RTView® Monitor for Solace® User's Guide

Version 3.4*

*This document is equivalent to Solution Package for Solace Version 3.4

RTView® Monitor for Solace®

© 2013-2016 Sherrill-Lubinski Corporation. All Rights Reserved.

RTView®

Copyright © 1998-2016. All rights reserved.

No part of this manual may be reproduced, in any form or by any means, without written permission from Sherrill-Lubinski Corporation. All trademarks and registered trademarks mentioned in this document are property of their respective companies.

LIMITATIONS ON USE
Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in the Technical Data - Commercial Items clause at DFARS 252.227-7015, the Rights in Data - General clause at FAR 52.227-14, and any other applicable provisions of the DFARS, FAR, or the NASA FAR supplement.

SL, SL-GMS, GMS, RTView, SL Corporation, and the SL logo are trademarks or registered trademarks of Sherrill-Lubinski Corporation in the United States and other countries. Copyright © 1998-2016 Sherrill-Lubinski Corporation. All Rights Reserved.

JMS, JMX and Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. They are mentioned in this document for identification purposes only.

No part of this manual may be reproduced, in any form or by any means, without written permission from Sherrill-Lubinski Corporation.

All trademarks and registered trademarks mentioned in this document are property of their respective companies.

SL Corporation
240 Tamal Vista Blvd.
Corte Madera, CA 94925 USA

Phone: 415.927.8400
Fax: 415.927.8401
Web: http://www.sl.com

Preface 1
About This Guide 1
Document Conventions 1
Additional Resources 1
Release Notes 2
Documentation and Support Knowledge Base 2
Contacting SL 2
Internet 2
Technical Support 2

Chapter 1 - Introduction to the Monitor 3
Overview 3
Monitor Standalone and Solution Package 3
Get Started 4
System Requirements 4

Chapter 2 - Quick Start - Standalone 5
Install & Setup 5
Connect Your Message Routers 6
Start the Monitor 7
Stop the Monitor 8
Troubleshooting 8
Log Files 9
JAVA_HOME 9
Permissions 9
Network/DNS 9
Verify Data Received from Data Server 9
Verify Port Assignments 9

Chapter 3 - Quick Start - Solution Package 11
Install & Setup 11
Connect Your Message Routers 12
Start the Monitor 13
Stop the Monitor 14
Troubleshooting 15
Log Files 15
JAVA_HOME 15
Permissions 15
Network/DNS 15
Verify Data Received from Data Server 15
Verify Port Assignments 16

Chapter 4 - Standalone Production Configuration 17
Configure the Database 17
Database Connections 17
Third Party Application 20
Configure Alert Notification 20
Substitutions for Batch Files or Shell Scripts 22
Notification Persistence 23
Configure HA 23
Setup Data Persistence 24

Chapter 5 - Using the Monitor 25
Overview 26
Monitor Main Display 26
Heatmaps 27
Tables 28
Trend Graphs 28
Title Bar 30
Context Menu 30
Multiple Windows 31
Export Report 31
Message Routers 33
All Message Routers Heatmap 33
All Message Routers Table 36
Message Router Summary 43
Environmental Sensors 47
Message Router Provisioning 48
Interface Summary 51
Message Spool Table 54
Message Router VPN Activity 56
CSPF Neighbors Table 58
VPNs 59
All VPNs Heatmap 59
All VPNs Table 63
Top VPNs Grid 67
Single VPN Summary 69
Clients 73
All Clients 74
Single Client Summary 79
Bridges 83
All Bridges 84
Single Bridge Summary 88
Endpoints 91
All Endpoints 92
Single Endpoint Summary 94
Single Endpoint Summary Rates 97

Capacity Analysis 100
All Message Router Capacity 101
Message Router Capacity 104
Message Router Capacity Trends 108
Syslog 111
All Syslog Events Table 111
Alert Views 114
Alert Detail Table 114
Administration 118
Alert Administration 119
Tabular Alert Administration 122
Setting Override Alerts 123
Alert Administration Audit 124
RTView Cache Tables 126
RTView Agent Admin 127
RTView Servers 129
Data Server Metrics 129
Display Server Metrics 133
Historian Servers 134
Tomcat Server Summary 136
Tomcat Modules Summary 139
JVM CPU/Mem Summary 142
JVM Mem Pool Trends 146
JVM Mem GC Trends 149
JVM System Properties 151
Version Info 152
About 154

Appendix A - Alert Definitions 155

Appendix B - Limitations 161
iPad Safari Limitations 161

Preface

Welcome to the *RTView® Monitor for Solace® User's Guide*.

Read this preface for an overview of the information provided in this guide and the documentation conventions used throughout, additional reading, and contact information. This preface includes the following sections:

- "About This Guide" on page 1
- "Additional Resources" on page 1
- "Contacting SL" on page 2

About This Guide

The *RTView® Monitor for Solace® User's Guide* describes how to install, configure and use the Monitor.

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, directory paths, file names, commands and GUI controls 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 <ipaddress>**

Additional Resources

This section describes resources that supplement the information in this guide. It includes the following information:

- "Release Notes" on page 2
- "Documentation and Support Knowledge Base" on page 2

Release Notes

The following online file supplements the information in this user guide. It is available on the SL Technical Support site at http://www.sl.com/support/.

Documentation and Support Knowledge Base

For a complete list and the most current version of SL documentation, visit the SL Support website located at http://www.sl.com/support/documentation/. The SL Knowledge Base is a database of known issues, how-to documents, system requirements, and common error messages. You can browse titles or search for keywords and strings. To access the SL Knowledge Base, log in to the SL Support site located at http://www.sl.com/support/.

Contacting SL

This section describes how to contact departments within SL.

Internet

You can learn about SL products at http://www.sl.com.

Technical Support

If you have problems installing, using, or replacing SL products, contact SL Support or your channel partner who provides support. To contact SL Support, open a trouble ticket by calling 415 927 8400 in the United States and Canada or +1 415 927 8400 outside the United States.

You can also go to http://www.sl.com/support/.

CHAPTER 1 Introduction to the Monitor

This section contains the following:

- "Overview" on page 3
- "System Requirements" on page 4

Overview

The RTView® Monitor for Solace® is an easy to configure and use monitoring system that gives you extensive visibility into the health and performance of your Solace message routers and the applications that rely on them.

The RTView® Monitor for Solace® enables Solace users to continually assess and analyze the health and performance of their infrastructure, gain early warning of issues with historical context, and effectively plan for capacity of their messaging system. It does so by aggregating and analyzing key performance metrics across all routers, bridges, endpoints and clients, and presents the results, in real time, through meaningful dashboards as data is collected.

Users also benefit from predefined dashboards and alerts that pin-point critical areas to monitor in most environments, and allow for customization of thresholds to let users fine-tune when alert events should be activated.

The RTView® Monitor for Solace® also contains alert management features so that the life cycle of an alert event can be managed to proper resolution. All of these features allow you to know exactly what is going on at any given point, analyze the historical trends of the key metrics, and respond to issues before they can degrade service levels in high-volume, high-transaction environments.

Monitor Standalone and Solution Package

The RTView® Monitor for Solace® can be installed as a standalone monitoring system for technical support teams to monitor the health and performance of their infrastructure. It can also be installed as a Solution Package within the RTView Enterprise Monitor® product. RTView Enterprise Monitor is an end-to-end monitoring platform that allows application support teams to understand how infrastructure, middleware, and application performance data affect the availability and health of the entire application. Used as a Solution Package for Solace within RTView Enterprise Monitor, the Solace metrics and health state are but one source of information that determines the entire health state of the application.

Get Started

Proceed to:

- "Quick Start - Standalone" on page 5 to run the standalone RTView® Monitor for Solace®.
- "Quick Start - Solution Package" on page 11 to run the Solution Package for Solace. RTView Enterprise Monitor® must be installed on your system.

For more information about RTView Enterprise Monitor®, see the *RTView Enterprise Monitor® User's Guide*, available at http://www.sl.com/support/documentation/.

System Requirements

Please refer to the **README_sysreq.txt** from your product installation. A copy of this file is also available on the product download page.

CHAPTER 2 Quick Start - Standalone

This section describes how to install, configure and start the standalone Monitor using default settings (for evaluation purposes).

Linux users:

- These instructions require a Bourne-compatible shell.
- JAVA_HOME is required for Tomcat.

  NOTE: LINUX users might see inconsistently aligned labels in displays. To resolve, set the client browser to download the fonts used by the server. Open the **rtvapm/common/conf/rtvapm.properties** file on the Display Server host machine and uncomment the following two lines:

  #sl.rtview.cp=%RTV_HOME%/lib/rtvfonts.jar

  #sl.rtview.global=rtv_fonts.rtv

For complete RTView® system requirements, see **README_sysreq.txt**.

This section includes:

- "Install & Setup," next
- "Connect Your Message Routers" on page 6
- "Start the Monitor" on page 7
- "Stop the Monitor" on page 8
- "Troubleshooting" on page 8

Install & Setup

1. Download the **RTViewSolaceMonitor_<VERSION>.zip** archive to your local Windows/UNIX/Linux server.

2. Extract the files:

   Windows:
   Type **unzip RTViewSolaceMonitor_<VERSION>.zip** and save the files to the **C:\RTView** directory.

   UNIX/Linux:
   Type **unzip -a RTViewSolaceMonitor_<VERSION>.zip** and save the files to the **/opt/RTView** directory.

   Important: In Linux use **unzip -a RTViewSolaceMonitor_<VERSION>.zip**.

   The **RTViewSolaceMonitor** directory is created under the destination directory.

3. Set JAVA_HOME to the location of your Java installation and include it in the path.

Important: This environment variable must also be defined in UNIX/Linux systems for Tomcat to start successfully.

4. If you prefer not to use the pre-configured Apache Tomcat 8 application server, you must obtain another application server. This change implies additional configuration steps.

Proceed to "Connect Your Message Routers," next.

Connect Your Message Routers

Connect your own message routers and enable for data collection.

1. Open the **sample.properties** file, located in the **RTViewSolaceMonitor/em-solmon/servers/solmon** directory.

2. Copy/paste the following lines for each Solace message router you want to monitor (to enable the Monitor to collect data from them):

```
collector.sl.rtview.http.conn=__name=UNIQUE_APPLIANCE_NAME url=http://<IP or hostname>:<port>/SEMP username=<user> password=<pass>

collector.sl.rtview.cache.config=sol_cache_source.rtv  $solConn:UNIQUE_APPLIANCE_NAME
```

where

- **<UNIQUE_APPLIANCE_NAME>** is a unique string to identify the connection of each monitored message router
- **<IP or host-name>** is either an IP address or the host name that can be resolved by your network name resolution method
- **<port>** is the SEMP port number configured for your message router.
- **<user>** and **<pass>** are the user credentials to log into the message router.

Example for two routers:
(where **xxx.xxx.xxx.xxx** = IP address)

```
collector.sl.rtview.http.conn=__name=example1 url=http://xxx.xxx.xxx.xxx:8050/SEMP username=rtviewadmin password=rtview

collector.sl.rtview.cache.config=sol_cache_source.rtv  $solConn:example1

collector.sl.rtview.http.conn=__name=example2 url=http://xxx.xxx.xxx.xxx:8080/SEMP username=rtviewadmin password=rtview

collector.sl.rtview.cache.config=sol_cache_source.rtv  $solConn:example2
```

3. If you do *not* have Syslog configured to capture event messages from your Solace message routers, skip this step. If you *do* have Syslog configured, uncomment and modify the following connection parameters as needed in your **sample.properties** file, located in the **RTViewSolaceMonitor/em-solmon/servers/solmon** directory:

```
#
# Configure connections to Syslog
#
```

#For messages sent via TCP, use
#collector.sl.rtview.syslogds.conn=__name=syslogTCP protocol=TCP host=localhost port=601
#collector.sl.rtview.cache.config=sol_syslog_cache_source.rtv $conn:syslogTCP

#For messages sent via UDP, use
#collector.sl.rtview.syslogds.conn=__name=syslogUDP protocol=UDP host=localhost port=514
#collector.sl.rtview.cache.config=sol_syslog_cache_source.rtv $conn:syslogUDP

NOTE: host refers to the network interface that will be used to receive Syslog messages (there might be more than one network interface available on the receiving system). Typically, this will be the IP address assigned to the selected network interface. If the system where the Monitor Data Server is running is also the Syslog receiver, then **localhost** can be used.

