riverbed

SteelCentral™ AppResponse 11 User's Guide

Version 11.4.x

March 2018

riverbed®

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

Part Number
712-00302-05

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
italics	Within text, new terms and emphasized words appear in *italic* typeface.
boldface	Within text, CLI commands, CLI parameters, and REST API properties appear in **bold** typeface.

Courier	Code examples appear in Courier font:
	`amnesiac > enable`
	`amnesiac # configure terminal`

< >	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.

1

Overview

AppResponse 11 Web User Interface

The Home page opens when you sign-in to SteelCentral AppResponse. A Monitoring Interface Group (MIfG), default_mifg, containing all monitoring interfaces is automatically configured. A capture job, default_job, using default_mifg 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 addreses 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.

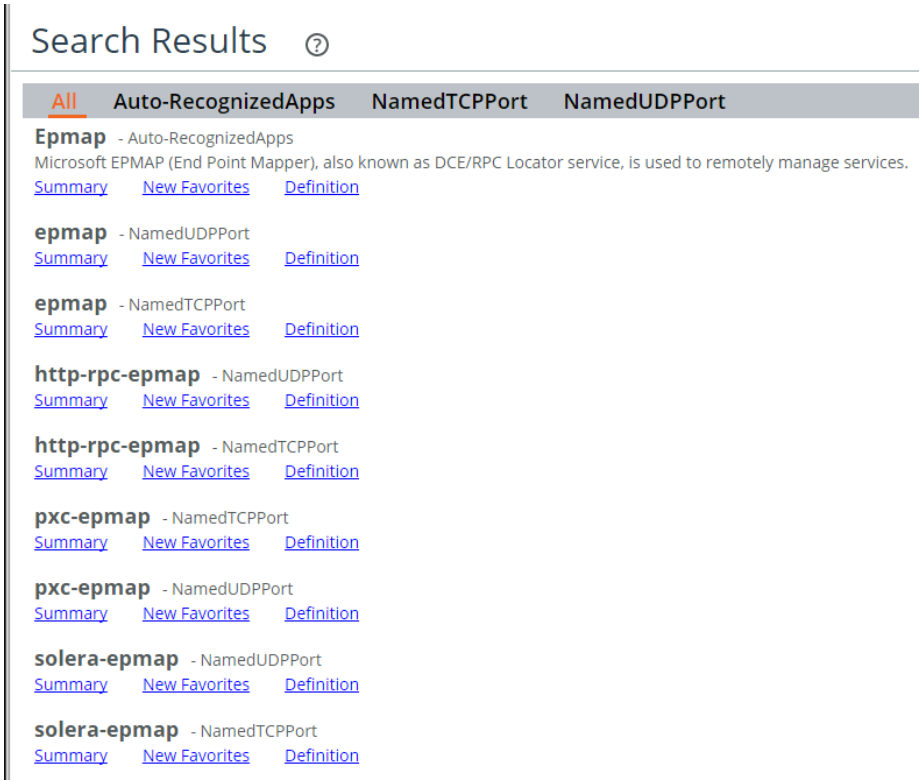
Search Result Tabs

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 Epmap. 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.



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, “Epmap- 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."

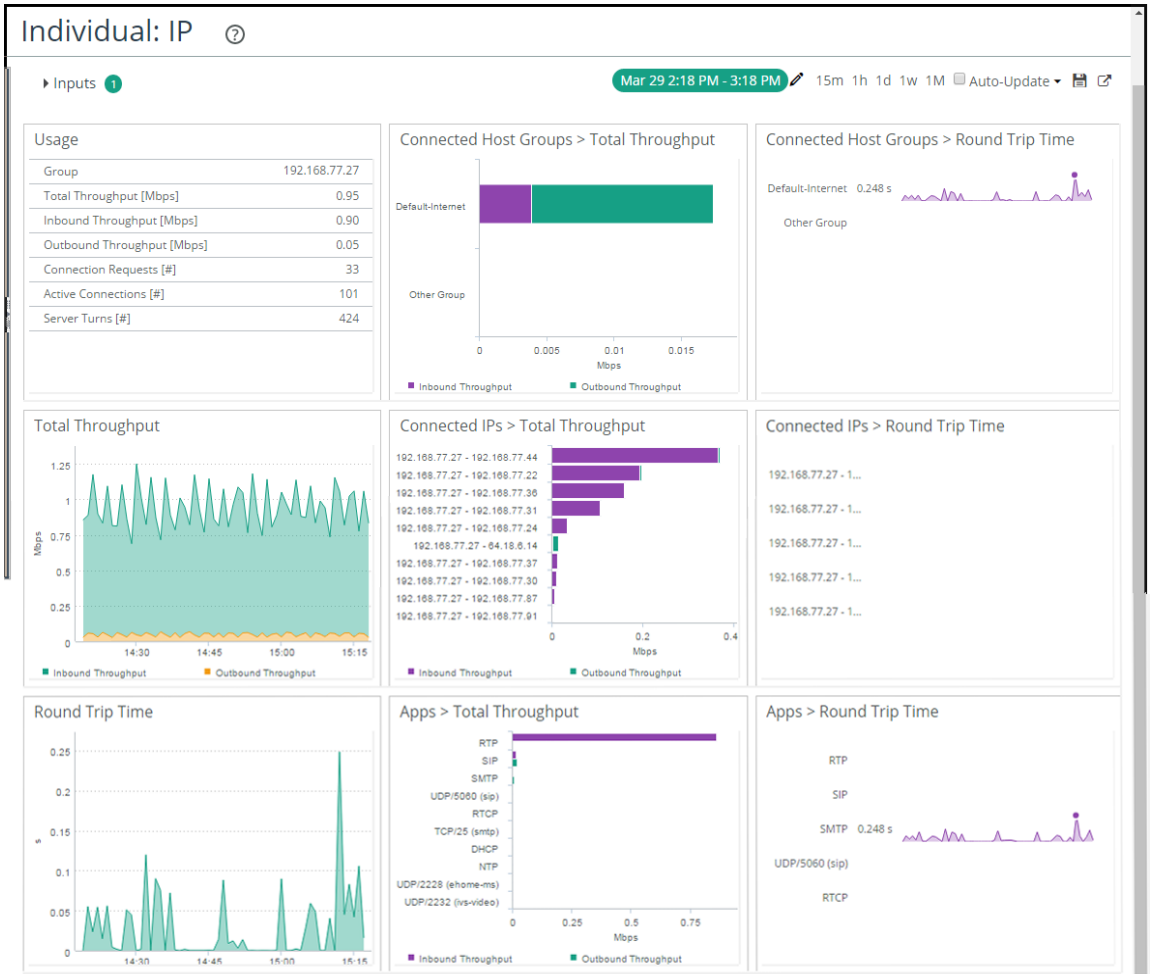
You can investigate the other search results tabs to find the TCP port or UDP port assigned to the Epmap application.

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:

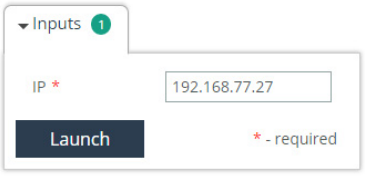
- IP Address
- General/URL App
- Host Group
- Web App
- Web User Group
- DB Server IP
- DB Client IP

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:



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. You use this web UI page to configure and manage each interface.

All detected interfaces and their status are listed under Monitoring Interfaces. A monitoring interface can be edited (see "Editing a Monitoring Interface" on page 9):

- 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 *monitoring interface group* (MIfG) is a logical grouping of one or more monitoring interfaces. AppResponse treats all physical or virtual interfaces in the same MIfG as one interface. To see what interfaces are used by a Monitoring Interface Group, go to Administration > System Settings: Monitoring Interface Groups web UI page. For more information, see "Monitoring Interface Groups (MIfGs)" on page 42.

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

This section discusses the following:

Using Packet Brokers

AppResponse 11 appliances can select from a set of supported packet brokers.

