End of Call)	The conversational quality MOS score for the channel.
MOS-V (End of Call)	The average relative MOS score for the video stream.
Gap Duration	The maximum duration of no packet loss for a single channel.
Gaps	The number of occurrences of packet loss gap for the channel.
Jitter (Min)	The jitter of the single RTP channel for the current interval.

Metric	Description
Jitter (Max)	RTP channel jitter of the current interval
Jitter	RTP channel jitter of the current interval
Lost Packets	The number of packets that have never been received for an RTP stream for the current interval.
Interval MOS-CQ (Min)	The lowest channel conversational quality MOS score for the current interval.
Interval MOS-CQ	The average channel conversational quality MOS score for the current interval.
Interval MOS-CQ (Max)	The highest channel conversational quality MOS score for the current interval.
MOS-CQ (Min)	The minimum cumulative channel conversational quality MOS score.
MOS-CQ (Max)	The maximum cumulative channel conversational quality MOS score.
Interval Absolute MOS-V (Min)	The minimum absolute MOS score for the video stream for the current interval.
Interval Absolute MOS-V (Max)	The maximum absolute MOS score of the video stream for the current interval.
Interval Absolute MOS-V	The average absolute MOS score of the video stream for the current interval, where the interval is calculated every minute, for the minute.
Absolute MOS-V (Max)	The maximum cumulative absolute MOS score of the video stream.
Absolute MOS-V (Min)	The minimum cumulative absolute MOS score of the video stream.
Interval MOS-V (Min)	The minimum relative MOS score for the video stream for the current interval.
Interval MOS-V (Max)	The maximum relative MOS score for the video stream for the current interval.
Interval MOS-V	The average relative MOS score of the video stream for the current interval, where the interval is calculated every minute, for the minute.
MOS-V (Min)	The minimum cumulative relative MOS score of the video stream.
MOS-V (Max)	The maximum cumulative relative MOS score of the video stream.
Packet Traffic	The number of RTP packets in the stream for the current interval.
Corrected Packets	The maximum cumulative number of stream packets corrected by FEC.
Discarded Packets	The number of stream packets discarded by the endpoint due to late arrival for the current interval.
Out Of Sequence Packets	The maximum cumulative number of stream packets arriving out of sequence for the current interval.
Traffic	The number of RTP bytes in the stream for the current interval.
Throughput	The rate of RTP traffic, in bits per second.
Jitter (Min)	The lowest jitter value observed across all channels associated with the call at the time observed.

Metric	Description
MOS-CQ (Max)	The best MOS CQ score observed across all RTP streams associated with this call.
MOS-V (Max)	The best MOS video score observed across all RTP streams associated with this call.
Call Duration	The cumulative duration of the call.
Call Ended Status Value	The numerical value corresponding to the final call status (Canceled, Rejected, Completed or Timeout).
Status (End of Call)	The text name corresponding to the final call status (Canceled, Rejected, Completed or Timeout).
MOS-CQ (End of Call)	The worst final cumulative MOS CQ score observed across all RTP streams associated this call.
MOS-V (End of Call)	The worst final cumulative MOS video score observed across all RTP streams associated this call.
Post Dial Delay	The time delay between dial and call start.
Jitter (Max)	The highest jitter value observed across all channels associated with the call at the time observed.
MOS-CQ (Min)	The worst MOS CQ score observed across all RTP streams associated with this call.
MOS-V (Min)	The worst MOS video score observed across all RTP streams associated with this call.