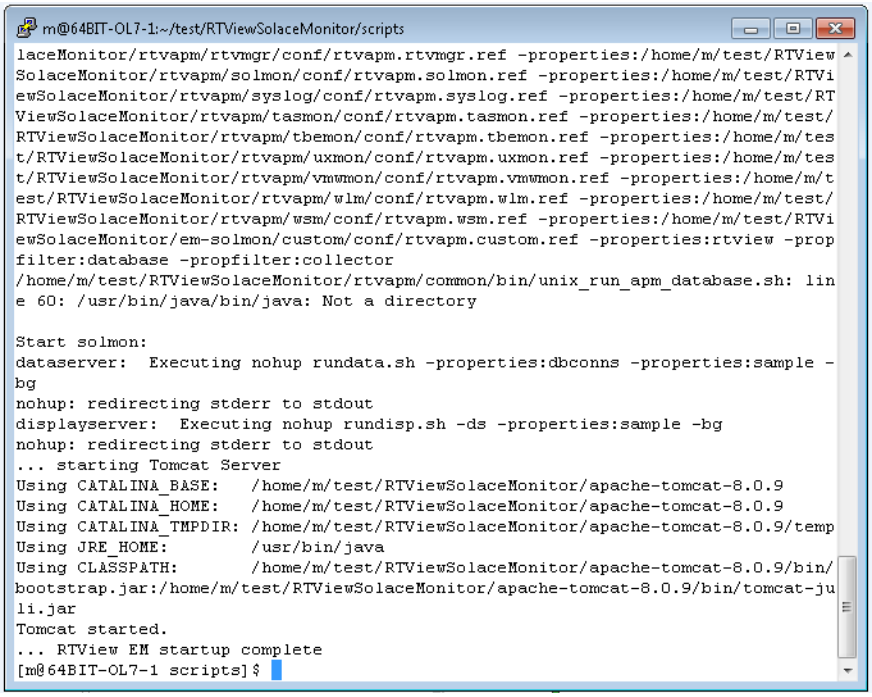
Proceed to "Start the Monitor," next.

Start the Monitor

To start the Monitor and Tomcat:

1. Change directory (**cd**) to **RTViewSolaceMonitor/bin**.
2. Execute **sh start_servers.sh** (or **start_servers.bat** for Windows) to start all Monitor components and Tomcat.

Important: UNIX/Linux - To make scripts in the **bin** directory executable you can use the **sh** command (as shown), or execute **chmod a+x start_servers.sh**, then execute **./start_servers.sh**.



3. Open a browser and go to **localhost:8068/rtview-solmon** (login ID/Password is **admin**/**admin**). Alternatively, if your system has a GUI available, you can open the Viewer by executing:

   ../start_viewer.sh (or **start_viewer.bat** for Windows).

   The Monitor opens.

4. In the Monitor, go to **Administration>**"RTView Cache Tables" on page 126 and verify that all caches are being populated with monitoring data (the number of rows in the table is greater than zero). If not, there is a problem with the connection to the Data Server. See "Troubleshooting" on page 8.

You have completed the Quick Start.

Stop the Monitor

To stop the Monitor and Tomcat:

1. Change directory (**cd**) to **RTViewSolaceMonitor/bin**.

2. Execute **../stop_servers.sh** (or **stop_servers.bat** for Windows) to stop all Monitor components and Tomcat.

3. Optionally, you can use **grep** or **Task Manager** to ensure that all RTView-related services are stopped.

- **UNIX**: Execute **ps –ef |grep rtv** to determine the Process Identifier of the processes still running and **kill -9 <ProcessId>** to terminate any that remain active.
- **Windows**: Open Task Manager and look for Java sessions with **hsqldb** or **rtv** in the execute statement and terminate any that remain active.

Troubleshooting

This section includes:

- "Log Files," next
- "JAVA_HOME" on page 9
- "Permissions" on page 9
- "Network/DNS" on page 9
- "Verify Data Received from Data Server" on page 9
- "Verify Port Assignments" on page 9

Log Files

When a Monitor component encounters an error, an error message is output to the console and/or to the corresponding log file. If you encounter issues, look for errors in the following log files, located in the **RTViewSolaceMonitor/em-solmon/servers/solmon/logs** directory:

- **dataserver.log**
- **displayserver.log**
- **historian.log**

Logging is enabled by default. If you encounter issues with log files, verify the **logs** directory exists in the **RTViewSolaceMonitor/em-solmon/servers/solmon** directory.

JAVA_HOME

If the terminal window closes after executing the **start_servers** command, verify that JAVA_HOME is set correctly.

Linux users: JAVA_HOME is required for Tomcat.

Permissions

If there are permissions-related errors in the response from the **start_servers** command, check ownership of the directory structure.

Network/DNS

If any log file shows reference to an invalid URL, check your system's hosts file and check with your Network Administrator that your access to the remote system is not being blocked.

Verify Data Received from Data Server

1. In the Monitor, go to **Administration>**"RTView Cache Tables" on page 126 and verify that all caches are being populated with monitoring data (the number of rows in the table is greater than 0). If not, there is a problem with the connection to the Data Server. Continue to the next step.

2. Verify the connection parameters in your **sample.properties** file.

3. "Stop the Monitor" and all processes.

4. After all processes stop, "Start the Monitor" and all processes.

5. In the Monitor, go to **Administration>**"RTView Cache Tables" on page 126 and verify that all caches are being populated with monitoring data (the number of rows in the table is greater than zero).

Verify Port Assignments

If the Viewer, Display Server or Historian fail to connect to the Data Server, or they receive no data, verify the ports are assigned correctly in your properties files and do the following:

1. "Stop the Monitor" and all processes.

2. After all processes stop, "Start the Monitor" and all processes.

3. In the Monitor, go to **Administration>**"RTView Cache Tables" on page 126 and verify that all caches are being populated with monitoring data (the number of rows in the table is greater than zero). If not, there is a problem with the connection to the Data Server.

CHAPTER 3 Quick Start - Solution Package

This section describes how to install, configure and start a Solution Package for an already deployed RTView EM system. These instructions are intended for users who installed the **standard** RTView Enterprise Monitor (which does not include Solution Packages) and now wish to add a Solution Package to their RTView Enterprise Monitor deployment.

See **README_sysreq.txt** for the full system requirements.

The Solution Package for Solace requires RTView Enterprise Monitor 3.2.

For Linux, these instructions require a Bourne-compatible shell.

This document assumes you created a project directory, **rtvapm_projects**, when you installed RTView Enterprise Monitor. All examples (of configurations, property settings, command execution and so forth) refer to the project directory. The Solution Package configuration is located in the **rtvapm_projects/emsample/servers** folder.

This section includes:

- "Install & Setup," next
- "Connect Your Message Routers" on page 12
- "Start the Monitor" on page 13
- "Stop the Monitor" on page 14
- "Troubleshooting" on page 15

Install & Setup

Prerequisite: RTView Enterprise Monitor 3.2 must be installed on your system.

To illustrate, we use the Solution Package for Solace as an example, where solmon is your Solution Package abbreviated name.

1. Download the **rtvapm_solmon_<version>.zip** archive to your local Windows/UNIX/Linux server.

2. Extract the files:

   Windows:
   Type **unzip rtvapm_solmon _<version>.zip** and save the files to the **C:\RTView** directory.

   UNIX/Linux:
   Type **unzip -a rtvapm_solmon _<version>.zip** and save the files to the **/opt/RTView** directory.

   Important: In Linux use **unzip -a RTViewSolaceMonitor_<VERSION>.zip**.

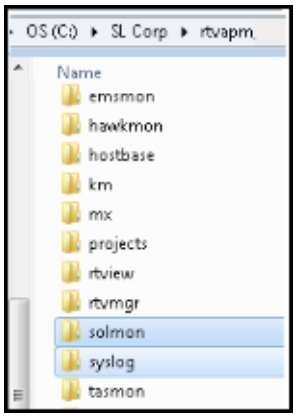
   Two directories are created under **rtvapm** in your RTView Enterprise Monitor installation: **solmon** and **syslog**.

3. Set JAVA_HOME to the location of your Java installation and include it in the path.

Important: This environment variable must also be defined in UNIX/Linux systems for Tomcat to start successfully.

4. Verify that the **solmon** and **syslog** directories were created under **rtvapm** and extracted correctly.

5. Verify you don't have an extra **rtvapm** directory containing **solmon** and **syslog**. If you do, move these directories under the first **rtvapm** directory and delete the nested **rtvapm**. Your directory structure should be similar to this:



6. Windows systems only: set JAVA_HOME to the location of your Java installation and include it in the path.

Proceed to "Connect Your Message Routers," next.

Connect Your Message Routers

Connect your own message routers and enable them for data collection.

1. Copy the **sample.properties** file, located in the **RTView/rtvapm/solmon/projects/sample** directory, to your Solution Package for Solace project directory, located in the **rtvapm_projects/emsample/solmon** directory.

2. Open the **sample.properties** file in your project directory and edit the following lines for each Solace message router you want to monitor (to enable the Monitor to collect data from them):

```
collector.sl.rtview.http.conn=__name=UNIQUE_APPLIANCE_NAME url=http://<IP or
hostname>:<port>/SEMP username=<user> password=<pass>
collector.sl.rtview.cache.config=sol_cache_source.rtv
$solConn:UNIQUE_APPLIANCE_NAME
```

where

- **<UNIQUE_APPLIANCE_NAME>** is a unique string to identify the connection of each monitored message router.
- **<IP or host-name>** is either an IP address or the host name that can be resolved by your network name resolution method.
- **<port>** is the SEMP port number configured for your message router.
- **<user>** and **<pass>** are the user credentials to log into the message router.

Example for two routers:
(where **xxx.xxx.xxx.xxx** = IP address)

```
collector.sl.rtview.http.conn=__name=example1 url=http://xxx.xxx.xxx.xxx:8050/SEMP
username=rtviewadmin password=rtview

collector.sl.rtview.cache.config=sol_cache_source.rtv  $solConn:example1

collector.sl.rtview.http.conn=__name=example2 url=http://xxx.xxx.xxx.xxx:8080/SEMP
username=rtviewadmin password=rtview

collector.sl.rtview.cache.config=sol_cache_source.rtv  $solConn:example2
```

3. If you do *not* have Syslog configured to capture event messages from your Solace message routers, skip this step and proceed to "Start the Monitor," next. If you *do* have Syslog configured, uncomment the lines under **SYSLOG CONNECTIONS** that apply and edit the connection parameters if needed.

```
#
# Configure connections to Syslog
#

#For messages sent via TCP, use
#collector.sl.rtview.syslogds.conn=__name=syslogTCP protocol=TCP host=localhost
port=601
#collector.sl.rtview.cache.config=sol_syslog_cache_source.rtv $conn:syslogTCP

#For messages sent via UDP, use
#collector.sl.rtview.syslogds.conn=__name=syslogUDP protocol=UDP host=localhost
port=514
#collector.sl.rtview.cache.config=sol_syslog_cache_source.rtv $conn:syslogUDP
```

NOTE: host refers to the network interface that will be used to receive Syslog messages (there might be more than one network interface available on the receiving system). Typically, this will be the IP address assigned to the selected network interface. If the system where the Monitor Data Server is running is also the Syslog receiver, then **localhost** can be used.

Proceed to "Start the Monitor," next.

Start the Monitor

Use the configuration defined in the **rtvservers.dat** file, located in the **RTView/rtvapm_projects/emsample/servers** directory. If you have started the central processes and your chosen application server, you only need to start the processes associated with the Solution Package for Solace, as described below.

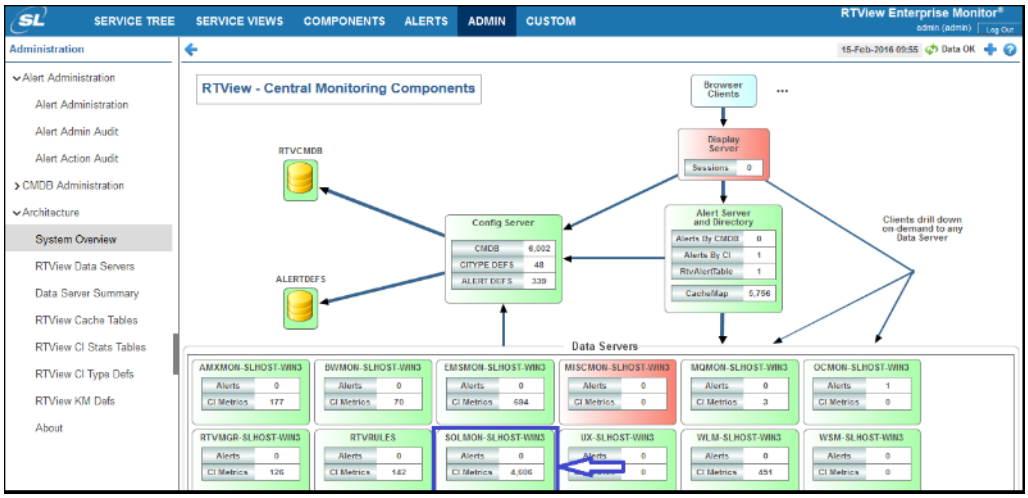
To start the Solution Package for Solace (in RTView Enterprise Monitor):

1. Change directory (**cd**) to **rtvapm_projects/emsample/servers**.

2. Execute **start_rtv.sh solmon –properties:sample** (or **start_rtv solmon –properties:sample** for Windows) to start all components of the Solution Package for Solace.

3. Open a browser and go to your RTView Enterprise Monitor deployment.

4. In the Monitor, open the Architecture->System Overview display to verify that the Data Server (named **SOLMON-LOCAL**, by default) is collecting data. The Data Server should be green and the **CI Metrics** value greater than zero (**0**). For example:



You have completed the Quick Start.

For information about configuring RTView Enterprise Monitor and Solution Packages for your production environment, see the *RTView Enterprise Monitor® User's Guide* available at http://www.sl.com/support/documentation/.