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.

Using a packet broker requires the following:

- Timestamps are correctly configured 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.
- The correct packet broker is selected. If the wrong packet broker is selected, timestamps may not be successfully processed, causing packets to be dropped. If a packet broker is selected but no packet broker is being used, timestamp processing also can result in dropped packets.

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.

To use a packet broker

1. Go to Administration > System Settings: Monitoring Interfaces.
2. Under General Configuration, 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 > System Settings: Monitoring Interfaces.
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 drop-down list.

7. 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:

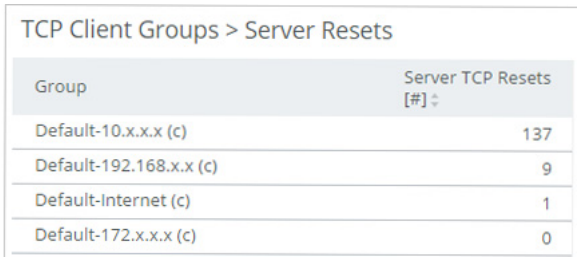
  - Total Data Transfer Time [sec]
  - Request Data Transfer Time [sec]
  - Response Data Transfer Time [sec]

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

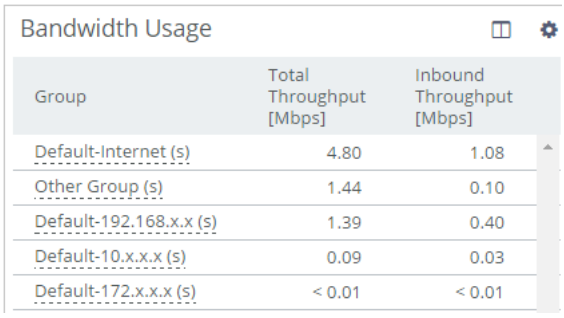
A Host Group can include both Clients and Servers. When you see a group that reads "*Group* (c)" the group refers to all IP addresses in the group that sent TCP data requests within the current time interval.

Figure 1-1. Client Groups



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



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

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 also have been revised in this release:

- **Throughput for Host Groups**—now 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. Previously, it was split into two metrics, Inbound and Outbound, relative to location of AppResponse.
- **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)

Two new sets of 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

In 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 wants 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 110 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 (11.1 or later) 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 11Host 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 U (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 11Favorites 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.

2

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

With a license, Feature Keys are installed automatically ifAppResponse 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 11virtual 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 he 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.

User Administration

This page provides controls for creating and managing user accounts for AppResponse 11.

- **User Administration tab**—Create and manage individual user accounts, including their role-based privileges.
- **Account Policy tab**—Configure global login and password policies for all user accounts.

User Administration tab

The User Administration 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 User Administration 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. **Password Never Expires**—Click this option if there is no need for the user to change the account password periodically.
7. **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.

Account Policy tab

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

- Allow Empty Passwords
- Failed Attempts to Lock Account
- Minutes to Lock Account
- 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
- Number of Days the Password is Valid
- Number of Days to Lock Account After Password Expiration
- Number of Days to Warn User Before Password Expiration

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. You can use the Administration > Authentication: Roles and Permissions page to create additional user roles.

To create a new user role:

1. Go to the Administration > Authentication: Roles and Permissions page.
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 on the Administration > Authentication: Roles and Permissions page. After being defined, the role becomes available to be assigned to individual user accounts on the Administration > Authentication: User Administration page.

To edit a user role:

1. Go to the Administration > Authentication: Roles and Permissions page.
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 and password expiration settings

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

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.

- 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

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

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 35 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.

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 35 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 35).

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 11appliance or virtual edition.

Specifying Authentication Types

1. Go to Administration > Authentication: Remote Authentication to display the Authentication Configuration page.
2. Select the Remote Authentication 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 > Authentication: Remote Authentication.
2. Select the Remote Authentication 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 83). These roles are shown under Default Roles at the bottom of the Remote Authentication tab.

Configuring default roles

1. Go to Administration > Authentication: Remote Authentication.
2. Select the Remote Authentication 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 > Authentication: Remote Authentication.
2. Select the RADIUS Configuration 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 > Authentication: Remote Authentication.
2. Select the RADIUS Configuration 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 > Authentication: Remote Authentication.
2. Select the TACACS+ Configuration 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.
7. 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

1. Go to Administration > Authentication: Remote Authentication.
2. Select the TACACS+ Configuration 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.

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 83.