Web Transaction Analysis (WTA) Metrics

The WTA metrics that are collected or calculated are:

Metric	Description
Client Busy Time	The calculated time spent by the end-user/browser between receiving a HTTP Response and sending a subsequent HTTP Request. This is the gap in time between a bar in the waterfall chart and its adjacent (in time) bar.
Client Busy Time (Normalized)	The relative amount of overall Page Time that was spent in end-user/browser processing time. This is calculated by comparing total Client/Server/Network Busy Times to each other and applying that relative proportion to overall Page Time.
Page Count ({user_label})	The number of Individual Page Views for which the attributes and values matched the definition of Custom Metric 1.
Page Count ({user_label})	The number of Individual Page Views for which the attributes and values matched the definition of Custom Metric 2.
Page Count ({user_label})	The number of Individual Page Views for which the attributes and values matched the definition of Custom Metric 3.
Page Count ({user_label})	The number of Individual Page Views for which the attributes and values matched the definition of Custom Metric 4.

Metric	Description
Page Count ({user_label})	The number of Individual Page Views for which the attributes and values matched the definition of Custom Metric 5.
Network Busy Time	The calculated time it took the network to transport HTTP Requests and Responses. This is distinct from the processing times in the end-user/browser and the web server.
Network Busy Time (Normalized)	The relative amount of overall Page Time that the network spent transporting HTTP Requests and Responses. This is calculated by comparing total Client/Server/Network Busy Times to each other and applying that relative proportion to overall Page Time.
Objects Requested	The number of HTTP Requests that were seen in the context of an Individual Page or coarser grained aggregate like a Page Family, Advanced Web App, etc.
Originating Hostname	The DNS-resolved hostname of end-user's/browser's IP address. If there were web proxies involved, this hostname will be different than the IP address that was seen in the L3 IP header of the HTTP packets that were analyzed.
Web User IP	The IP address of the end-user's/browser's host. If there were web proxies involved, this IP address is usually extracted from X-Forwarded-For headers and will not match the IP address that was seen in the IP header of the HTTP packets that were analyzed.
Page Family ID	A unique number that is used to internally associate Individual Page Views with the Page Families that were associated with it. This has no practical use for the end-user.
Page Views	The number of Individual Page Views that were observed for each coarser grained group/object such as Web App, Page Family, Geography, etc. Not available for IPVs.
Page View Rate	The per-second rate of Individual Page Views that were observed for each coarser grained group/object such as Web App, Page Family, Geography, etc. Not available for IPVs.
% 1xxs	The percentage of objects associated with a coarser grained group/object for which the HTTP Status Codes were ≥ 100 and < 200 , used to provide Information such as Continue or Processing.
% 2xxs	The percentage of objects associated with a coarser grained group/object for which the HTTP Status Codes were ≥ 200 and < 300 , used to indicate Success, such as OK, Created, Accepted.
% 304s	The percentage of objects associated with a coarser grained group/object for which the HTTP Status Code was 304, indicating Not Modified.
% 3xxs (Misc)	The percentage of objects associated with a coarser grained group/object for which the HTTP Status Codes were ≥ 300 and < 400 , used to indicate miscellaneous status, such as Moved Permanently or Found.
% 400s	The percentage of objects associated with a coarser grained group/object for which the HTTP Status Codes were ≥ 400 and < 500 , used to indicate Client Errors, such as Bad Request, Not Authorized, Forbidden, and Not Found.