Stop the Monitor

To stop the Solution Package for Solace (in RTView Enterprise Monitor):

1. Change directory (**cd**) to **RTView/rtvapm_projects/emsample/servers**.

2. Execute **stop_rtv.sh solmon** (or **stop_rtv solmon** for Windows) to stop all components of the Solution Package for Solace.

3. Optionally, you can use **grep** or **Task Manager** to ensure that all RTView related services are stopped.

- **UNIX**: Execute **ps –ef |grep rtv** to determine the Process Identifier of processes still running and **kill -9 <ProcessId>** to terminate any that remain active.
- **Windows**: Open Task Manager and look for Java sessions with **hsqldb** or **rtv** in the execute statement and terminate any that remain active.

Troubleshooting

This section includes:

- "Log Files," next
- "JAVA_HOME" on page 15
- "Permissions" on page 15
- "Network/DNS" on page 15
- "Verify Data Received from Data Server" on page 15
- "Verify Port Assignments" on page 16

Log Files

When a Monitor component encounters an error, it outputs an error message to the console and/or to the corresponding log file. If you encounter issues, look for errors in the following log files:

- **dataserver.log**
- **displayserver.log**
- **historian.log**

which are located in the **rtvapm_projects/emsample/servers/solmon/logs** directory.

Logging is enabled by default. If you encounter issues with log files, verify the **logs** directory exists in the **rtvapm_projects/emsample/servers/solmon** directory.

JAVA_HOME

If the terminal window closes after executing the **start_rtv** command, verify that JAVA_HOME is set correctly.

Permissions

If there are permissions-related errors in the response from the **start_rtv** command, check ownership of the directory structure.

Network/DNS

If any log file shows reference to an invalid URL, check your system's hosts file and confirm with your Network Administrator whether your access to the remote system is being blocked.

Verify Data Received from Data Server

If you encounter problems collecting data, restart the Data Server, start the Monitor and go to Administration>RTView Cache Tables in the navigation tree. You should see all caches being populated with monitoring data (the number of rows in the table is greater than 0). If not, there is a problem with the connection to the Data Server.

Verify Port Assignments

If the Viewer, Display Server or Historian fail to connect to the Data Server or they receive no data, verify the ports are assigned correctly in your properties files and restart the Data Server.

CHAPTER 4 Standalone Production Configuration

This section describes how to configure the Monitor components for operation in your production environment. For Linux, these instructions assume a Bourne-compatible shell. For details about RTView® system requirements, see **README_sysreq.txt**.

This section includes:

- "Configure the Database," next
- "Configure Alert Notification" on page 20
- "Configure HA" on page 23
- "Setup Data Persistence" on page 24

Information you need:

- Login credentials for each Solace message router you will monitor.
- Defined connection string names that uniquely identify each Solace message router you will Monitor.

Configure the Database

The Monitor is delivered with a default memory resident HSQLDB database which is suitable for evaluation purposes. However, for production deployments, we recommend that you deploy one of our supported databases. For details about supported databases, see the *RTView Core® User's Guide*.

This section describes how to configure an alternate supported database for your production environment. You configure the database by editing properties in the **dbconns.properties** file, located in the **RTViewSolaceMonitor/em-solmon/conf** directory. To configure the database you will need login credentials for each Solace message router to be monitored.

Database Connections

The Monitor requires two database connections that provide access to the following information:

- Alert Settings

  Alert administration and alert auditing information is contained in the ALERTDEFS database. The values in the database are used by the alert engine at runtime. If this database is not available, the Self-Service Alerts Framework, under which alerts are executed, will not work correctly.

- Historical Data

Historical data that is used to track system behavior for future analysis, and to show historical data in displays, is contained in the RTVHISTORY database.

To Configure the Monitor Database:

1. Install a database engine of your choice. Supported database engines are Oracle, Sybase, Microsoft SQL Server, MySQL and DB2.

IMPORTANT: The default page size of DB2 is 4k. It is required that you create a DB2 database with a page size of 8k. Otherwise, table indexes will not work.

2. Open the **dbconns.properties** file, located in the **RTViewSolaceMonitor/em-solmon/conf** directory, and edit as described in the following steps.

3. In both the **ALERTDEFS** and **RTVHISTORY** sections, comment out the lines that apply to HSQLDB:

```
# Define the ALERTDEFS DB
# HSQLDB
#ConfigClient.sl.rtview.sql.sqldb=ALERTDEFS sa - jdbc:hsqldb:hsql://localhost:9099/
alertdefs org.hsqldb.jdbcDriver - false true

...

# Define the RTVHISTORY DB
# HSQLDB
#collector.sl.rtview.sql.sqldb=RTVHISTORY sa - jdbc:hsqldb:hsql://localhost:9099/
rtvhistory org.hsqldb.jdbcDriver - false true

# HSQLDB
#historian.sl.rtview.historian.driver=org.hsqldb.jdbcDriver
#historian.sl.rtview.historian.url=jdbc:hsqldb:hsql://localhost:9099/rtvhistory
#historian.sl.rtview.historian.username=sa
#historian.sl.rtview.historian.password=
```

4. Edit the initial property line to designate the location of the jar where the JDBC driver resides in your environment as follows:

   collector.sl.rtview.cp=JDBCDriverClassPath

   where **JDBCDriverClassPath** is the location of the JDBC driver file to use when connecting to your database. For example:

   collector.sl.rtview.cp=/opt/oracle/ora92/jdbc/lib/ojdbc14.jar

5. Under the **Define the ALERTDEFS DB** section, uncomment the line that corresponds to your supported database. For example, if your database is MySQL you uncomment the following:

```
# MySQL

ConfigClient.sl.rtview.sql.sqldb=ALERTDEFS myusername mypassword jdbc:mysql://
myhost:3306/myinstance com.mysql.jdbc.Driver - false false
```

6. Edit parameters in the line you just uncommented as appropriate for your environment, as follows:

- **myusername** - User name to enter into this database when making a connection.
- **myhost** - Full database URL to use when connecting to this database using the specified JDBC driver.
- **myinstance** – Instance name to use when connecting to this database
- **JDBCDriverClass** - Fully qualified name of the JDBC driver class to use when connecting to this database. In the example above the driver class is **com.mysql.jdbc.Driver**.
- **mypassword** - Password to enter into this database when making a connection. If there is no password, use "**-**".

Encrypt Password

If you need to provide an encrypted password (rather than expose server password names in a clear text file), use the encode_string command window option in an initialized command window with the following syntax:

encode_string sql mypassword

where **mypassword** is your plain text password.

For example:

encode_string sql mypassword

You then receive an encrypted password that you enter as your password. For example:

013430135501346013310134901353013450134801334

7. In the **Define the RTVHISTORY DB** section, uncomment the lines that correspond to your database. For example, if your database is MySQL you uncomment the following:

MySQL

collector.sl.rtview.sql.sqldb=RTVHISTORY myusername mypassword jdbc:mysql://myhost:3306/myinstance com.mysql.jdbc.Driver - false false

and

MySQL

historian.sl.rtview.historian.driver=com.mysql.jdbc.Driver
historian.sl.rtview.historian.url=jdbc:mysql://myhost:3306/myinstance
historian.sl.rtview.historian.username=myusername
historian.sl.rtview.historian.password=mypassword

8. Edit parameters in the line you just uncommented as appropriate for your environment (as previously) for **driver**, **url**, **username** and **password**.

9. **Save** the **dbconns.properties** file.

10. Create the database tables using the **.sql** template files provided. If your configured database user has table creation permissions, you only need to create the Alerts tables. If your configured database user does *not* have table creation permission, you must create both the Alerts tables and the History tables.

Use the **.sql** template file that corresponds to your database platform, located in the following directories:

- **RTViewSolaceMonitor/rtvapm/common/dbconfig/** for Alerts tables named **create_common_alertdefs_tables_<db>.sql**, where **<db>** is the prefix of the Data Base (**db2**, **mysql**, **oracle**, **sqlserver** or **sybase**).
- **RTViewSolaceMonitor/rtvapm/solmon/dbconfig/** for History tables named **create_solmon_history_tables_<db>.sql**, where **<db>** is the prefix of the Data Base (**db2**, **mysql**, **oracle**, **sqlserver** or **sybase**).

NOTE: The standard SQL syntax is provided for each database, but requirements can vary depending on database configuration. If you require assistance, consult with your database administrator.

The most effective method to load the .sql files to create the database tables depends on your database and how the database is configured. Some possible mechanisms are:

- **Interactive SQL Tool**

  Some database applications provide an interface where you can directly type SQL commands. Copy/paste the contents of the appropriate **.sql** file into this tool.

- **Import Interface**

  Some database applications allow you to specify a **.sql** file containing SQL commands. You can use the .sql file for this purpose.

Before loading the **.sql** file, create the database and declare the database name in the command line of your SQL client. For example, on MySQL 5.5 Command Line Client, to create the tables for the Alert Settings you first create the database:

create database myDBName;

before loading the .sql file:

mysql -u myusername -mypassword myDBName < create_common_alertdefs_tables_mysql.sql;

If you need to manually create the Historical Data tables, repeat the same process. In some cases it might also be necessary to split each of the table creation statements in the **.sql** file into individual files.

Third Party Application

If your database does not have either of the two above capabilities, a third party tool can be used to enter SQL commands or import **.sql** files. Third party tools are available for connecting to a variety of databases (RazorSQL, SQLMaestro, Toad, for example).

You have finished configuring the databases.

Configure Alert Notification

This section describes how to configure alert notification. This section includes:

- "Substitutions for Batch Files or Shell Scripts" on page 22
- "Notification Persistence" on page 23

The Monitor provides alerts concerning conditions in your system through RTView alerts. This section describes how to configure the alerts to execute an automated action. By default, alerts execute a **.bat** script. The script, by default, is not configured to execute an automated action. However, you can uncomment a line in the script that prints alert data to standard output. Or, you can modify the script to execute an automated action (such as sending an email alert).

There are two options for configuring Monitor alert notification: Batch/Shell Script files and Customization of the Java Command Handler. This document describes the configuration of Alert Notification through Batch/Shell Script files, which requires switching to an OS-specific set of alert definitions that execute the appropriate file type.

Windows and UNIX alert definition files are provided with the Monitor.

A sample batch file, **my_alert_actions.bat**, and a sample shell script, **my_alert_actions.sh**, located in the **RTViewSolaceMonitor/rtvapm/common/bin** directory, are provided as templates that you can modify as needed. Use the appropriate file for the platform that hosts Monitor processes. By default, both scripts send alert information to standard output.

To configure alert notification:

1. Copy the **my_alert_actions.sh|.bat** file, located in the **RTViewSolaceMonitor/rtvapm/common/bin** directory, into your **RTViewSolaceMonitor/em-solmon/servers/solmon** directory.

2. Open the **my_alert_actions.sh|.bat** file you just copied to **RTViewSolaceMonitor/em-solmon/servers/solmon** directory, and uncomment the echo line (near the end of the file) to print alert information to standard output. Or, you can modify the script to execute an automated action (such as sending an email alert).

3. Open the **sample.properties** file, located in your **RTViewSolaceMonitor/em-solmon/servers/solmon** directory, and uncomment the lines that apply in the **Configure Alert Notification** section:

For UNIX/Linux:

```
#sl.rtview.cmd_line=-sub:$scriptEnding:bat
sl.rtview.cmd_line=-sub:$scriptEnding:sh
sl.rtview.cmd_line=-sub:$alertActionScript:my_alert_actions
```

For Windows:

```
sl.rtview.cmd_line=-sub:$scriptEnding:bat
#sl.rtview.cmd_line=-sub:$scriptEnding:sh
sl.rtview.cmd_line=-sub:$alertActionScript:my_alert_actions
```

4. Save the **sample.properties** file.

5. Stop the Monitor as described in "Stop the Monitor" on page 8.

6. Start the Monitor as described in "Start the Monitor" on page 7.

Substitutions for Batch Files or Shell Scripts

The default **my_alert_actions** scripts use the substitutions described in the table below. When you customize the script, you can use a use substitution to get any of the columns in the alert table. To do this, modify the **sl.rtview.alert.notifiercommandnew** and **sl.rtview.alert.notifiercommandfirstsevchange** properties from Step 3 (above) to replace the default substitutions with the substitutions you want to use. You must make corresponding modifications to your script to use modified substitution values.