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"
    }
}
```

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 > Authentication: Remote Authentication.
2. Select the SAML 2.0 Configuration 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+.

Monitoring Interface Groups (MIfGs)

A *monitoring interface group* (MIfG) is a logical grouping of one or more monitoring interfaces. AppResponse treats all physical or virtual interfaces in the same MIfG as one interface. A MIfG can be configured to remove duplicate packets. Also, a filter can be applied to MIfG traffic.

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

Each interface on a Windows system running Packet Analyzer Plus is assigned a default MIfG name. These MIfGs cannot be modified.

A default MIfG, *default_mifg*, containing all monitoring interfaces is automatically created when AppResponse 11 is installed. A default capture job, *default_job*, is also configured. Traffic analysis is done on all configured MIfGs. Monitoring interfaces with traffic must be a member of a MIfG if that traffic is to be analyzed.

This section discusses the following:

Monitoring Interface Group Configuration

When planning and configuring MIfGs, keep in mind the following:

- A monitoring interface can be a member of *only one* MIfG.
- A MIfG has one or more monitoring interface members.
- The maximum number of MIfGs 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 MIfG must have a unique name. If a MIfG is deleted, that name can then be used by another MIfG.
- Any changes to a MIfG takes effect immediately.

Monitoring Interface Groups Page

Choose Administration > System Settings: Monitoring Interface Groups.Select a radio button at the top to view:

- Monitoring Interface Groups by monitoring interfaces.
  - Edit a group to change name. description, interfaces, filter, and enable or disable deduplication.
- Monitoring Interfaces by monitoring interface groups.

- Edit a monitoring interface to change its monitoring interface group membership.

Creating or Editing a Monitoring Interface Group

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

1. Choose Administration > System Settings: Monitoring Interface Groups.
2. Select Monitoring Interface Groups.
3. Add or Edit?
   - Click **Add** to create a new MIfG.
   - To edit, hover with your mouse over an existing MIfG and click the pencil icon on the right.
4. Specify or select the following fields:
   - Name
   - Description
   - Interfaces - select a monitoring interface from the drop-down list. Click **x** next to an existing interface name to remove it from the MIfG.
   - Filter- Enter a BPF (default) or SteelFilter filter for MIfG traffic. Traffic dropped by a filter is not analyzed or stored in packet storage.
   - Enable Deduplication - Packet deduplication is done on a per MIfG basis - packets are only identified as duplicates of other packets in the same MIfG.

Deleting a Monitoring Interface Group

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

Managing Monitoring Interface Group Members

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

1. Choose Administration > System Settings: Monitoring Interface Groups.
2. Select Monitoring Interfaces.
3. Hover with your mouse over a monitoring interface and click the pencil icon on the right.
4. In the Monitoring Interface Group field, click the expansion icon to open a drop-down list of choices.
5. To change membership to a different MIfG, click the target MIfG name from the list.
   To remove from a MIfG, click **Unassigned**.
6. 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.

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 Monitoring Interface Group (MIfG) 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 BPF filter per MIfG.

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 45
- "Checking Flow Export Status" on page 46

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 > System Settings: Flow Export in the web U.
2. Select Enable Flow Export. This enables export to NetProfiler/Flow Gateway and NetFlow collectors.
3. Select Include All Interface Groups or include individual interface groups from the list of configured MIfGs.
   - A BPF filter can be specified for the selected MIfG.
4. Select VOIP Quality metrics o export VOIP quality metrics (no Telchemy metrics).
5. Enter the hostname or IP address of each NetProfiler/Flow Gateway to receive the flow exports.
   - NetProfiler does not support NetFlows from IPv6 exporters.
6. To manage port name and custom application definitions from a NetProfiler to ensure consistent traffic identification, select Manage Port Names and Customer 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.

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

To export flows to NetFlow Collectors

1. Go to Administration > System Settings: Flow Export in the web U.
2. Select Enable Flow Export. This enables flow export to NetFlow v9 flow collectors.
3. Select Include All Interface Groups or include individual interface groups from the list of configured MIfGs.
   – A BPF filter can be specified for the selected MIfG.
4. Enter the hostname or IP address of the NetFlow collectors to receive the flow exports.
5. Enter the UDP port to use for flow export.
6. Click **Apply** to begin flow export.

Checking Flow Export Status

The Status tab on the Flow Export 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 MIfGs. 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:

Managing Capture Jobs

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
- Clearing 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 New Capture Jobs

To create a new capture job:

1. Go to the Administration > System Settings: Capture Jobs page.
2. Choose the Add button to open the New Capture Jobs Definition page.
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 MIfG with the traffic to be captured (required).
5. Select a filter (optional). SteelFilter is the default filter type and the recommended filter type. No filter is used if the text box is empty. Any BPF filter can be used when indexing is not checked.

   If BPF and indexing are both selected, a message is displayed about issues that may occur. BPF filters using IP addresses, ports, or IP protocols work as expected. However, BPF filters that create a subset of a flow may result in an incorrect microflow index and an incorrect view in Packet Analyzer Plus. A workaround, if packets are available, is to force Packet Analyzer Plus to create the view from the packets, not 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. 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.
8. 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.

Option	Notes
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.

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.

Packet Export

To save captured packets as a trace file, do the following:

1. Go to the Administration > System Settings: Capture Jobs page.
2. Choose the Packet Export button to open the Packet Export page.
3. Select or specify an export time interval.
4. Select the file format and time stamp resolution desired.

5. Select the number of bytes in each packet to be exported.
6. Click Prepare Export URL to specify a destination other than your local system.
7. Click Download Packets Now. Packets are sent to a trace file on your local system.

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.

Packet Dissection

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

- **GRE** —Can be enabled (the default) or disabled using this check box. When GRE is enabled, the inner packet will be analyzed. If this option is disabled, packet analysis will happen on the outer packet instead.
- **VXLAN** —Can be enabled or disabled (the default) using this check box.
  If VXLAN is enabled, the inner packet will be analyzed. That means that VXLAN views will show no data since the inner packet likely does not use VXLAN. To get meaningful results from VXLAN views, leave this checkbox disabled so that the outer packet will be analyzed.
- **MAC in MAC** — If this option is enabled (the default), the 802.1ah frame will 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. When this option is disabled, packet dissection will stop at the 802.1ah header; the IP packet of the previous example will not be recognized as IP.
- **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 0 -255; values start from 1 (bottom of the stack) and increase; a value of 0 is a special value which means the top of the stack.
- **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 > System Settings: Packet Dissection.
2. Enable or disable GRE, VXLAN, or MAC in MAC by selecting or clearing the check box preceding each protocol at the top of the list of options.
3. If VXLAN is enabled, specify the UDP port used by VXLAN. The default UDP port is 4789.
4. Specify the MPLS level.
5. Specify the VLAN level.
6. Click **Apply** to make or **Revert** to reset the changes made.

Security

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: Security. 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

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: Security.
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: Security.
2. Under Settings, 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.

Enabling FIPS Mode

AppResponse 11 supports the use of certified Federal Information Processing Standard (FIPS) cryptography. This feature uses a FIPS-140-2 certified module for all cryptographic operations; this is a FIPS-certified version of the libcrypto library in openssl. FIPS affects any client that makes a secure connection to the appliance, including the web UI, Packet Analyzer Plus, Profiler, Portal, SSH, and raw REST calls over HTTPS. Precision Time Protocol (PTP) is not affected by this feature.

Setting FIPS to ON runs the system 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: 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.

To access the control for enabling and disabling FIPS, click Administration > Security, 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.

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 need to be disabled when FIPS mode is on. AppResponse 11 can be updated after disabling FIPS mode off.
- If traffic coming in to a probe is non-FIPS-compliant, the traffic will not be analyzed by the probe.
- When FIPS mode is on, logs written by individual processes in /var/log/messages.
- The message authentication codes that can be used for SSH in FIPS mode are:
  - hmac-sha1
  - hmac-sha2-256
  - hmac-sha2-512
- MySQL is not FIPS-compliant.
- 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 does not work if MD5 encryption is used.
- Wireshark dissection is not FIPS-compliant.

Viewing the SSL Certificate

To view the SSL certificate

1. Go to Administration > System Settings: Security.
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: Security.
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 76 for more information. The certificate details for each certificate show the Common Name record and other records encoded into the certificate.

Traffic Decryption

Adding Decryption Keys

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 > System Settings: SSL Decryption 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.