Metric	Description
% 401s	The percentage of objects associated with a coarser grained group/object for which the HTTP Status Code was 401, indicating Unauthorized.
% 402s	The percentage of objects associated with a coarser grained group/object for which the HTTP Status Code was 402, indicating Payment Required.
% 403s	The percentage of objects associated with a coarser grained group/object for which the HTTP Status Code was 403, indicating Forbidden.
% 404s	The percentage of objects associated with a coarser grained group/object for which the HTTP Status Code was 404, indicating Not Found.
% 407s	The percentage of objects associated with a coarser grained group/object for which the HTTP Status Code was 407, indicating Proxy Authentication Required.
% 4xxs (Misc)	Percent of 4xx errors
% 500s	The percentage of objects associated with a coarser grained group/object for which the HTTP Status Codes were ≥ 500 , used to indicate Internal Server Errors, such as Not Implemented, Service Unavailable, and HTTP Version Not Supported.
% 501s	The percentage of objects associated with a coarser grained group/object for which the HTTP Status Code was 501, indicating Not Implemented.
% 503s	The percentage of objects associated with a coarser grained group/object for which the HTTP Status Code was 503, indicating Service Unavailable.
% 5xxs (Misc)	Percent of 5xx errors
% Slow Pages	The percentage of objects requested that exceeded the Slow Page Threshold value.
1xxs	The number of objects associated with a coarser grained group/object for which the HTTP Status Codes were ≥ 100 and < 200 , e.g., used to indicate Continue, Processing.
2xxs	The number of objects with a status code ≥ 200 and < 300 , used to indicate Success, such as OK, Created, Accepted.
304s	The number of objects with a status code of 304, indicating Not Modified.
3xxs (Misc)	The number of objects with a status code ≥ 300 and < 400 and $\neq 304$.
400s	The number of objects with a status code of 400, indicating Bad Request.
401s	The number of objects with a status code of 401, indicating Unauthorized.
402s	The number of objects with a status code of 402, indicating Payment Required.
403s	The number of objects with a status code of 403, indicating Forbidden.

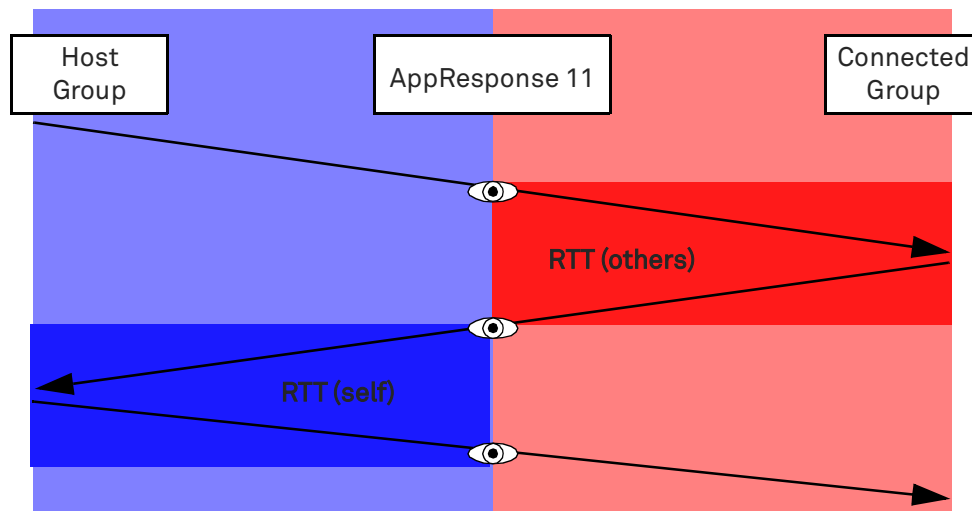
Metric	Description
404s	The number of objects with a status code of 404, indicating Not Found.
407s	The number of objects with a status code of 407, indicating Proxy Authentication Required.
4xxs (Misc)	The number of objects with a status code > 404 and < 500 and != 407.
500s	The number of objects with a status code of 500, indicating Internal Server Error.
501s	The number of objects with a status code of 501, indicating Not Implemented.
503s	The number of objects with a status code of 503, indicating Service Unavailable.
5xxs	The number of objects with a status code of 500 and greater.
5xxs (Misc)	The number of objects with a status code of 502 or > 503.
Server Busy Time	The amount of time it took a web server to start sending HTTP Responses after receiving the corresponding HTTP Requests. This is distinct from the processing times in the end-user/browser and the network.
Server Busy Time (Normalized)	The relative amount of overall Server Busy Time that the server took to start responding to HTTP Requests. This is calculated by comparing total Client/Server/Network Busy Times to each other and applying that relative proportion to overall Page Time.
Slow Pages	The number of Individual Page View whose Page Times were greater than the applicable Slow Page Threshold. It is possible for an Individual Page View to be associated with multiple Web Applications and Page Families. If you are looking at this metric for a Web Server IP->Web App group path, the # of slow pages for that Web Server IP may not be the sum of this metric's values for the Web Apps shown for that Web Server IP.
Slow Page Rate	The number of pages exceeding the Slow Page Threshold value.
Page Time	The total amount of elapsed time for the end-user/browser to receive HTTP Responses for all the HTTP Requests that constituted an Individual Page View. If an IPV contains a hundred objects, this is the time it took for all those objects to be received by the browser.
Page Response Traffic	The sum, in bytes, of all HTTP responses (body plus header).
Page Response Throughput	The average rate, in bytes per second, of all HTTP responses (body plus header).
Page Request Traffic	The sum, in bytes, of all HTTP requests (body plus header).
Page Request Size	The average size, in bytes, of all HTTP requests (body plus header).
Page Size	The average number of bytes that made up all the headers and bodies of the HTTP Requests and Responses that were stitched into Individual Page Views. This is a measure of how many bytes were involved in a single page.