The substitution names map to the names of the columns in the alert table. Convert the column name to camel case and if it does not start with Alert, prepend alert to it. For example, to use the value of the **Alert Name** column, use **$alertName**. To use the value of the **ID** column, use **$alertID**. To use the value of the **Row Update Time** column, use **$alertRowUpdateTime**. The following table contains the substitutions used by the default **my_alert_actions** scripts:

Argument	Description	Values
$alertId	This substitution specifies the unique ID for the alert. For example: **alertId = 1004**	Text or Numeric
$alertIndex	This substitution specifies which source triggered the alert. With tabular objects, the first column of data is typically the **Index** column. The value in the **Index** column is a name that uniquely identifies each table row. The **alertIndex** uses the **Index** column name. For example, if the **CapactityLimitAllCaches** alert is configured to monitor all of your caches, and to trigger when any of the caches exceed the specified capacity threshold, the **alertIndex** indicates specifically which cache triggered the alert. With scalar objects, which do not have a table and therefore do not have a column (the **useTabularDataFlag** property is **False**), the **alertIndex** is blank. For example: **alertIndex = MyCache01**	Text or Numeric
$alertName =	This substitution specifies the name of the alert. For example: **alertName = CapacityLimitAllCaches**	Values vary.
$alertSeverity	This substitution specifies the severity level of the alert. **0**: The alert limit has not been exceeded therefore the alert is not activated. **1**: The alert warning limit has been exceeded. **2**: The alert alarm limit has been exceeded. For example: **alertSeverity = 1**	Numeric
$alertText	This substitution specifies the text that is displayed when the alert executes. For example: **alertText = High Warning Limit exceeded, current value: 0.9452 limit: 0.8**	Text
$alertTime	This value is the time the alert was initially generated.	Text

Notification Persistence

To prevent duplication and missed notifications after restart or failover, you must configure the Data Server for alert persistence. To do so, add the following property to your **sample.properties** file, located in the **RTViewSolaceMonitor/em-solmon/servers/solmon** directory:

collector.sl.rtview.alert.persistAlerts=true

Configure HA

High Availability (HA) mitigates single point of failure within the Monitor by providing a means of defining redundant system components, together with failover capability, for users of those components.

To setup HA you designate two components: the PRIMARY and the BACKUP. If the PRIMARY component fails, failover occurs to the BACKUP component. And when the PRIMARY component is subsequently restarted, the BACKUP component allows the newly restarted component to take the primary role and returns to its backup role.

The Monitor is available with a HA Data Server configuration. The **RTViewSolaceMonitor/em-solmon/servers** directory provides an example of HA for the Data Server. The property values controlling HA are defined in the **ha.properties** file located in the **RTViewSolaceMonitor/em-solmon/servers/solmon** directory.

The example assumes the availability of two machines which are defined by two environment variables: PRIMARYHOST and BACKUPHOST. You define these two environment variables on the PRIMARY and BACKUP machines that will host the Data Servers. HA configuration will not work if they are incorrectly defined.

The Monitor is configured by using the **solmon-primary** and **solmon-backup** configurations in the **rtvservers.dat** file located in the **RTViewSolaceMonitor/em-solmon/servers** directory.

The PRIMARY Data Server runs on **PRIMARYHOST**; the **BACKUP** Data Server runs on **BACKUPHOST**; the other Monitor applications failover between the Data Servers as appropriate. Assuming the environment variables **PRIMARYHOST** and **BACKUPHOST** are set correctly, Monitor components on the PRIMARYHOST are started as normal using the **solmon-primary** configuration (instead of the default configuration) with the **start_rtv** command. The **BACKUP** Monitor Data Server on the BACKUPHOST is started using the **solmon-backup** configuration with the **start_rtv** command.

To start the HA configuration, first start the PRIMARY Monitor components on the **PRIMARYHOST** using the **solmon-primary** configuration with the **start_rtv** command. For example, if you configured the connections of your Solace message routers in **sample.properties** file from the **RTViewSolaceMonitor\em-solmon\servers\solmon** directory:

UNIX

start_rtv.sh solmon-primary –properties:sample

Windows

start_rtv solmon-primary –properties:sample

Then start the BACKUP Monitor Data Server on the backup machine using the **solmon-backup** configuration with the **start_rtv** command. For example:

UNIX

start_rtv.sh solmon-backup –properties:sample

Windows

start_rtv solmon-backup –properties:sample

Setup Data Persistence

To enable storage of historical data:

Edit the **start_servers.sh|.bat** and **stop_servers.sh|.bat** scripts, located in the **RTViewSolaceMonitor/bin** directory, by uncommenting the following two lines as follows:

start_rtv.sh solmon historian $*

and

stop_rtv.sh solmon historian $*

By default, storage of historical data is only enabled for the **SolAppliances** and **SolVpns** caches. If you want to enable storage of historical data for all caches, comment out the property associated with the cache in the **sample.properties** file, located in the **RTViewSolaceMonitor/em-solmon/servers/solmon** directory:

- To persist data for the **SolApplianceInterfaces** cache, comment out the following line:

#collector.sl.rtview.sub=$SOL_INTERFACE_TABLE:''

- To persist data for the **SolBridgeStats** cache, comment out the following line:

#collector.sl.rtview.sub=$SOL_BRIDGE_STATS_TABLE:''

- To persist data for the **SolClientStats** cache, comment out the following line:

#collector.sl.rtview.sub=$SOL_CLIENT_STATS_TABLE:''

- To persist data for the **SolEndpoints** cache, comment out the following line:

#collector.sl.rtview.sub=$SOL_ENDPOINT_TABLE:''

- To persist data for the **SolEndpointStats** cache, comment out the following line:

#collector.sl.rtview.sub=$SOL_ENDPOINT_STATS_TABLE:''

- To persist data for the **SolApplianceMessageSpool** cache, comment out the following line:

#collector.sl.rtview.sub=$SOL_MESSAGE_SPOOL_TABLE:''

CHAPTER 5 Using the Monitor

The RTView® Monitor for Solace® is an advanced messaging platform that allows customer applications to efficiently exchange messages over dedicated VPNs. The RTView® Monitor for Solace® provides pre-configured alerts and dashboards to monitor current status and manage history for the Solace message router. The RTView® Monitor for Solace® can help operators avoid or detect many problems relating to configuration, topology, and performance. This section describes Monitor features, graphs and functionality as well as Monitor displays. This section includes:

- "Overview" on page 26: Describes the Monitor features and functionality.
- "Message Routers" on page 33: The displays in this View present views of message router-level metrics, which reflect configuration settings, total throughput, current status, errors, and value-added calculations that summarize metrics across all of the VPNs.
- "VPNs" on page 59: The displays in this View present views of the VPN-level metrics.
- "Clients" on page 73: The displays in this View present views of all clients for the message router. These views can be filtered to limit the displays to clients for a single VPN.
- "Bridges" on page 83: The displays in this View present views of all bridges for the message router. These views can be filtered to limit the displays to bridges for a single VPN.
- "Endpoints" on page 91: The displays in this View present views of all topics and queues for the message router, which can be filtered to limit the displays to topics and queues for a single VPN.
- "Capacity Analysis" on page 100: The displays in this View present current metrics, alert count and severity at the message router level.
- "Syslog" on page 111: View all Syslog events for your Solace message routers.
- "Alert Views" on page 114: The displays in this View show current alerts across all message routers and allow you to track, manage, and assign alerts.
- "Administration" on page 118: The displays in this View enable you to set global alerts and override alerts. You can also view internal data gathered and stored by RTView (used for troubleshooting with SL Technical Support).
- "RTView Servers" on page 129: The displays in this View enable you to monitor performance of all RTView Servers.

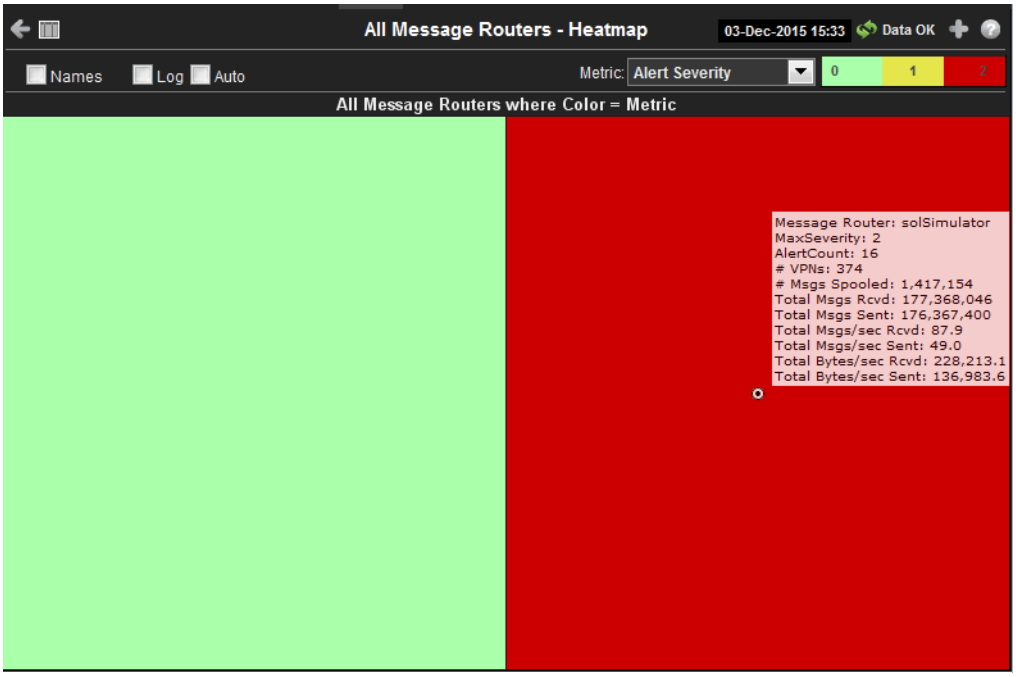
Overview

This section describes the main Monitor features, how to read Monitor objects, GUI functionality and navigation. This section includes:

- "Monitor Main Display" on page 26: Describes the Monitor display that opens by default as well as the navigation tree.
- "Heatmaps" on page 27: Describes how to read heatmaps and heatmap functionality.
- "Tables" on page 28: Describes how to read tables and table functionality.
- "Trend Graphs" on page 28: Describes how to read trend graphs and trend graph functionality.
- "Title Bar" on page 30: Describes the top layer of the title bar shared by Monitor displays.
- "Context Menu" on page 30: Describes right-click popup menu in the Monitor.
- "Multiple Windows" on page 31: Describes opening multiple windows in the Monitor.
- "Export Report" on page 31: Describes how to export reports from the Monitor.

Monitor Main Display

The **All Message Routers Heatmap** is the default display of the Monitor. This color-coded heatmap provides a good starting point for immediately getting the status of all your Solace message routers. To open the Solution Package for Solace in the RTView Enterprise Monitor®, choose the **Components** tab > **By Vendor** option > **Other** > **Solace Message Router** or choose the **Components** tab > **By Technology** option > **Middleware** > **Solace Message Router**. The following figure illustrates the Monitor.



NOTE: It takes about 60 seconds after the Monitor Data Server is started for data to initially appear in Monitor displays. By default, data is collected every 20 seconds and displays are refreshed every 2 seconds.

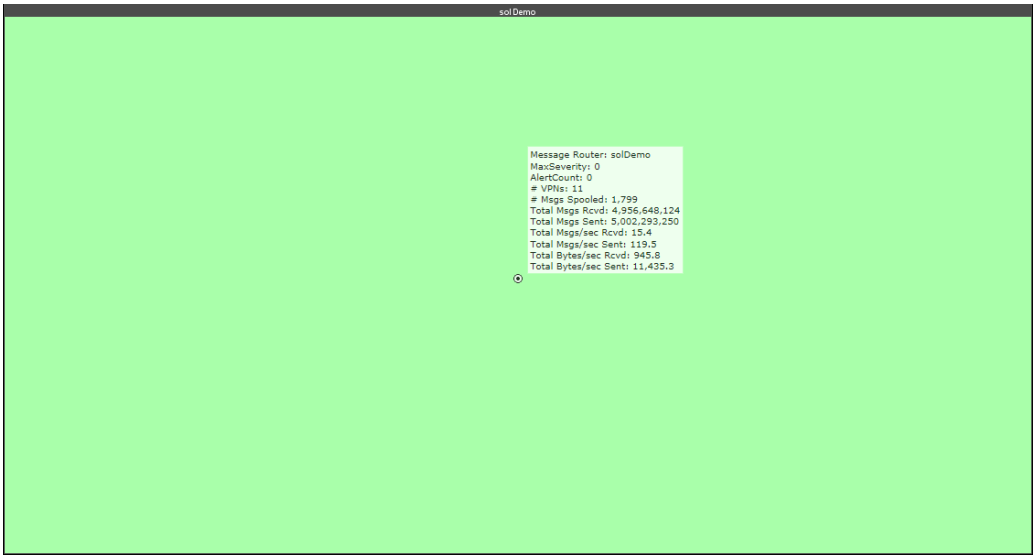
Navigation Tree

The Monitor navigation tabs are organized by *Views.* Each View features performance data for a type of system resource. Typically, the performance data is shown in a tabular, heatmap, and summary display for each View.

Heatmaps

Heatmaps organize your Solace resources (message routers, VPNs, and so forth) into rectangles and use color to highlight the most critical values in each. Heatmaps enable you to view various metrics in the same heatmap using drop-down menus. Each metric has a color gradient bar that maps relative values to colors. In most heatmaps, the rectangle size represents the number of resources in the rectangle. Heatmaps include drop-down menus to filter data by. The filtering options vary among heatmaps.

For example, each rectangle in the **All Message Routers Heatmap** represents an message router, where color is representative of the selected **Metric**.