AppResponse 11 decrypts RSA key exchange based ciphers only. It does not decrypt Diffie-Hellman key exchange based ciphers.

To add a private key for SSL decryption

1. Go to Administration > System Settings: SSL Decryption to open the Decryption Keys page.
2. Choose Add to open the Add New SSL Decryption page.
3. Enter the name and description as you want it to appear on the 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-----
   MIIAsTCCARqgAwIBAgIJAOqvgxZRcO+ZMA0GCSqGSIb3DQEBBAUAMA8xDTALBgNVBAMTBE1henUwHhcNMDYxMDAyMTY0Mz
   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 Decryption Keys page.

For AppResponse 11 to use the private key to decrypt data, SSL Decoding must be enabled on the Administration > Web Transaction Analysis: Page Analysis page.

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.

SSL Ciphers Supported For Decryption

The following SSL ciphers are supported for decoding:

Cipher Suite (OpenSSL)	Name
SSL_RSA_WITH_NULL_MD5	NULL-MD5
SSL_RSA_WITH_NULL_SHA	NULL-SHA
SSL_RSA_WITH_RC4_128_MD5	RC4-MD5
SSL_RSA_WITH_RC4_128_SHA	RC4-SHA
SSL_RSA_WITH_IDEA_CBC_SHA	IDEA-CBC-SHA
SSL_RSA_WITH_DES_CBC_SHA	DES-CBC-SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA
TLS_RSA_WITH_NULL_MD5	NULL-MD5
TLS_RSA_WITH_NULL_SHA	NULL-SHA
TLS_RSA_WITH_RC4_128_MD5	RC4-MD5
TLS_RSA_WITH_RC4_128_SHA	RC4-SHA
TLS_RSA_WITH_IDEA_CBC_SHA	IDEA-CBC-SHA
TLS_RSA_WITH_DES_CBC_SHA	DES-CBC-SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA
TLS_RSA_WITH_AES_128_CBC_SHA	AES128-SHA
TLS_RSA_WITH_AES_256_CBC_SHA	AES256-SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	CAMELLIA128-SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	CAMELLIA256-SHA
TLS_RSA_WITH_SEED_CBC_SHA	SEED-SHA
TLS_RSA_WITH_NULL_SHA256	NULL-SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256	AES128-SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256	AES256-SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256	AES128-GCM-SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384	AES256-GCM-SHA384

SSL Ciphers Supported In FIPS Mode

The following SSL ciphers are supported for decoding in FIPS mode:

Cipher Suite (OpenSSL)	Name
TLS_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA
TLS_RSA_WITH_AES_128_CBC_SHA	AES128-SHA
TLS_RSA_WITH_AES_256_CBC_SHA	AES256-SHA
TLS_RSA_WITH_AES_128_CBC_SHA256	AES128-SHA256

Cipher Suite (OpenSSL)	Name
TLS_RSA_WITH_AES_256_CBC_SHA256	AES256-SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256	AES128-GCM-SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384	AES256-GCM-SHA384

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 61
- "Replacing the NetProfiler Export SSL Certificate" on page 62
- "Viewing the Trusted NetProfiler Certificates" on page 63
- "Adding a Trusted NetProfiler Certificate" on page 63

Viewing the NetProfiler Export Certificate

To view the SSL certificate

1. Go to Administration > System Settings: NetProfiler Integration.
2. Select the NetProfiler Export 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 > System Settings: NetProfiler Integration.
2. Select the NetProfiler Export 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: Host Settings web UI page. See "Hostname and DNS Servers" on page 76 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 > System Settings: 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 > System Settings: 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 > System Settings: 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.

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 (MIfG).
- 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 Analysis 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 > System Settings: Server Response Time Analysis, 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 > System Settings: Server Response Time Analysis, 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 > System Settings: Server Response Time Analysis, 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 > System Settings: Server Response Time Analysis, 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.

3

General Settings

Base 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 69
- "Configuring Management Interfaces" on page 70
- "Managing Routes" on page 70

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: Base Interfaces.
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 69 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 is installed. You can change the system date and time in the Administration > System Settings: Time 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 synced 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 virtual edition.

This section covers the following:

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 80.

Configuring PTP

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

1. On the General 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 Administration > System Settings: Time page:

- 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 General 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: Time page.
2. Select the NTP Servers tab.
3. Click **Add** in the toolbar at the top of the table.
4. 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.
5. 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: Time page.
2. Select the NTP Status tab.
3. 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 General 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.

Host Settings

Use the controls on this page 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: Host Settings.

1. Select 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: Host Settings.
2. Select the Static Name Resolution tab 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: Host Settings.
2. Select the Static Name Resolution tab.
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 Settings

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:SNMP to display the SNMP Settings page. 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.
- 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.

4

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

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"
- "Date Style"
- "Time Style"
- "Data Units"
- "Default Insight"
- "Search Settings"

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. Click **Apply** to save or **Revert** to reset the change(s) made.

Date Style

Change the date style used in the UI as follows:

1. Go to Administration > Other: User Preferences page.
2. Select a date style from the options displayed.
3. Click **Apply** to save or **Revert** to reset the change(s) made.

Time Style

Change the time style used in the UI as follows:

1. Go to Administration > Other: User Preferences page.
2. Select a time style from the options displayed.
3. 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.

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.

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 > OTHER: Email page.
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: Host Settings page 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 or SNMP trap when a policy violation causes an alert. Recipients must be defined on the Administration > System Settings: Recipients page before they are available for inclusion in policy definitions.

Defining Recipients

A recipient is a named list consisting of one or more Email addresses or SNMP receivers. A recipient can be a person, system, or group.

To specify a recipient

1. Go to the Administration > System Settings: Recipients page.
2. Choose Add to create a new recipient entry.
3. Enter the name of the recipient as you want it to appear wherever a user looks at a recipients list.
4. Select Email or SNMP or both to indicate the type of the recipient. Selecting a check box makes the fields below it accessible.
5. Specify the recipient's details: its Email address or SNMP receiver information, or both. Also for SNMP, specify the SNMP version to use, along with corresponding settings such as the community string for versions 1 and 2c, or the more robust security settings for version 3.
6. Choose Save.

Recipients and their details are listed on the Recipients page. You can click Test to send an Email message or SNMP trap 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.

5

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

TheAppResponse 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 mode*l, 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 171.

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 Area Status

- `show storage data_areas`—displays storage data areas status and details

- `show storage data_areas section <name>`—displays status and details of data areas on a data section
- `show storage data_area <name>`—displays storage data area <name> status and details
- `show storage data_area <name> section <name>`—displays status and details of the data area belonging to the named data module on a given data section if one exists

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>

Storage Data Area Section Enable/Disable

- storage data_area <name> section <name>—Enables data area <*data_module*> section <*data_section*>
- no storage data_area <name> section <name>—Disables data area <*data_module*> section <*data_section*>

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 > Other: System Dumps.
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 > Other: System Dumps.
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.

Update

Software updates to AppResponse 11 can be installed using the Update page in the web UI. 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.

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

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: Update to display the Update page.
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 gracefully shut down. Shutting down the appliance using the power switch may result in data loss.

Use this page 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

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: Reboot/Shutdown.
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: Reboot/Shutdown.
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 downing 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.

This page enables you save an appliance's configuration information and upload it to an external host for safekeeping, from which you can download it later to place the configuration on a new appliance. This capability is provided in the event that it is necessary to replace an appliance through Riverbed's RMA process; it is not intended for use as a means of cloning a configuration rapidly to deploy new equipment.

The backup process saves configuration information only; it does not save stored data. Most configuration information is backed up, although some is omitted for security reasons, or due to issues caused by not backing up data. All settings under Administration > Security are backed up, with the exception of the web certificate. Backups are not encrypted, so nothing that is a potential security risk is backed up. Upon reboot after a restore, the system will create a new self-signed web certificate. User accounts and passwords are backed up, stored in one-way hash format.