Metric	Description
Page Traffic	The total number of bytes that made up all the headers and bodies of the HTTP Requests and Responses that were stitched into Individual Page Views. This is a measure of how many bytes were involved in all the IPVs associated with the selected group/object.
Page Response Size	The average size, in bytes, of all HTTP responses (body plus header).
Page Request Throughput	The average rate, in bytes per second, of all HTTP requests (body plus header).
Page Throughput	The average rate, in bytes per second, of all HTTP requests and responses (body plus header).
User ID	An internal ID that is used to map User Names with Individual Page Views. This is not useful to the end-user.
User	The Username that was derived from applying User Session Tracking rules to the Individual Page View. In most cases, this represents the username who logged in and setup the web sessions that produced all the Individual Pages.

Round Trip Time

This metric is an estimate of how quickly the network between the client and server would transport TCP bits in both directions if the client and server were infinitely fast, and took no time to respond to Responses and Requests.

As of AppResponse 11 Version 11.10.0, Round Trip Time (RTT) comprises two distinct metrics: RTT (self) and RTT (others). RTT (self) is the round trip time as the traffic passes the AppResponse 11 system both from and to the originating IP address or host group. (This is similar to the RTT inbound metric that was used in AppResponse 9.) RTT (others) is the round trip time from when the traffic passes the AppResponse 11 system to when it arrives at another network element, such as an IP address or host group. (This is similar to the RTT outbound metric that was used in AppResponse 9.) RTT, undifferentiated as either (self) or (others), is the sum of the two constituent RTTs: $RTT = RTT (self) + RTT (others)$.



Security Mechanisms for General Access

AppResponse 11 users can access an AppResponse 11 system via three methods.

Method 1: Browser/Web UI access

The Web UI is accessible from HTTPS, with the customer able to supply their own SSL certificate. HTTP can be enabled, but is insecure. Users authenticate with username/password through Local, RADIUS, or TACACS+ authentication methods. User authentication with SAML is also supported. With SAML enabled, the user credentials depends on the IdP used; e.g., CAC cards may be supported. Once authenticated, further communications use OAUTH2 with signed JWT access tokens.

Method 2: REST API

REST API access is accessible from HTTPS, with the customer able to supply their own SSL certificate. HTTP can be enabled, but is insecure. Users authenticate with username/password through Local, RADIUS, or TACACS+ authentication methods. Once authenticated, further communications use OAUTH2 with signed JWT access tokens.

Method 3: CLI

The CLI is accessible from SSH and serial port. Users authenticate with username/password through Local, RADIUS, or TACACS+ authentication methods. Internally, the CLI makes the same REST calls as the Web UI does. The commands are protected by OAUTH2 + JWT.

Security Mechanisms for Captured/Stored Packets

AppResponse 11 users decide which packets are stored on/captured to disk. (Part of AppResponse 11 setup and configuration is deciding which users should have the admin privileges to create/update Capture Job configurations that control which packets are – and are not – captured on disk.)