The **Metric** drop-down menu in this heatmap contains options to show **Alert Severity**, **Alert Count**, as well as other metrics. Menu options vary according to the data populating the heatmap. **Alert Severity** is selected and its corresponding color gradient bar is shown. **Alert Severity** is the maximum level of alerts in the heatmap rectangle. Values range from **0** - **2**, as indicated in the color gradient bar, where **2** is the highest **Alert Severity**:

Red indicates that one or more resources associated with that application currently has an alert in an alarm state.

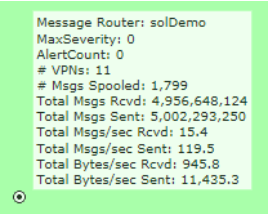
Yellow indicates that one or more resources associated with that application currently have an alert in a warning state.

Green indicates that no resources associated with that application have alerts in a warning or alarm state.

In most heatmaps, you can also drill-down to a *Summary* display containing detailed data for the resource (in this case, you drill-down to detailed data for the selected message router in the **Single Message Router Summary** display). You can also open a new window and then drill-down. The drill-down opens a display that contains relevant and more detailed data.

Mouse-over

The mouse-over functionality provides additional detailed data in an over imposed pop-up window when you mouse-over a heatmap. The following figure illustrates mouse-over functionality in a heatmap object.

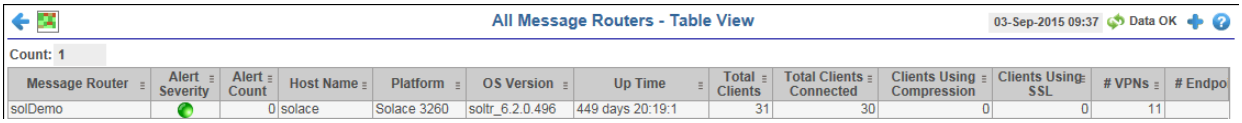


Log Scale

Typically, heat maps provide the Log Scale option, which enables visualization on a logarithmic scale. This option should be used when the range in your data is very broad. For example, if you have data that ranges from the tens to the thousands, then data in the range of tens will be neglected visually if you do not check this option. This option makes data on both extreme ranges visible by using the logarithmic of the values rather than the actual values.

Tables

Monitor tables contain the same data that is shown in the heatmap in the same View. Tables provide you a text and numeric view of the data shown in that heatmap, and additional data not included the heatmap. For example, the **All Message Routers Table** display (shown below) shows the same data as the **All Message Routers Heatmap** display (shown previously).



Message Router	Alert Severity	Alert Count	Host Name	Platform	OS Version	Up Time	Total Clients	Total Clients Connected	Clients Using Compression	Clients Using SSL	# VPNs	# Endpo
solDemo		0	solace	Solace 3260	soltr_6.2.0.496	449 days 20:19:1	31	30	0	0	11	

Table rows also sometimes use color to indicate the current most critical alert state for all resources associated with a given row. For example, the color coding is typically as follows:

Red indicates that one or more resources associated with that message router currently has an alert in an alarm state.

Yellow indicates that one or more resources associated with that message router currently have an alert in a warning state.

Green indicates that no resources associated with that message router currently have an alert in a warning or alarm state.

Sorting

The Monitor allows you to sort table rows. Select sort in the column title, then choose **Sort Ascending**, **Sort Descending**, **Columns**, **Filter**, **Lock**/**Unlock** or **Settings**.

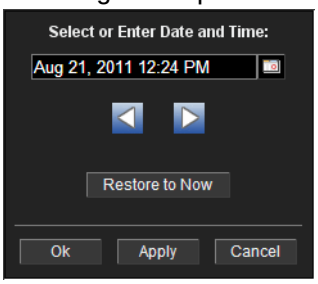
Trend Graphs

Monitor trend graphs enable you to view and compare performance metrics over time. You can use trend graphs to assess utilization and performance trends.

For example, the following figure illustrates a typical Monitor trend graph.

Time Range

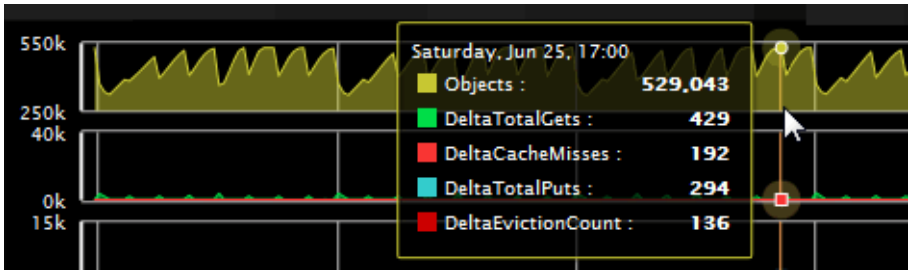
Select a time range from the drop down menu varying from **2 Minutes** to **Last 7 Days**, or display **All Data**. By default, the time range end point is the current time.



To change the time range click Open Calendar , choose the date and time, then click **OK**. Or enter the date and time in the text field using the following format: **MMM dd, YYYY HH:MM:ss**. For example, Aug 21, 2011 12:24 PM. Click **Apply**. Use the Navigation Arrows to move forward or backward one time period (the time period selected from the Time Range drop-down menu). Click **Restore to Now** to reset the time range end point to the current time.

Mouse-over

The mouse-over functionality provides additional detailed data in an over imposed pop-up window when you mouse-over trend graphs. The following figure illustrates mouse-over functionality. In this example, when you mouse-over a single dot, or data point, a pop-up window shows data for that data point.



Log Scale

Typically, trend graphs provide the **Log Scale** option. **Log Scale** enables you to see usage correlations for data with a wide range of values. For example, if a minority of your data is on a scale of tens, and a majority of your data is on a scale of thousands, the minority of your data is typically not visible in non-log scale graphs. **Log Scale** makes data on both scales visible by applying logarithmic values rather than actual values to the data.

Title Bar

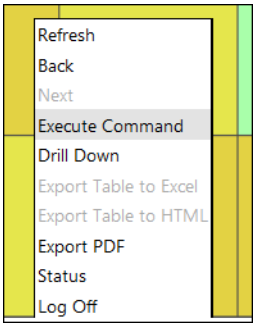
Displays share the same top layer in the title bar, as shown below.

The following table describes the functionality in the display title bar.

	Opens the previous display.
	Opens the display that is up one level.
Table	Navigates to a display that is most commonly accessed from the current display. The target display differs among displays.
	Opens the Alerts Table display in a new window.
19-Feb-2014 16:50	The current date and time. If the time is incorrect, this might indicate that RTView stopped running. When the date and time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.
Data OK	The data connection state. Red indicates the data source is disconnected (for example, if the Data Server is not receiving data, or if the Display Server does not receive data from the Data Server, this will be red). Green indicates the data source is connected. When the date and time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.
	Opens an instance of the same display in a new window. Each window operates independently, allowing you to switch views, navigate to other displays in RTView EM, and compare server performance data.
	Opens the online help page for the current display.

Context Menu

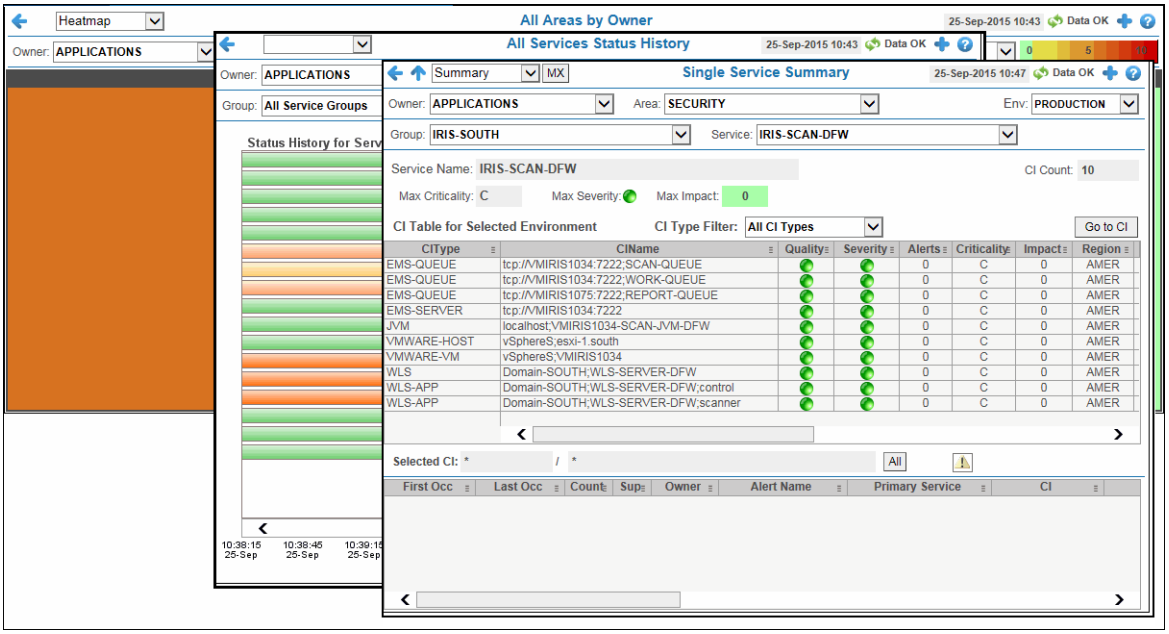
Typically, you can right-click on displays to open a popup menu. By default, options include **Refresh**, **Back**, **Next**, **Execute Command**, **Drill Down**, **Export Table to Excel**, **Export Table to HTML**, **Export PDF**, **Status** and **Log Off**. The following figure illustrates the popup menu in a heatmap.



For details about exporting a PDF report, see "Export Report" on page 31.

Multiple Windows

The following illustrates the use of Open New Window in the RTView Enterprise Monitor.

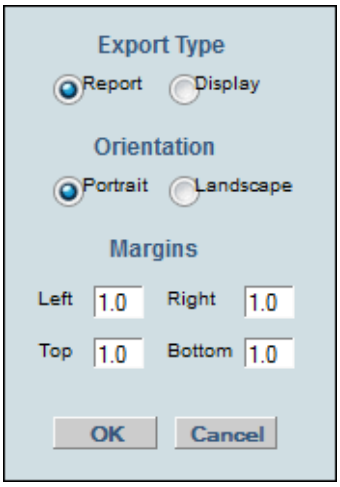


Export Report

You can quickly export reports for displays, or for tables and grid objects in a display, to a PDF file.

To generate a report for a display:

Right-click on the display and select **Export PDF**. The **Export to PDF** dialog opens.

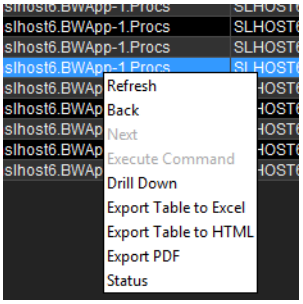


Set the margins and choose the **Export Type**:

- **Report**: Generates an image of the display on the first page, followed by at least one page for each table or object grid in the display. As many pages as are necessary to show all the data in each table or object grid are included in the report. This enables you to view all data in a table or object grid that you otherwise must use a scrollbar to see. If there are no tables or object grids in your display, you only get a image of the display.
- **Display**: Generates an image of the display in PDF format.Choose the page orientation (**Portrait** or **Landscape**), set the page margins and click **OK**. The report opens in a new window.

To generate a report for a table or grid object in a display:

Right-click on the table or grid object and choose **Export PDF**, **Export Table to Excel** or **Export Table to HTML**.