The backup is written to a .tgz (G-zipped TAR) file.

Sensitive configuration such as SSL certificates/keys will not be backed up, and will be reset to defaults upon a restore operation. This includes the default SSL certificate used when logging into the WebUI; your browser will complain about a self-signed certificate after a restore operation. Licenses will be left untouched, neither backed up nor deleted. Licenses are not transferrable between devices. User accounts, including one-way-hashed passwords, will be backed up and restored.

Note: A restore operation can be performed only on an appliance running the exact same software build as the appliance from which the backup was created.

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.

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

Note: The reset and restore process can take multiple minutes to finish, possibly hours (in situations in which the system being restored had a large amount of performance (ASA) data). The system does not provide a progress indicator, so, when you execute the Restore command, be prepared to allow the process a period of time to run to completion, and monitor it occasionally to see if it has finished.

In general, the backup and restore process will follow this sequence:

1. Execute a backup command on the Web UI.
2. Once the backup completes successfully, download the backup .tgz file.
3. Upload the backup .tgz file to another compatible system, running the exact same software build.
4. Execute a Restore command for that backup.
5. The appliance will reboot, and come up with the restored configuration. Licenses will remain untouched.

6

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.

Defining Host Groups

To define an additional host group

1. Go to the ADMINISTRATION > 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, or 3800 appliance or a VMon or v2000 virtual appliance can choose to export business groups (BGs) and import them into AppResponse 11.1.0 (and later) 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 Administration > 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 11host 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 ADMINISTRATION > 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 ADMINISTRATION > 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 ADMINISTRATION > 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.

Applications

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 100 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.
- "Advanced 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.

The Administration > Definitions: Applications page 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 100).

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. Go to Administration > Definitions: Applications 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 FILEA.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.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 Administration > Definitions. 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. Go to the Administration > Definitions: Applications page 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. 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.
5. Choose Add to open the new definition window.
6. 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.
7. Click Save to save the definition and return to the New General Application window. The new definition is listed.
8. 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.
9. Click Save to save the definition and return to the New General Application window. The new definition is listed.
10. 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. Go to the Administration > Definitions: Applications page 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.

Advanced Web

The Advanced 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 Advanced Web tab. An Advanced Web definition takes precedence over any definition in the library of auto-recognized applications. The product saves all statistics for application traffic that matches an Advanced Web definition.

To define an application on the Advanced Web tab

1. Go to the Administration > Definitions: Applications page Advanced 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

Property Name (case insensitive)	Type
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
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
  - 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 Advanced Web App page 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

Application 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 application definitions in a short amount of time.

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

Clicking Export displays a dialog with checkboxes for URL Applications and General Applications. Each is selected by default. Click Export to create a zip file that contains separate CSV files for URL applications and general 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

To export application definitions to CSV file:

1. Go to the ADMINISTRATION > DEFINITIONS: Application Configuration page.

2. Click Export at the upper right of the Application Configuration page. Clicking Export displays a dialog with checkboxes for URL Applications and General Applications. Each is selected by default. Click Export to create a zip file that contains separate CSV files for URL applications and general applications. By default, the file names are: “applications.zip”, “gen_apps_ar11.csv”, and “url_apps_ar11.csv”. The application definitions table is written to the specified CSV file immediately.

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 application definitions from CSV file:

1. Go to the ADMINISTRATION > DEFINITIONS: 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 > System 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 > System 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 > System 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. Go to Administration > Definitions: Port Aliases.
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. Go to Administration > Definitions: Port Aliases 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

A policy defines what is considered normal behavior for traffic on the network. It defines “normal” by specifying the limits beyond which the network behavior should cause an alert. A policy specifies network segments and metrics to monitor, when to monitor them, criteria to decide if a violation has occurred, what level of alert to generate if a violation occurs, and who to notify.

A policy can be made very specific by defining a series of qualifications for the traffic to which it applies. For example, you could limit the traffic that the policy monitors to only certain host groups. Then within those host groups, you could limit the monitoring to only certain applications. From there you could further limit it to only certain metrics.

Once a policy has been defined, you can edit it to place additional restrictions on the traffic it monitors, to change the violation criteria, to add notification recipients, and so on.

You can define up to 200 policies. The number of policies that have been defined is indicated in the upper right corner of the page.

To define a policy

1. Go to the Administration > Definitions: Policies page.
2. Choose Add to open the “Create new policy” wizard.
3. Complete the steps in the wizard. Each step is described below.

The wizard provides four worksheets for specifying the policy:

- “General” - The name and description of the policy and whether or not it is active.
- “Groups” - The traffic entities or attributes the policy monitors. Each entity you want the policy to apply to must exist before you create the policy. For example, entities such as Host Groups and Preferred Applications must be defined before you can specify them in a policy definition.
- “Trigger” - The level of policy violations that triggers an alert.
- “Notification” - 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 panel on the left side of the “Create new policy” wizard indicates which step you are working on. Refer to the descriptions below for assistance on completing the steps.

General

To complete the General specification step

1. Specify the policy name as you want it to appear throughout the product.
2. Optionally, enter a short description of the policy for the benefit of other users.
3. Ensure the Active check box is selected if the policy is to be placed in effect as soon as you finish defining it.
4. Choose Next to move to the Groups step.

Groups

To complete the Groups specification step

1. Choose Add to open the Select Group page.
2. Expand the hierarchical list of filtering options as necessary to specify the order in which each filter is applied to the monitored traffic.

   The tree has label nodes and selectable nodes. A label node can be expanded to list group types under that label. The OK button does not become active until you select a group type.
3. Choose OK to move to the next page, where you can specify the value of each type of grouping you included in the filtering path.
4. Each row that has an edit icon (pencil) must be edited to specify members of the group before you can move to the next step. Choose the pencil icon and enter the value for the group type.

   As you specify the criteria for each group type, the values you enter are displayed.

   You can edit your entries before leaving this step.

   – To change a value, choose the edit icon (pencil) to reopen the popup window and select or enter new values.

   – To delete an entry, choose the delete icon (x) for the entry, which becomes visible when you hover your mouse over the row. This deletes the entry and all entries beneath it.

   – To replace the entire filtering path, choose Replace near the top of the “Create new policy” window. This opens the tree diagram on which you can specify a new filtering path.
5. Choose Next to move to the Trigger specification step.

Trigger

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 complete the Trigger specification step

1. In the "Add a metric comparison" section, choose the 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 have specified 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, choose the "Add a metric comparison" icon 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, choose the "Add a condition" icon 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 the section below for an example of how this setting affects alerting.

6. Choose Next to move to the Notification step.

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

The Notification step specifies the recipient to notify when an alert occurs. Notifications are sent by Email or SNMP trap or both. You can define recipients using the Administration > System Settings: 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 complete the Notification specification step

1. Choose Add Recipient to open a list of recipients that have been specified on the Administration > System Settings: Recipients page.

2. Select the check boxes in the entries for the recipients that are to receive notifications.

3. 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.

4. Choose the alerting thresholds the recipient/address is monitoring.