AppResponse 11 stores packets to disk exactly as they were seen “on the wire” – in-the-clear packets are stored as such, encrypted packets are stored as encrypted packets.

AppResponse 11 users can optionally supply private keys that allow AppResponse 11 to decrypt packets (i.e., HTTPS) that involve the specific servers the private keys relate to. The packet analysis that is done on these decrypted packets produces the packet metadata (groups/objects and related metrics/statistics) that are calculated by the ASA and WTA feature modules. Even though AppResponse 11 can decrypt encrypted packets and calculate packet metadata from them, it will continue to store those packets on disk as encrypted packets.

AppResponse 11's RBAC architecture supports an explicit permission that controls if an AppResponse 11 user has access to the packets stored in AppResponse 11, as shown here:

Edit Role

Name: System Administrator

Description: System Administrator

Permission	No Access	View Only	Full Control
User Management User account, roles and password policy	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Access Other Users' Objects Read/Edit other users' private Insights, reports, schedules etc.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
System configuration Configuration settings in Administration menu	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Access Packets / Live Views Packet export/download, apply PA+ live views	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Configure Trace Clips Trace clip configuration	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Feature Settings and Definitions Feature Settings sub-menu and definitions	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Apply Revert

As a result, only users who have been assigned a role that has given **Full Control** for this **Access Packets/Live Views** permission can access packet data in AppResponse 11. (Again, part of AppResponse 11 setup and configuration is deciding which users should have this permission.) This is the fundamental mechanism that controls which users have access to packets in an AppResponse 11 system. This applies to all users who are authenticated via any of the supported authentication mechanisms: Locally, or via TACACS+, or via RADIUS, or via a SAML-enabled system. This also applies regardless of whether users interact with an AppResponse 11 appliance via its web UI, via Packet Analyzer Plus, or via the published AppResponse 11 REST API.

AppResponse 11 users (whose role grants **Full Control** to the **Access Packets/Live Views** permission) can access packets via the web UI, Packet Analyzer Plus, and the AppResponse 11 REST API. Again, all packets that are accessed by any of these methods will be the packets as they are stored on-disk – in-the-clear packets will be downloaded as such, encrypted packets will be downloaded as encrypted packets. What this means:

- If you want to analyze packets downloaded from AppResponse 11 in Packet Analyzer Plus (or Transaction Analyzer, Wireshark, etc.) that are encrypted, you will need to obtain/supply the private keys needed for decrypting those packets via some other means.
In other words, you can download encrypted packets but you *cannot* download the private keys that you configured in AppResponse 11 to allow it to do real-time packet decryption.
- Once you configure AppResponse 11 to use private keys for real-time packet decryption, there is no way to extract those private keys off the AppResponse 11 appliance for any offline packet analysis.

The AppResponse 11 8180 model (only) supports the option for an additional level of data-at-rest encryption for all packet (and non-packet metadata) that is stored on one or more 120 TB storage units that are attached to an 8180.

Security Mechanisms for SSL/TLS Keys

As part of normal product use, AppResponse 11 users routinely provide the following types of sensitive information:

- SSL/TLS private key to secure browser-appliance and REST API-appliance communication (for management/admin and data analysis)
- SSL/TLS private keys to decrypt encrypted traffic for individual servers (usually web)
- SSL/TLS private key
- to secure the enhanced NetFlow information that an AR11 appliance can export to NetProfiler
- SSL/TLS private key to secure the communication between AR11 and a SAML IdP (if the AR11 user has chosen to use SAML)

This user-provided information is automatically encrypted and stored in a secure vault in the appliance. The vault is protected by a key that is auto-generated algorithmically and is known only to the software running on the appliance. The information in the vault is decrypted/unlocked during normal boot and is made available in system memory for use by relevant software components. Once the user inputs any sensitive information into the vault, there is no way to get that information out of the vault, i.e., AppResponse 11 does not support copying or exporting information out of the vault. This means, this sensitive info is protected even if someone were to get physical access to AppResponse 11's hard disks.