Message Routers

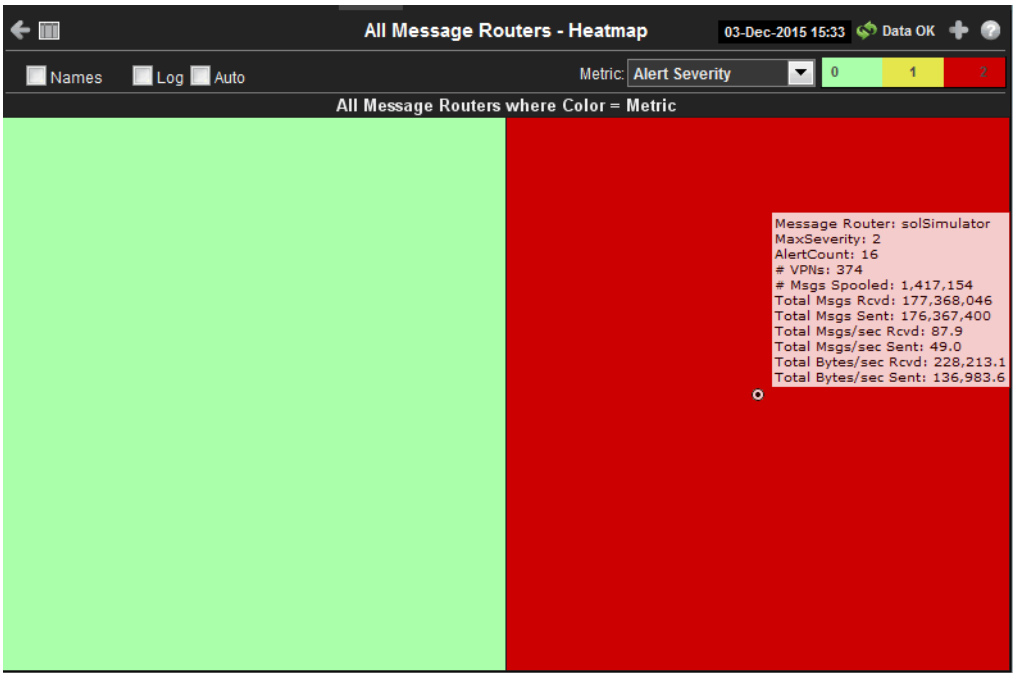
These displays provide detailed data and statuses for message routers and their connected message routers. Displays in this View are:

- "All Message Routers Heatmap" on page 33: A color-coded heatmap view of the current status of each of your message routers.
- "All Message Routers Table" on page 36: A tabular view of all available message router performance data.
- "Message Router Summary" on page 43: Current and historical metrics for a single message router.
- "Environmental Sensors" on page 47: Provides value and status information for all sensors on a single message router or for all sensors for all message routers.
- "Message Router Provisioning" on page 48: Provides message router host, chassis, redundancy, memory, and fabric data for a particular message router.
- "Interface Summary" on page 51: Provides detailed data and status information for the interfaces associated with one or all message router(s). You can also view current and historical amounts of incoming and outgoing packets and bytes for a selected interface in a trend graph.
- "Message Spool Table" on page 54: Provides status and usage data for message spools associated with one or all message router(s).
- "Message Router VPN Activity" on page 56: Provides the number of connections for each client connected to a specific message router and lists the average incoming and outgoing bytes per minute for each of the connected clients.
- "CSPF Neighbors Table" on page 58: View metrics for Solace "neighbor" message routers that use the Content Shortest Path First (CSPF) routing protocol to determine the shortest path in which to send messages from one message router to another message router in the Solace network.

All Message Routers Heatmap

This heatmap shows the current status of all message routers for the selected metric. Use this to quickly identify the current status of each of your message routers for each available metric: the current alert severity, alert count, number of spooled messages, total messages received, total messages sent, total number of messages received per second, total number of messages sent per second, total bytes received per second, and the total bytes sent per second. By default, this display shows the heatmap based on the **Alert Severity** metric.

You can use the **Names** check-box ☑ to include or exclude labels in the heatmap, and you can mouse over a rectangle to see additional metrics for an message router. Clicking one of the rectangles in the heatmap opens the "Message Router Summary" display, which allows you to see additional details for the selected message router.



Title Bar: Indicators and functionality might include the following:

Open the previous and upper display.

Table Navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

Fields and Data:

Names	Select this check box to include labels in the heatmap.
Log	Select to this check box to enable a logarithmic scale. Use **Log Scale** to see usage correlations for data with a wide range of values. For example, if a minority of your data is on a scale of tens, and a majority of your data is on a scale of thousands, the minority of your data is typically not visible in non-log scale graphs. **Log Scale** makes data on both scales visible by applying logarithmic values rather than actual values to the data.
Auto	Select to enable auto-scaling. When auto-scaling is activated, the color gradient bar's maximum range displays the highest value. **Note:** Some metrics auto-scale automatically, even when **Auto** is not selected.
Metric	Choose a metric to view in the display.

Alert Severity The current alert severity. Values range from **0** - **2**, as indicated in the color gradient bar, where **2** is the highest Alert Severity:

Red indicates that one or more metrics exceeded their ALARM LEVEL threshold.

Yellow indicates that one or more metrics exceeded their WARNING LEVEL threshold.

Green indicates that no metrics have exceeded their alert thresholds.

Alert Count The total number of critical and warning unacknowledged alerts in the message router. The color gradient bar, populated by the current heatmap, shows the value/color mapping. The numerical values in the gradient bar range from **0** to the maximum count of alerts in the heatmap. The middle value in the gradient bar indicates the average alert count.

 # Msgs Spooled The total number of spooled messages in the message router. The color gradient bar, populated by the current heatmap, shows the value/color mapping. The numerical values in the gradient bar range from 0 to the defined alert threshold of **SolMsgRouterSpoolUtilization**. The middle value in the gradient bar indicates the middle value of the range.

When **Auto** is checked, the numeric values in the color gradient bar show the range of the data being displayed rather than the default values. The middle value changes accordingly to indicate the color of the middle value of the range.

Total Msgs Rcvd The total number of received messages in the message router. The color gradient bar, populated by the current heatmap, shows the value/color mapping. The numerical values in the gradient bar range from **0** to the maximum count of total messages received in the heatmap. The middle value in the gradient bar indicates the average count.

The **Auto** flag does not have any impact on this metric.

Total Msgs Sent The total number of sent messages in the message router. The color gradient bar, populated by the current heatmap, shows the value/color mapping. The numerical values in the gradient bar range from **0** to the maximum count of total messages sent in the heatmap. The middle value in the gradient bar indicates the average count.

The **Auto** flag does not have any impact on this metric.

Total Msgs/ sec Rcvd The total number of messages received per second in the message router. The color gradient bar, populated by the current heatmap, shows the value/color mapping. The numerical values in the gradient bar range from 0 to the defined alert threshold of **SolMsgRouterInboundMsgRateHigh**. The middle value in the gradient bar indicates the middle value of the range.

When **Auto** is checked, the numeric values in the color gradient bar show the range of the data being displayed rather than the default values. The middle value changes accordingly to indicate the color of the middle value of the range.

Total Msgs/ sec Sent The total number of messages sent per second in the message router. The color gradient bar, populated by the current heatmap, shows the value/color mapping. The numerical values in the gradient bar range from 0 to the defined alert threshold of **SolMsgRouterOutboundMsgRateHigh**. The middle value in the gradient bar indicates the middle value of the range.

When **Auto** is checked, the numeric values in the color gradient bar show the range of the data being displayed rather than the default values. The middle value changes accordingly to indicate the color of the middle value of the range.

Total Bytes/ sec Rcvd

The total number of bytes received per second in the message router. The color gradient bar, populated by the current heatmap, shows the value/color mapping. The numerical values in the gradient bar range from 0 to the defined alert threshold of **SolMsgRouterInboundByteRateHigh**. The middle value in the gradient bar indicates the middle value of the range.

When **Auto** is checked, the numeric values in the color gradient bar show the range of the data being displayed rather than the default values. The middle value changes accordingly to indicate the color of the middle value of the range.

Total Bytes/ sec Sent

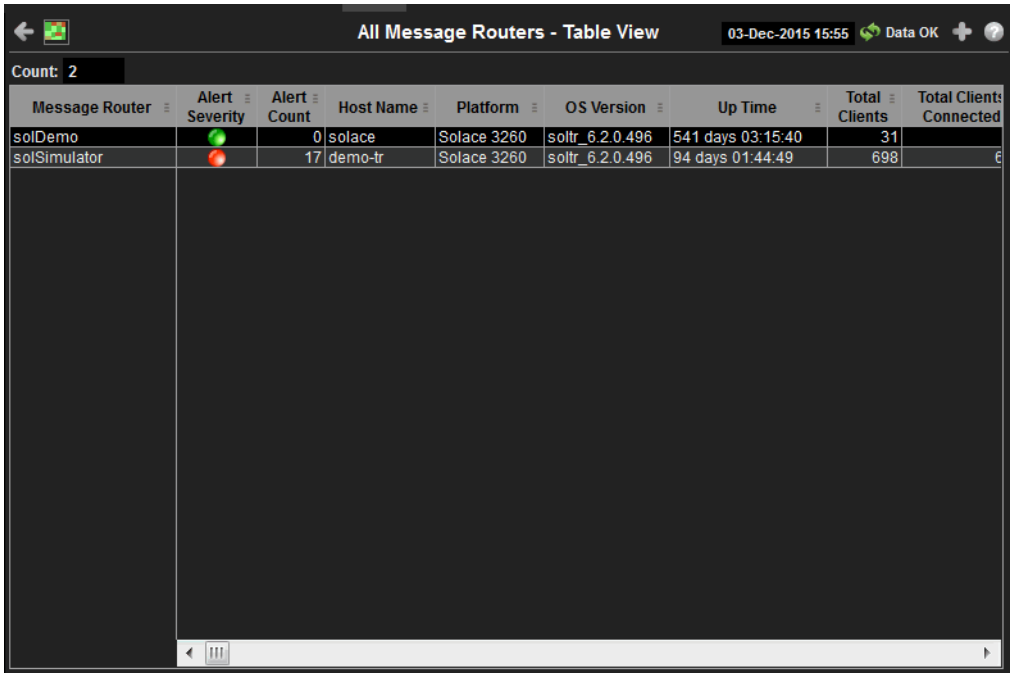
The total number of bytes sent per second in the message router. The color gradient bar, populated by the current heatmap, shows the value/color mapping. The numerical values in the gradient bar range from 0 to the defined alert threshold of **SolMsgRouterOutboundByteRateHigh**. The middle value in the gradient bar indicates the middle value of the range.

When **Auto** is checked, the numeric values in the color gradient bar show the range of the data being displayed rather than the default values. The middle value changes accordingly to indicate the color of the middle value of the range.

All Message Routers Table

View current status data for all message routers in a tabular format. Data shown in the "All Message Routers Heatmap" is included here with additional details. Each row in the table is a different message router. You can click a column header to sort column data in numerical or alphabetical order.

Drill-down and investigate by clicking a row to view details for the selected message router in the "Message Router Summary" display



Message Router	Alert Severity	Alert Count	Host Name	Platform	OS Version	Up Time	Total Clients	Total Clients Connected
solDemo		0	solace	Solace 3260	soltr_6.2.0.496	541 days 03:15:40	31	
solSimulator		17	demo-tr	Solace 3260	soltr_6.2.0.496	94 days 01:44:49	698	6

Title Bar: Indicators and functionality might include the following:

Open the previous and upper display.
Table Navigate to displays commonly accessed from this display.
19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.
Open the **Alert Views - RTView Alerts Table** display.
Open an instance of this display in a new window.
Open the online help page for this display.

Fields and Data:

Count	Total number of message routers found.

Table:
Each row in the table is a different message router.

Message Router	The name of the message router.
Alert Severity	The current alert severity. Values range from **0** - **2**, as indicated in the color gradient bar, where **2** is the highest Alert Severity: Red indicates that one or more metrics exceeded their ALARM LEVEL threshold. Yellow indicates that one or more metrics exceeded their WARNING LEVEL threshold. Green indicates that no metrics have exceeded their alert thresholds.
Alert Count	The total number of alerts.
Host Name	The name of the host.
Platform	The name of the platform.
OS Version	The version of the operating system.
Up Time	The amount of time that the message router has been up and running.
Total Clients	The total number of clients associated with the message router.
Total Clients Connected	The total number of clients that are currently connected to the message router.
Clients Using Compression	The number of clients who send/receive compressed messages.
Clients Using SSL	The number of clients using SSL for encrypted communications.
Max Client Connections	The maximum number of available client connections.
# VPNs	The total number of VPNs configured on the message router.
# Endpoints	The total number of Endpoints configured on the message router.
# Bridges	The total number of bridges configured on the message router.
# Local Bridges	The total number of local bridges configured on the message router.

# Remote Bridges	The total number of remote bridges configured on the message router.
# Remote Bridge Subscriptions	The total number of remote bridge subscriptions configured on the message router.
Routing Enabled	This check box is checked when the message router is configured to route messages to other message routers.
Routing Interface	The name of the interface configured to support message routing.
Total # Conflicting Destinations	The total number conflicting destinations.
Pending Messages	The number of pending messages on the message router.
Total Client Msgs Rcvd	The total number of client messages received on the message router.
Total Client Msgs Sent	The total number of client messages sent by the message router.
Total Client Msgs Rcvd / sec	The total number of client messages received per second by the message router.
Total Client Msgs Sent / sec	The total number of client messages sent by the message router.
Total Client Bytes Rcvd	The total number of client bytes received by the message router.
Total Client Bytes Sent	The total number of client bytes sent by the message router.
Total Client Bytes Rcvd / sec	The total number of client bytes received per second by the message router.
Total Client Bytes Sent / sec	The total number of client bytes sent per second by the message router.
Total Client Direct Msgs Rcvd	The total number of direct client messages received by the message router.
Total Client Direct Msgs Sent	The total number of direct client messages sent from the message router.
Total Client Direct Msgs Rcvd / sec	The total number of direct client messages received per second by the message router.
Total Client Direct Msgs Sent / sec	The total number of direct client messages sent per second by the message router.
Total Client Direct Bytes Rcvd	The total number of direct client bytes received by the message router.
Total Client Direct Bytes Sent	The total number of direct client bytes sent by the message router.