5. 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.

6. Choose Finish to exit the wizard and add the policy 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.

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.

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 they are monitoring. They receive notifications about only the alert levels selected in the Notification step of the policy definition.

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 the choose Delete near the top of the page.

Importing policies from AppResponse 9

Policies can be imported to AppResponse 11 using a CSV file containing alert definitions exported from AppResponse 9. Do this by clicking Import at the top right of the Policies page and specifying the CSV file to import.

Note: Prior to importing alert 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.

PA Protocol Filters

Protocol 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

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 > Definitions: PA Protocol Filters.
2. With your mouse, hover over the application filter to be revised.
3. Click the pencil icon that appears at the end of the row.
4. The Edit Packet Analyzer Filters window 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.

5. In the Edit Filter window, 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.
6. Click **Apply** to make the changes or **Revert** to discard them.
7. In the Edit Packet Analyzer Filters window, Click **Save** to update the filter.

Adding a Definition to a Filter

1. Go to Administration > Definitions: PA Protocol Filters.
2. With your mouse, hover over the application filter to be revised.
3. In the Edit Packet Analyzer Filters window, 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 PA Protocol Filters they must be synchronized with Packet Analyzer Plus so application views correctly show your network traffic.For more information on synchronizing PA Protocol Filters see the *SteelCentral Packet Analyzer Plus User's Guide*.

7

Insights

An Insight provides a quick 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 *Snapshot* 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 Snapshots that you create.

This section covers the following:

Related topics:

- "The Navigator Workspace" on page 137

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 130.

4. Choose the Insight you wish to view.

5. If an Individual Insight is chosen, enter Inputs to identify the desired group or network element.

6. Click **OK** to open the Insight.

Supported Insights

The built-in insights that are provided in the current release are:

- Alert Events: View system and traffic alert events.
- Bandwidth Hogs: Isolate host groups, IPs and apps that are consuming most bandwidth.
- Individual: DB Client IP: Shows load, network anomalies and performance of a DB client IP.
- Individual: DB Server IP: Shows load, network anomalies and performance of a DB server IP.
- Individual: App: Shows performance, load and network anomalies of an individual application.
- Individual: Client Group: Shows load, network anomalies and performance of a client host group.
- Individual: Client IP: Shows load, network anomalies and performance of a Client IP.
- Individual: Host Group: Shows load, performance and network anomalies of an individual host group.
- Individual: IP: Shows load, network anomalies and performance of an IP.
- Individual: Server Group: Shows load, network anomalies and performance of an individual server group.
- Individual: Server IP: Shows load, network anomalies and performance of a Server IP.
- Individual: UC Host Group: Shows VoIP/Video load, performance and network anomalies of an individual host group.
- Individual: Web App: Shows performance, load and HTTP status codes of an individual web application.
- Individual: Web Server IP: Shows load, network anomalies and performance of a web server IP.
- Individual: Web User Group: Shows load, network anomalies and performance of a web user group.
- Individual: Web User IP: Shows load, network anomalies and performance of a web user IP.
- Slow Apps: Isolate slow applications and identify what network or server is experiencing poor performance
- Slow Web Apps: Isolate slow web applications and identify what network or server is experiencing poor performance
- Summary: All DB Traffic: Shows all database traffic being monitored.
- Summary: All Traffic: Shows all traffic being monitored.
- Summary: All UC Traffic: Shows all UC traffic being monitored.

- Summary: Apps: Shows performance, load and network anomalies of top applications.
- Summary: Client Groups: Shows load, network anomalies and performance of top client groups.
- Summary: DB Queries: Summary of Individual DB Queries.
- Summary: DB Sessions: Summary of Individual DB Sessions.
- Summary: Host Groups: Shows load, network anomalies and performance of top host groups.
- Summary: Page Views: Summary of individual page views.
- Summary: Server Groups: Shows load, network anomalies and performance of top server groups.
- Summary: TCP Connections: Summary of TCP connections.
- Summary: VoIP/Video Calls: Summary of indiviudal calls.
- Summary: Web Apps: Shows performance and load of top web applications.
- Summary: Web User Groups: Shows load, network anomalies and performance of top web user groups.
- Traffic Diagnostics: Shows load on monitoring interfaces, connections and web requests being processed, as well as flows exported to NetProfiler.
- WebUI System Health Report: View system health information.

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 Snapshot.
  - 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.

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 Snapshot.
  - 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 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 time interval is used to calculate the data and metrics in the tables and charts in the Insight.
- **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.
- 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

Insights with owners can be edited by roles with read/write access. Predefined 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.

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.

Schedules

Most insights can be scheduled to run at specific times, or at specific intervals, to generate snapshots. 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 snapshots that are generated as a result.

Click Insights > Actions:Schedules to display the Schedules page for defining and managing snapshot 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 snapshot 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 snapshot will encompass (Time Frame). The next time the schedule will execute is shown, along with the particular span of time that will be snapshot 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.

9. Specify one or more Email recipients for the snapshot. 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 snapshot's PDF file.

10. Specify whether the resulting snapshot 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 snapshots are available on the Snapshots page. Each scheduled snapshot can be clicked on to be explored, and is available as a PDF for convenient distribution.

Viewing Snapshots

When viewing a Snapshot:

- the time interval of the snapshot 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 snapshot cannot be saved; however, the most recent instance of a scheduled snapshot is available as a PDF document that can be downloaded and shared.
- the list of snapshots can be sorted by snapshot 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"

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.

Alert Events Table

Based on the inputs provided, AppResponse 11displays 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.
- 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, the 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.
- Snapshot—A Snapshot 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
   - Snapshot
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.

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.

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.
- Snapshot—A Snapshot 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
   - Snapshot
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.

8

Navigator

Navigating Groups

Use 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.

- 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 Snapshots.
- Right-click menus provide additional options for the top table and workspace data.

In addition, you can create custom groups known as Favorites. You select the groups in a Favorite from all available AppResponse11 groups, table rows, and chart elements. Favorites can assist you:

- in troubleshooting.
- in quickly building and sharing custom Insights or Snapshots.

Important: 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.

This section contains information on the following:

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: 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 139 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 139 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 Snapshot by clicking the Save button in the workspace toolbar. See "Save Insight" under "The Navigator Workspace" on page 137 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 141.
- **Column Selector**—Click the columns icon in the top right corner of the top table.
  - The Column Chooser window opens displaying the available columns and the selected columns. In Browse mode available columns (metrics) are grouped by metric type. In Filter mode you search for a column by a word or phrase and also specify the type of calculation used for the metric (average or sum).
  - To move a selected column, hover over the column name and click the grab icon, then drag it to its new position.
- **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 Snapshot. 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 Insight to display in the workspace.
- **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.
  - Snapshot—A Snapshot 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, and sparkline 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

In AppResponse 11.1 (or later) 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.

Favorites

Favorites are user-selected groups that can be built from all available AppResponse 11data groupings. A data grouping may be added to a Favorite from a top table row selection or a chart element. Favorites can be used in troubleshooting workflows and building Insights.

A Favorite can be saved and revised. A group and all of its subgroups are saved, along with any open charts. The new Favorite appears Under Favorites in the Navigator navigation pane.

Creating a Favorite

There are two ways to create a Favorite:

- Select a group in the top table and click the star icon in the upper right corner of the top table toolbar. 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 select "Add to Favorites." 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.

Adding or Deleting Groups in a Favorite

The simplest 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 Favorites.
3. On the Add to Favorites screen that opens, select Current Favorites.
4. Choose the Favorite for the data.
5. Select the data to add and click OK.

Deleting a Favorite

1. Select the Favorite in the navigation pane to display it in the top table.
2. Click the trash icon on the far right end of the top table toolbar.

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 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**—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 "Packet Export" 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.
- **Show TCP Connections**—The TCP Connections group opens, filtered by the right-clicked group. The filter is shown in the table toolbar.
- **This Application**—Opens an Insight based on the type of chart element selected.

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 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.
- **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

9

Web Transaction Analysis

Page Analysis Configuration

You enable and set up Web Transaction Analysis Module (WTA) on the Administration > Web Transaction Analysis: Page Analysis Configuration web UI page.

Data Collection Options

Option	Notes
Enable Page Analysis	When enabled, the appliance collects web page analysis data for the specified ports and IP addresses. 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 156. **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 *before you enable Page Analysis*.
Ports	Collect data for the specified ports only.
Server IP Addresses	Collect data for a subset of IP addresses or select check box for all IP addresses. **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.
Default Slow Page Threshold	The appliance uses this threshold, in seconds, to determine metrics such as Slow Pages and Slow Page Rate. Range: 1 - 600; default is 5 seconds.
Enable SSL Decoding	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: "Traffic Decryption,"
"Enable SOAP Processing"	
"Advanced Options"	

Option	Notes
Unique User Definition	Configure the parameters used to identify a unique user.
GeoMap Private Data	Import an AppResponse 9.6.x .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.asmx [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. The CSV file can also be exported or deleted.

Note: An AppResponse version 9.6.x IP-to-Region Custom Mapping CSV File is not compatible with AppResponse 11.1.0 .

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 > Web Transaction 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 11.1.0 (or later).

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 152

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	Apply the rule only to objects that match a URL pattern in the list. For example:
	`www.riverbed.com/*` matches both
	▪ `http://www.riverbed.com/*` and
	▪ `https://www.riverbed.com/*`
	Include the protocol prefix (`http://`, `https://`, or `http*://`) only if you specifically want to match only http or only https. For example:
	`http://*popup-ad-click.com/*`
	`https://*redir.adap.tv/redir*`
	`http*://*redir.adap.tv/redir*`

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"l pages into families. You can group pages by "Truncated URL" and/or .
Stop processing object after this rule is applied	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 1. It applies a rule with this option selected, or 2. All enabled rules are applied. 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.

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 *on the page objects themselves* and not simply on objects that might be included in these pages.
Allow pages that start with an unobserved redirect Allow pages that start with zero-length content Allow pages that start with an unrecognized content type	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. One possible workflow you might be use is to ▪ 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).
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	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: ▪ 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 152

Custom Page Family Rule Settings

You can specify the rules AppResponse 11uses 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 “Advanced Web” in the Administration > Definitions: Applications Help.

Setting	Notes

URL Patterns	Apply the rule only to pages that match a URL pattern in the list. Each entry should include the protocol prefix (`http://`, `https://`, or `http*://`). Examples include:
	`https://*mycompany.com/*calendar*`
	`http://www.example.com/*.aspx`

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	Group page views into families based on Truncated URLs. 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. 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. 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 trxtype. **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: ▪ 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. For more information, see "Content Values" on page 149.
Minimum Length	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. 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 *WILL NOT* 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 *STILL* longer than 150 characters, then the Content Values portion will get shortened to make it all fit into 150 characters.
Truncate at character___	Truncate all characters at or after a custom character. If the appliance is configured to truncate at the semicolon(;), the result is `http://www.example.com/a;bcd...` (URL stem) `http://www.example.com/a...` (page family name)

Setting	Notes
Truncate at ___ slashes	Truncate all characters after the first instance of the ***n***th slash (includes `http://`). The ***n***th slash is not truncated. For example, if the appliance is configured to truncate at the fourth slash, the result is: `http://www.example.com/a/b/c/d/e...` (URL stem) `http://www.example.com/a/...` (page family name)

Advanced Options	Use Advanced Options to match and replace strings within the page family name.
	▪ Uses this format: `"match" => "replace"`
	▪ Multiple match/replacements can be entered by putting them on separate lines.
	You also can use regular expressions, with \N denoting a back-reference. For example, the following entry in the Advanced Options section:
	– 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:
	`"riverbed" => "rvbd"`
	`"company" => "co"`
	`"http://([^/]*)/([^/]*)/([^/]*)/(.*)" => "http://\1/\3/\2/\4"`

Content Values	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. 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 `trx_type`. Each entry has the following attributes: ▪ 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. **Important—**The more content values you include in this table, the more page families you will get. For more information, see “Truncated URL” on page 153.
Prepended Display Label	A prefix string to insert before the content values in the Page Family name. 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.
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

Setting	Notes
Key	The `[key]` string in the `[key]=[value]` pairs that contain the private information to exclude. For information about how to find the key string, see "Information Privacy Definition Settings" on page 156.
Description	
Status	If the definition is not enabled, private information for the specified key will not be hidden.
IP Addresses Ports URLs	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. For information about how to find this information, see "Information Privacy Definition Settings" on page 156.

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.

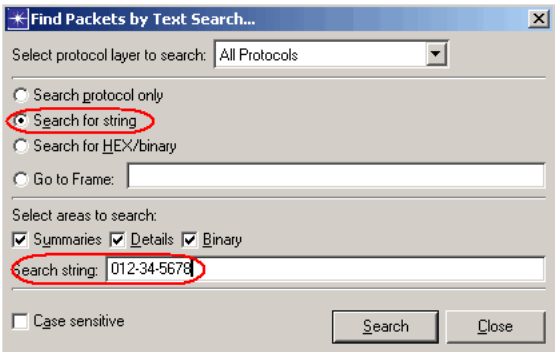
3. Go to Administration > Web Transaction Analysis: Information Privacy.
4. Click Add to create a new Information Privacy definition.
5. Specify the Key, IP Address(es), Port(s), and URL(s) in which the private information will be found.

   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)



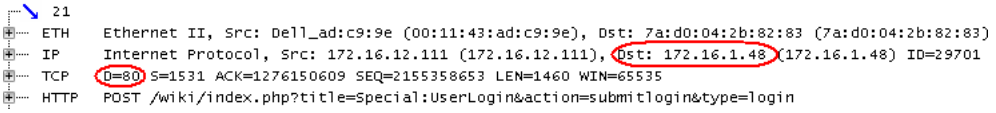
   For each packet that contains the `[value]` string, parse the HTTP contents of that packet to locate the corresponding `[key]` string. This best places to look are in the `POST` data (most likely) or the URL parameter of a `GET` request (less likely, but possible).

   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:

- "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 160. 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.

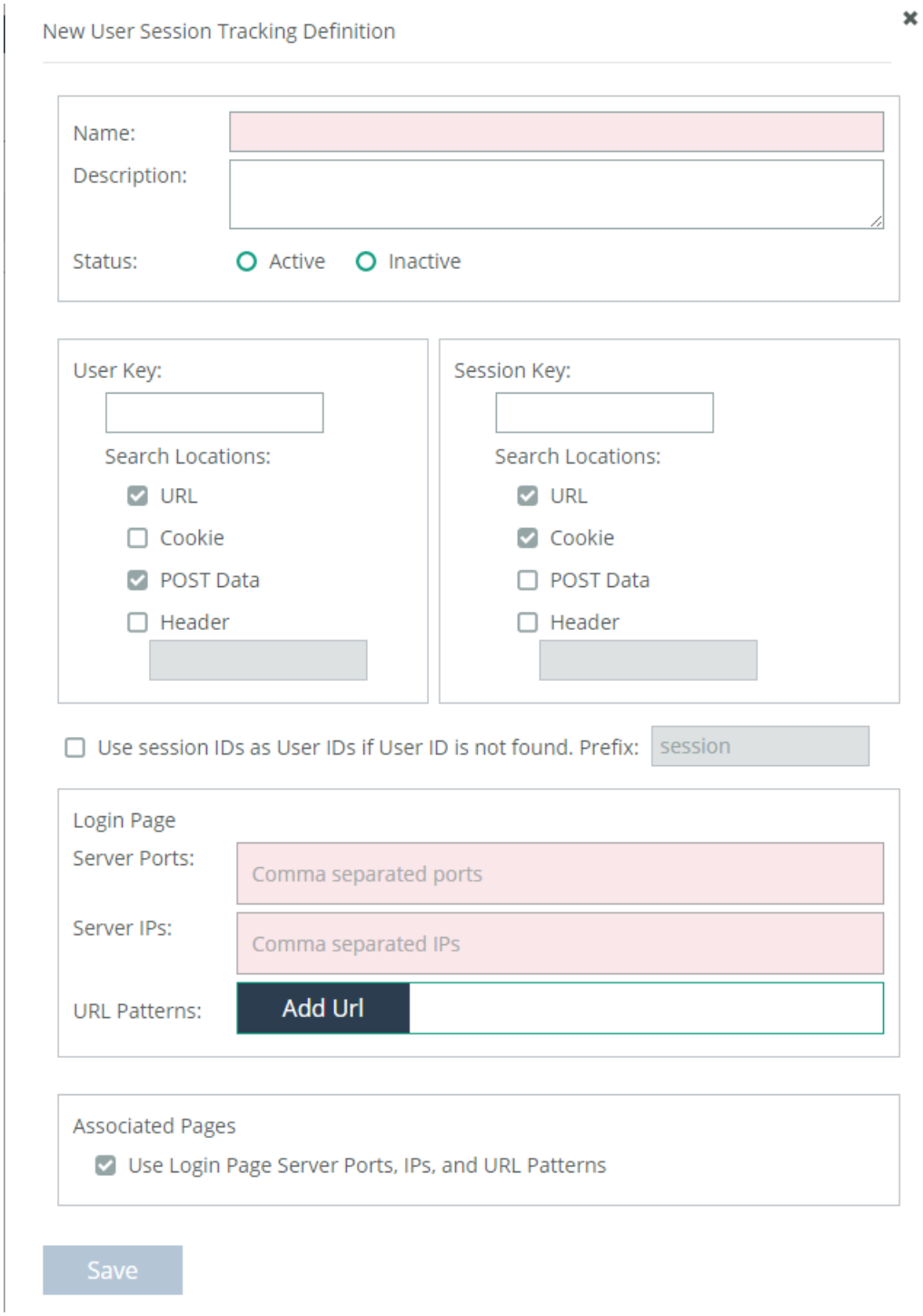
  When you specify the host and path, your goal is to enter a regular expression that matches all page views of interest for the web application of interest (and no other web applications that you are tracking in AppResponse 11). The following are some example URL patterns:

  - `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 /shopcart/")

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"**



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:	This option is useful to track users when the appliance did not observe the initial login sequence for a session. This can occur because ▪ A web application uses an authentication server whose traffic is not monitored by the appliance. ▪ The login occurred before WTA was enabled. When this option is enabled, WTA creates User names with the label [*prefix*]+[*session_tag*]. 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: 'FinTrx$Session').

Setting	Notes
Login Page	The login pages where users enter usernames. ▪ 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: ▪ 1+ strings/patterns for the hostname/domain (examples: **`www.acme.com`** and **`*.google.com`**). Do not include a port number in this field, even if the web application normally includes one in its URL—for example, enter only `www.mywebapp.com` and not `www.mywebapp.com:8010`. ▪ 1+ strings patterns for the login page (examples: **`*/identification.aspx`** and **`*AUTH_Login*`**)
Associated Pages	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. ▪ 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: ▪ 1+ strings/patterns for the hostname/domain (examples: **`www.acme.com`** and **`*.google.com`**). Do not include a port number in this field, even if the web application includes one in its URL—for example, enter `www.mywebapp.com` and not `www.mywebapp.com:8010`. ▪ 1+ strings patterns for the login page (examples: **`*/identification.aspx`** and **`*AUTH_Login*`**)

10

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, and 2012
- MySQL 5.0 through 5.5
- Oracle 8.1.7 through 11gR2
- 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

DB Analysis in 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 167 for an overview and a list of topics.

Disabling database analysis

1. Go to Administration > Database Analysis: DB Analysis.
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 > Database Analysis: DB Analysis.
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 > Analyses: Module Traffic Filters and 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 > Analyses > Database Analysis.

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 123.

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 135.

A

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 only done 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
```