Total Client Direct Bytes Rcvd / sec	The total number of direct client bytes received per second by the message router.
Total Client Direct Bytes Sent / sec	The total number of direct client bytes sent per second by the message router.
Total Client Non-Persistent Msgs Rcvd	The total number of non-persistent client messages received by the message router.
Total Client Non-Persistent Msgs Sent	The total number of non-persistent client messages sent by the message router.
Total Client Non-Persistent Msgs Rcvd / sec	The total number of non-persistent client messages received per second by the message router.
Total Client Non-Persistent Msgs Sent / sec	The total number of non-persistent client messages sent per second by the message router.
Total Client Non-Persistent Bytes Rcvd	The total number of non-persistent client bytes received by the message router.
Total Client Non-Persistent Bytes Sent	The total number of non-persistent client bytes sent by the message router.
Total Client Non-Persistent Bytes Rcvd / sec	The total number of non-persistent client bytes received per second by the message router.
Total Client Non-Persistent Bytes Sent / sec	The total number of non-persistent client bytes sent per second by the message router.
Total Client Persistent Msgs Rcvd	The total number of persistent client messages received by the message router.
Total Client Persistent Msgs Sent	The total number of persistent client messages sent by the message router.
Total Client Persistent Msgs Rcvd / sec	The total number of persistent client messages received per second by the message router.
Total Client Persistent Msgs Sent / sec	The total number of persistent client messages sent per second by the message router.
Total Client Persistent Bytes Rcvd	The total number of persistent client bytes received by the message router.
Total Client Persistent Bytes Sent	The total number of persistent client bytes sent by the message router.
Total Client Persistent Bytes Rcvd / sec	The total number of persistent client bytes received per second by the message router.

Total Client Persistent Bytes Sent / sec	The total number of persistent client bytes sent per second by the message router.
Avg Egress Bytes / min	The average number of outgoing bytes per minute.
Avg Egress Compressed Msgs / min	The average number of outgoing compressed messages per minute.
Avg Egress Msgs / min	The average number of outgoing messages per minute.
Avg Egress SSL Msgs / min	The average number of outgoing messages per minute being sent via SSL-encrypted connections.
Avg Egress Uncompressed Msgs / min	The average number of uncompressed outgoing messages per minute.
Avg Ingress Bytes / min	The average number of incoming bytes per minute.
Avg Ingress Compressed Msgs / min	The average number of compressed incoming message per minute.
Avg Ingress Msgs / min	The average number of incoming messages per minute.
Average Ingress SSL Msgs / min	The average number of incoming messages per minute being received via SSL-encrypted connections.
Avg Ingress Uncompressed Msgs / min	The average number of uncompressed messages per minute.
Current Egress Bytes / sec	The current number of outgoing bytes per second.
Current Egress Compressed Msgs / sec	The current number of outgoing compressed messages per second.
Current Egress Msgs / sec	The current number of outgoing messages per second.
Current Egress SSL Msgs / sec	The current number of outgoing messages per second sent via SSL-encrypted connections.
Current Egress Uncompressed Msgs / sec	The current number of outgoing uncompressed messages per second.
Current Ingress Bytes / sec	The current number of incoming bytes per second.
Current Ingress Compressed Msgs / sec	The current number of incoming compressed messages per second.
Current Ingress Msgs / sec	The current number of incoming messages per second.
Current Ingress SSL Msgs / sec	The current number of incoming messages per second received via SSL-encrypted connections.

Current Ingress Uncompressed Msgs/sec	The current number of incoming uncompressed messages per second.
Ingress Comp Ratio	The percentage of incoming messages that are compressed.
Egress Comp Ratio	The percentage of outgoing messages that are compressed.
Egress Compressed Bytes	The number of outgoing compressed bytes.
Egress SSL Bytes	The number of outgoing compressed bytes being sent via SSL-encrypted connections.
Egress Uncompressed Bytes	The number of outgoing uncompressed bytes.
Ingress Compressed Bytes	The number of incoming compressed bytes.
Ingress SSL Bytes	The number of incoming bytes via SSL-encrypted connections.
Ingress Uncompressed Bytes	The number of incoming uncompressed bytes.
Total Egress Discards	The total number of outgoing messages that have been discarded by the message router.
Total Egress Discards/sec	The total number of outgoing messages per second that have been discarded by the message router.
Total Ingress Discards	The total number of incoming messages that have been discarded by the message router.
Total Ingress Discards/sec	The total number of incoming messages per second that have been discarded by the message router.
Client Authorization Failures	The number of failed authorization attempts
Client Connect Failures (ACL)	The number of client connection failures caused because the client was not included in the defined access list.
Subscribe Topic Failures	The number of failed attempts at subscribing to topics.
TCP Fast Retrans Sent	The total number of messages that were retransmitted as a result of TCP Fast Retransmission (one or more messages in a sequence of messages that were not received by their intended party that were sent again).
Memory (KB)	The total available memory (in kilobytes) on the message router.
Memory Free (KB)	The total amount of available memory (in kilobytes) on the message router.
Memory Used (KB)	The total amount of memory used (in kilobytes) on the message router.
Memory Used %	The percentage of total available memory that is currently being used.

Swap (KB)	The total available swap (in kilobytes) on the message router.
Swap Free (KB)	The total amount of available swap (in kilobytes) on the message router.
Swap Used (KB)	The total amount of swap used (in kilobytes) on the message router.
Swap Used %	The percentage of total available swap that is currently being used.
Subscription Mem Total (KB)	The total amount of available memory (in kilobytes) that can be used by queue/ topic subscriptions.
Subscription Mem Free (KB)	The current amount of available memory (in kilobytes) that can be used by queue/ topic subscriptions.
Subscription Mem Used (KB)	The current amount of memory (in kilobytes) being used by queue/topic subscriptions.
Subscription Mem Used %	The percentage of available memory being used by queue/topic subscriptions.
Chassis Product Number	The product number of the chassis in which the router is contained.
Chassis Revision	The revision number of the chassis.
Chassis Serial	The serial number of the chassis.
BIOS Version	The basic input/output system used by the chassis.
CPU-1	The name of the central processing unit (CPU 1) used by the message router.
CPU-2	The name of the central processing unit (CPU 2) used by the message router.
Operational Power Supplies	The number of available power supplies that are operational on the chassis.
Power Redundancy Config	The configuration used by the backup message router.
Max # Bridges	The maximum number of bridges allowed on the message router.
Max # Local Bridges	The maximum number of local bridges allowed on the message router.
Max # Remote Bridges	The maximum number of remote bridges allowed on the message router.
Max # Remote Bridge Subscriptions	The maximum number of remote bridge subscriptions allowed on the message router.
Redundancy Config Status	The status of the redundancy configuration.
Redundancy Status	The status of the redundant message router.
Redundancy Mode	Refer to Solace documentation for more information.
Auto-revert	Refer to Solace documentation for more information.
Mate Router Name	If redundancy is configured, this field lists the redundant router name (mate router name).

ADB Link Up	This check box is checked if a message router is set up to use guaranteed messaging and an Assured Delivery Blade (ADB) is set up and working correctly.
ADB Hello Up	Refer to Solace documentation for more information.
Pair Primary Status	The primary status of the message router and its redundant (failover) mate.
Pair Backup Status	Refer to Solace documentation for more information.

Expired	When checked, performance data about the message router has not been received within the time specified (in seconds) in the **$solRowExpirationTime** field in the **conf\rtvapm_solmon.properties** file. The **$solRowExpirationTimeForDelete** field allows you to define the amount of time (in seconds) in which the row will be removed from the table if there is no response from the message router. To view/edit the current values, modify the following lines in the **.properties** file:
	`# Metrics data are considered expired after this number of seconds`
	`#`
	`collector.sl.rtview.sub=$solRowExpirationTime:45`
	`collector.sl.rtview.sub=$solRowExpirationTimeForDelete:3600`
	
	In the example above, the **Expired** check box would be checked after 45 seconds, and the row would be removed from the table after 3600 seconds.

Time Stamp	The date and time the row data was last updated.

Message Router Summary

This display shows current and historical performance metrics for a single message router. You can view the total number of clients that are connected, number of incoming flows, current **Up Time**, and additional information specific to a message router. You can also view alert statuses for the message router and any associated **VPNs**/**Endpoints**/**Bridges**/**Clients**, total number of **Connections/Destinations**, **Incoming**/**Outgoing**/**Pending** messages data, and **Spool Status** data for the message router.

Data Quality Indicators:

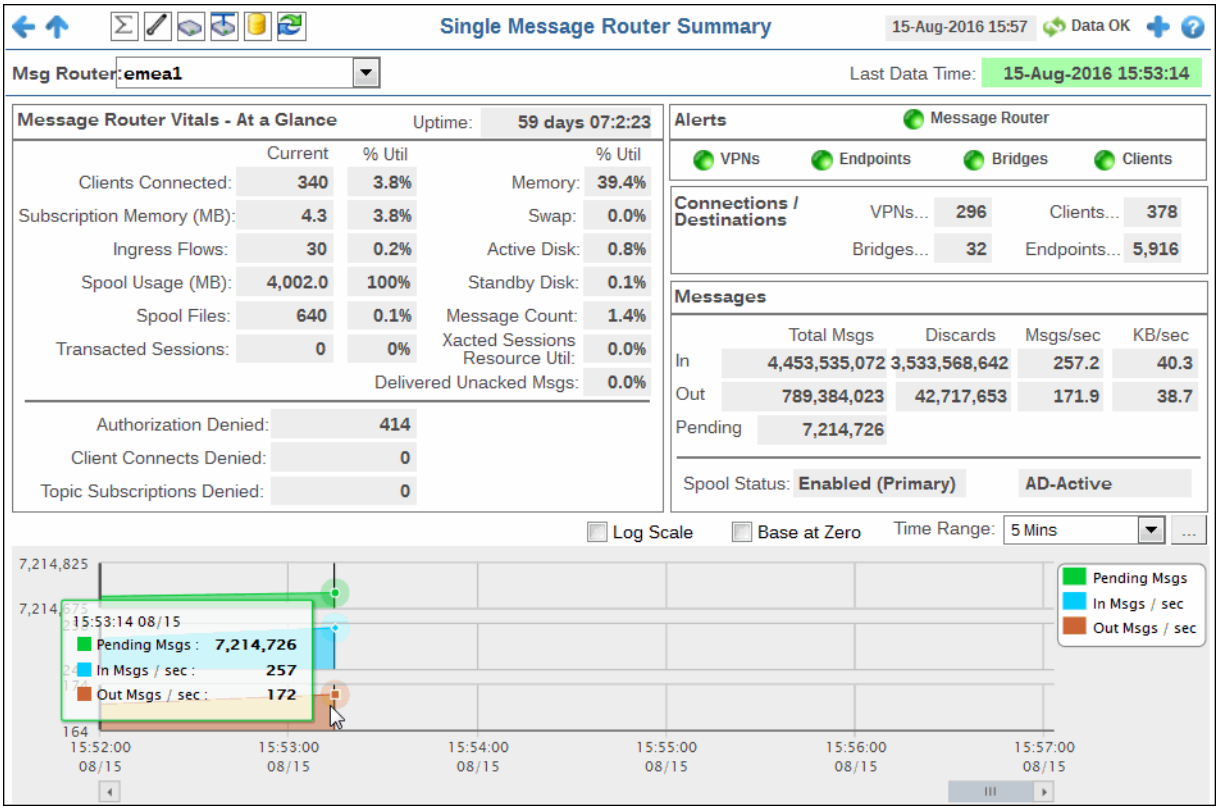
- When the display background color is (Red) the data is stale.
- The Last Data Time shows the date and time the selected message router was last updated.

If the **Last Data Time** background is:

(Red) the selected message router is offline or expired.

(Green) the selected message router is connected and receiving data.

This display also includes a trend graph containing the current and historical incoming, outgoing, and pending message data.



Title Bar: Indicators and functionality might include the following:

Open the previous and upper display.

Table Navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

Note: The upper icons ( ) also open displays within the **Message Routers** View.

Filter By:
The display might include these filtering options:

Msg Router: Choose the message router for which you want to show data in the display.

Last Data Time

Last Data Time: 15-Aug-2016 14:34:00

The date and time the selected message router was last updated.

Red indicates the selected message router is offline or expired.

Green indicates the selected message router is connected and receiving data.

Fields and Data:

Message Router Vitals - At a Glance

Uptime	The amount of time the message router has been up and running.
Clients Connected	The current number of clients connected and the percent utilization of the total number of available clients (current number of clients connected divided by the total number of available clients).
Subscription Memory (MB)	The current subscription memory used (in megabytes) and the percent utilization of the total amount of subscription memory available (current amount of subscription memory used divided by the total amount of available subscription memory).
Ingress Flows	The current number of incoming flows and the percent utilization of the total number of flows allowed (current number of incoming flows divided by the total number of flows allowed).
Spool Usage (MB)	The current spool usage (in megabytes) and the percent utilization of the total amount of available spool usage (current spool usage divided total available spool usage).
Spool Files	The current number of spool files and the percent utilization total number of spool files allowed (current number of spool files divided by the total number of spool files allowed).
Transacted Sessions	The current number of transacted sessions and the percent utilization total number of transacted sessions allowed (current number of transacted sessions divided by the total number of transacted sessions allowed).
Memory Used	The total percentage of memory used on the message router.
Swap Used	The total percentage of swap used on the message router.
Active Disk Used	The amount of active disk space used.
Stndby Disk Used	The amount of standby disk space used.
Msg Cnt Util	Refer to Solace documentation for more information.
Xacted Sessions Resource Util	Refer to Solace documentation for more information.
Delivered Unacked Msgs	The percentage of delivered messages that have not been acknowledged.
Authorization Denied	The number of failed authorization attempts.
Client Connects Denied	The number of attempted client connections that have been denied.
Topic Subscriptions Denied	The number of denied topic subscriptions.