B

AppResponse 11 Metric Descriptions

Group Metrics

The Group Metrics include all of the "Total Traffic Metrics" plus the following metrics.

Metric	Notes
Inbound Packet Traffic [#]	Total number of packets received by all hosts in group.
Inbound Throughput [bps]	Average rate of bytes received by all hosts in group in bytes per second.
Inbound Traffic [bytes]	Total amount of data received by all hosts in group in bytes.
Inbound Utilization [%]	Average percentage of inbound link utilization.
Outbound Packet Throughput [#/sec]	Average rate of packets sent by all hosts in group in packets per second.
Outbound Packet Traffic [#]	Total number of packets sent by all hosts in group.
Outbound Throughput [bps]	Average rate of bytes sent by all hosts in group in bytes per second.
Outbound Traffic [bytes]	Total amount of data sent by all hosts in group in bytes.
Outbound Utilization [%]	Average percentage of outbound link utilization.

Host Group Metrics

In addition to the "WTA Metrics" above the following metrics are available for Host Groups.

Metric	Notes
Inbound Utilization [%]	Average percentage of inbound link utilization.
Outbound Utilization [%]	Average percentage of outbound link utilization.

Total Traffic Metrics

Metric	Notes
Active Connections [#]	Total number of active TCP connections.
Client Reset Rate (*#/min*)	Average number of TCP Connections that terminated with a TCP client reset per minute.
Client Resets [#]	Total number of TCP Connections that terminated with a TCP client reset.
Connection Request Rate [#/min]	Average number of TCP Connection Requests per minute.
Connection Requests [#]	Total number of TCP Connection Requests.
Connection Setup Time [sec]	AverageTCP Connection Setup Time in seconds.
Connections Failed [#]	Total number of TCP Connections that failed.
Connections Failed Rate [#/min]	Average rate of TCP Connection failures per minute.
Connections Opened [#]	Total number of TCP Connections opened.
Connections Opened Rate [#/min]	Average rate of TCP Connections opened per minute.
Request Data Transfer Time [sec]	Average TCP Request Data Transfer Time in seconds.
Request Payload [bytes]	Average TCP Client Request Payload size in bytes.
Request Payload Transfer Time [sec]	Average TCP Request Payload Transfer Time in seconds.
Request Pkt Payload [#]	Average number of packets in TCP Request Payload
Request Retrans [%]	Percentage of Request packets retransmitted.
Request Retrans Delay [sec]	AverageTCP Request Retransmit Delay in seconds.
Request Retrans Pkt Rate [pkts/sec]	Average rate of TCP Request Retransmission in packets per second.
Request Retrans Rate [bps]	Average rate of TCP Request Retransmission in bytes per second.
Response Data Transfer Time [sec]	Average TCP Response Data Transfer Time time in seconds.
Response Payload [bytes]	Average Response Payload in bytes.
Response Payload Transfer Time [sec]	Average Response Payload Transfer Time in seconds.
Response Pkt Payload [#]	Average number of packets in TCP Response Payload
Response Retrans [%]	Percentage of Response packets retransmitted.
Response Retrans Delay [sec]	AverageTCP Response Retransmit Delay in seconds.
Response Retrans Pkt Rate [pkts/sec]	Average rate of TCP Response Retransmission in packets per second.
Response Retrans Rate [bps]	Average rate of TCP Response Retransmission in bytes per second.
Retrans Rate [bps]	Average rate of total TCP Request and Response Retransmissions in bytes per second.
Round Trip Time [sec]	Average TCP Round Trip Time in seconds.
Server Reset Rate [#/min]	Average rate of TCP server resets per minute.
Server Resets [#]	Total number of TCP server resets.

Metric	Notes
Server Response Time [sec]	Average TCP Server Response Time in seconds.
Server Responses [#]	Total number of TCP Server Responses
Server Responses Rate [#/min]	Average rate of TCP Server Responses per minute.
Total Data Transfer Time [sec]	Average Total Data Transfer Time in seconds.
Total Packet Throughput [#/sec]	Average Total Packet Throughput in packets per second.
Total Packet Traffic [#]	Total number of Packet Tragic packets.
Total Payload Transfer Time [sec]	Average Payload Transfer Time in seconds.
Total Reset Rate [#/min]	Average Total Reset Rate per minute.
Total Resets [#]	Total number of TCP Resets.
Total Retrans [%]	Percentage of Request and Response packets retransmitted.
Total Retrans Delay [sec]	Average Total Retransmission Delays in seconds.
Total Throughput [bps]	Average Total Traffic Throughput Time in seconds
Total Traffic [bytes]	Total size of Traffic in bytes.
User Response Time [sec]	Average TCP User Response Time in seconds.

WTA Metrics

Metric	Description
% HTTP *status-code*	Percentage of HTTP responses with a specific status code or range
% Slow Pages	Percentage of Individual Page Views with page times that exceed a slow threshold
Client Busy Time	Average Client Busy Time in seconds.
Client Busy Time (Normalized)	Average Client Busy Time (Normalized) in seconds.
Custom metric 1	See “Custom WTA Metrics/Columns” on page 155 for more information.
Custom metric 2	See “Custom WTA Metrics/Columns” on page 155 for more information.
Custom metric 3	See “Custom WTA Metrics/Columns” on page 155 for more information.
Custom metric 4	See “Custom WTA Metrics/Columns” on page 155 for more information.
Custom metric 5	See “Custom WTA Metrics/Columns” on page 155 for more information.
HTTP XXXs	Number of HTTP responses the specified status code or code or range
Objects Requested	Number of HTTP server responses to HTTP client requests
Network Busy Time	Average network transfer time in seconds for the full payload of an individual request or response, from the first observed packet to the last. This metric appears in the “Individual Page Views Waterfall (Resource Timeline)” Graph only.

Metric	Description
Network Busy Time (Normalized	Average network transfer time in seconds for all resources in a page. Because the server might have processed multiple requests in parallel, the total-page-view busy time might be less than the sum of the busy times for all resources in the view. This metric appears in the “Individual Page Views Waterfall (Resource Timeline)” Graph only.
Page Request Size	Average size of HTTP request messages sent
Page Request Throughput	Average bytes-per-second of HTTP request messages
Page Request Traffic	Total size all of HTTP request messages sent
Page Response Size	Average size of HTTP response messages sent
Page Response Throughput	Average bytes-per-second of HTTP response messages sent
Page Response Traffic	Total size of all HTTP response messages sent
Page Time	Average page time per page
Page Total Size	Average total page size
Page Total Throughput	Average bytes-per-second of total request and response messages
Page Total Traffic	Total of page request and response traffic
Page View Rate	Average number of page views per second
Page Views	Total Number of Page Views
Server Busy Time	Average time in seconds that the HTTP server spent processing an individual resource request. This time is measured from the resource request (last observed packet of HTTP request) to the initial response (first observed packet). This metric appears in the “Individual Page Views Waterfall (Resource Timeline)” Graph only.
Server Busy Time (Normalized)	Average total time in seconds that the HTTP server spent processing all resource requests in a page. Because the server might have processed multiple requests in parallel, the total-page-view busy time might be less than the sum of the busy times for all resources in the view. This metric appears in the “Individual Page Views Waterfall (Resource Timeline)” Graph only.
Slow Pages	Number of Individual Page Views with page times that exceed a slow threshold
Slow Page Rate	Average rate per second of page views with page times that exceed a slow threshold

C

AppResponse 11 Supported CODECS

Supported CODECS

AppResponse 11 supports the following CODECS for unified communications analysis in the current version:

Audio

- MPEGL1
- MPEGL2
- MPEGL3
- 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