Alerts
Indicates the severity level for the message router and its associated **VPNs**, **Endpoints**, **Bridges**, and **Clients**. Click on the alert indicator to drill down to the "All Message Routers Table" display, "All VPNs Table" display, "All Bridges" display, and "All Clients" display, respectively, to view current alerts for the selected application.

Values are:

- One or more alerts exceeded their ALARM LEVEL threshold.
- One or more alerts exceeded their WARNING LEVEL threshold.
- No alert thresholds have been exceeded.

Message Router	The current alert status for the message router.

VPNs	The current alert status for the VPNs associated with the message router.
Endpoints	The current alert status for the endpoints associated with the message router.
Bridges	The current alert status for the bridges associated with the message router.
Clients	The current alert status for the clients associated with the message router.

Connections/ Destinations

VPNs	The total number of VPNs connected to the message router.
Clients	The total number of client connections on the message router.
Bridges	The total number of defined VPN bridges on the message router.
Endpoints	The total number of endpoints defined on the message router.

Messages

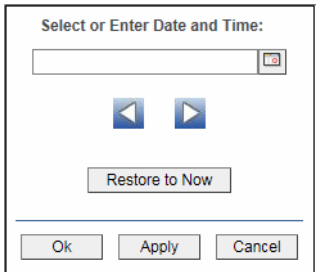
Total Msgs In	The total number of incoming messages on the message router.
Total Msgs Out	The total number of outgoing messages on the message router.
Total Msgs Pending	The total number of pending messages on the message router.
Discards In	The total number of incoming messages that were discarded.
Discards Out	The total number of outgoing messages that were discarded.
Msgs/sec In	The number of incoming messages per second.
Msgs/sec Out	The number of outgoing messages per second.
KB/sec In	The number of incoming kilobytes per second.
KB/sec out	The number of outgoing kilobytes per second.
Spool Status	The status of the message spool on the message router.
% Utilization	The percentage of the message spool that is currently being used.
Active Disk Usage (MB)	The current message spool usage in megabytes.

Trend Graphs
Traces the sum of process metrics across all processes in all slices of the selected message router.

Pending Msgs	Traces the number of currently pending messages.
In Msgs/ sec	Traces the number of incoming messages per second.
Out Msgs/ sec	Traces the number of outgoing messages per second.
Log Scale	Select to enable a logarithmic scale. Use **Log Scale** to see usage correlations for data with a wide range of values. For example, if a minority of your data is on a scale of tens, and a majority of your data is on a scale of thousands, the minority of your data is typically not visible in non-log scale graphs. **Log Scale** makes data on both scales visible by applying logarithmic values rather than actual values to the data.

Base at Zero Select to use zero (**0**) as the Y axis minimum for all graph traces.

Time Range Select a time range from the drop down menu varying from **2 Minutes** to **Last 7 Days**, or display **All Data**. To specify a time range, click Calendar ...



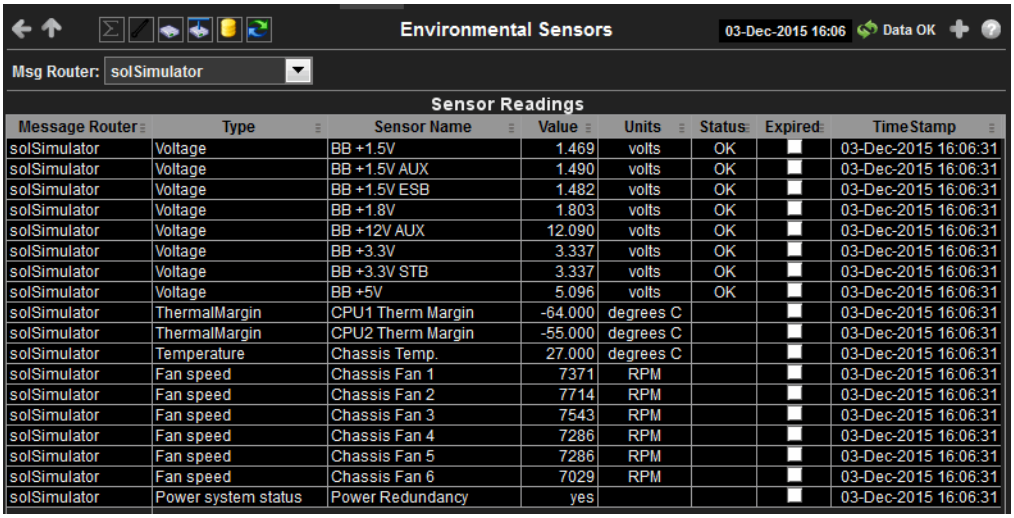
By default, the time range end point is the current time. To change the time range end point, click Calendar ... and select a date and time from the calendar or enter the date and time in the text field using the following format: **MMM dd, YYYY HH:MM**. For example, **Aug 21, 2011 12:24 PM**.

Use the navigation arrows to move forward or backward one time period. NOTE: The time period is determined by your selection from the **Time Range** drop-down menu.

Click **Restore to Now** to reset the time range end point to the current time.

Environmental Sensors

This tabular display contains sensor metrics for one message router. You can see the current sensor readings for all sensors on a particular message router. Use this display to find out the type, name, value, and status of the sensors.



Message Router	Type	Sensor Name	Value	Units	Status	Expired	TimeStamp
solSimulator	Voltage	BB +1.5V	1.469	volts	OK	☐	03-Dec-2015 16:06:31
solSimulator	Voltage	BB +1.5V AUX	1.490	volts	OK	☐	03-Dec-2015 16:06:31
solSimulator	Voltage	BB +1.5V ESB	1.482	volts	OK	☐	03-Dec-2015 16:06:31
solSimulator	Voltage	BB +1.8V	1.803	volts	OK	☐	03-Dec-2015 16:06:31
solSimulator	Voltage	BB +12V AUX	12.090	volts	OK	☐	03-Dec-2015 16:06:31
solSimulator	Voltage	BB +3.3V	3.337	volts	OK	☐	03-Dec-2015 16:06:31
solSimulator	Voltage	BB +3.3V STB	3.337	volts	OK	☐	03-Dec-2015 16:06:31
solSimulator	Voltage	BB +5V	5.096	volts	OK	☐	03-Dec-2015 16:06:31
solSimulator	ThermalMargin	CPU1 Therm Margin	-64.000	degrees C		☐	03-Dec-2015 16:06:31
solSimulator	ThermalMargin	CPU2 Therm Margin	-55.000	degrees C		☐	03-Dec-2015 16:06:31
solSimulator	Temperature	Chassis Temp.	27.000	degrees C		☐	03-Dec-2015 16:06:31
solSimulator	Fan speed	Chassis Fan 1	7371	RPM		☐	03-Dec-2015 16:06:31
solSimulator	Fan speed	Chassis Fan 2	7714	RPM		☐	03-Dec-2015 16:06:31
solSimulator	Fan speed	Chassis Fan 3	7543	RPM		☐	03-Dec-2015 16:06:31
solSimulator	Fan speed	Chassis Fan 4	7286	RPM		☐	03-Dec-2015 16:06:31
solSimulator	Fan speed	Chassis Fan 5	7286	RPM		☐	03-Dec-2015 16:06:31
solSimulator	Fan speed	Chassis Fan 6	7029	RPM		☐	03-Dec-2015 16:06:31
solSimulator	Power system status	Power Redundancy	yes			☐	03-Dec-2015 16:06:31

Title Bar: Indicators and functionality might include the following:

Open the previous and upper display.

Table Navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

Note: The upper icons ( ) also open displays within the **Message Routers** View.

Filter By:
The display might include these filtering options:

Msg Router:	Select the message router for which you want to show data in the display.

Fields and Data:

Message Router	Lists the selected message router.
Type	Lists the type of sensor.
Sensor Name	Lists the name of the sensor.
Value	Lists the value of the sensor.
Units	Lists the unit of measure for the sensor.
Status	The current status of the sensor.
Expired	When checked, performance data about the sensor has not been received within the time specified (in seconds) in the **$solRowExpirationTime** field in the **conf\rtvapm_solmon.properties** file. The **$solRowExpirationTimeForDelete** field allows you to define the amount of time (in seconds) in which the row will be removed from the table if there is no response from the sensor. To view/edit the current values, modify the following lines in the **.properties** file:

```
# Metrics data are considered expired after this number of seconds
#
collector.sl.rtview.sub=$solRowExpirationTime:45
collector.sl.rtview.sub=$solRowExpirationTimeForDelete:3600
```

In the example above, the **Expired** check box would be checked after 45 seconds, and the row would be removed from the table after 3600 seconds.

Time Stamp	The date and time the row data was last updated.

Message Router Provisioning

This display shows provisioning metrics for a single message router. Use this to see the host, platform, chassis, memory, redundancy and fabric data for a specific message router.

Data Quality Indicators:

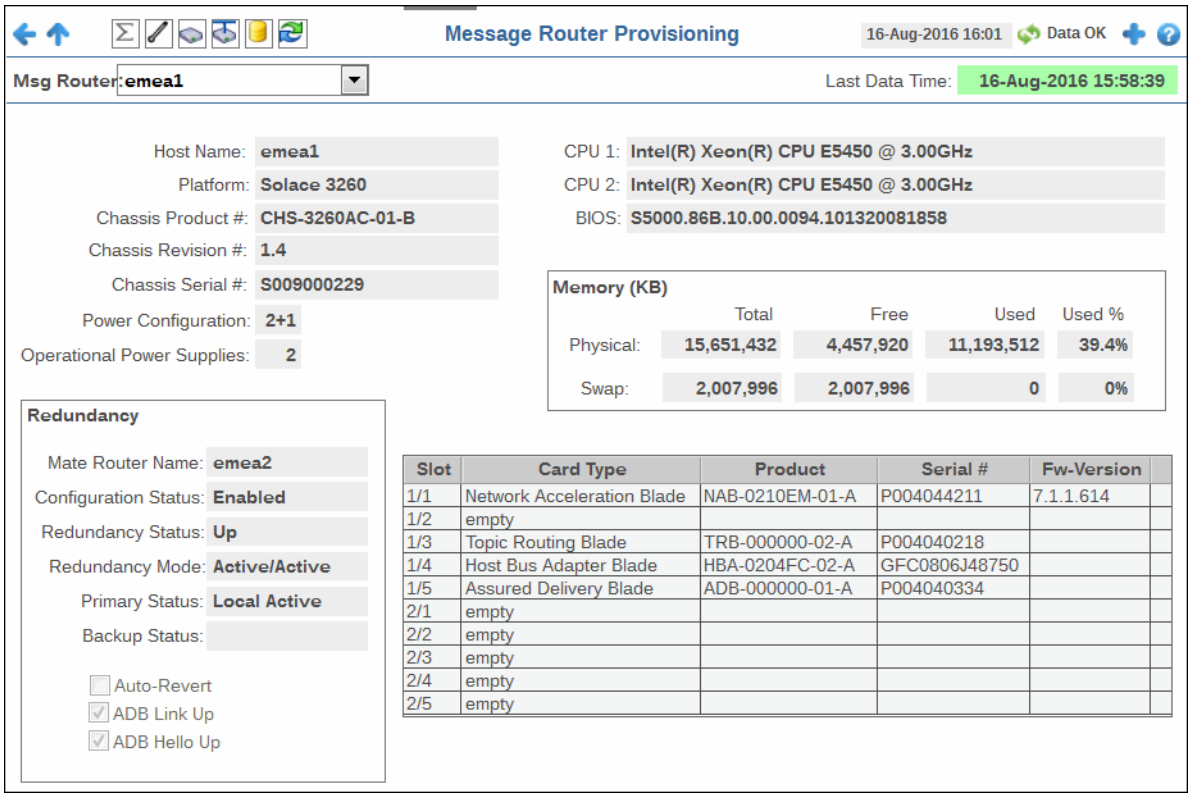
- When the display background color is (Red) the data is stale.
- The Last Data Time shows the date and time the selected message router was last updated.

Last Data Time: 15-Aug-2016 14:34:00

If the **Last Data Time** background is:

(Red) the selected message router is offline or expired.

(Green) the selected message router is connected and receiving data.



Title Bar: Indicators and functionality might include the following:

Open the previous and upper display.

Table Navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

Note: The upper icons ( ) also open displays within the **Message Routers** View.

Filter By:
The display might include these filtering options:

Msg Router: Select the message router for which you want to show data in the display.

Fields and Data:

Last Data Time

Last Data Time: **15-Aug-2016 14:34:00**

The date and time the selected message router was last updated.
Red indicates the selected message router is offline or expired.
Green indicates the selected message router is connected and receiving data.

Host Name The name of the host.

Platform The platform on which the message router is running.

Chassis Product # The product number of the chassis in which the router is contained.

Chassis Revision # The revision number of the chassis.

Chassis Serial # The serial number of the chassis.

Power Configuration The power configuration used by the chassis.

Operational Power Supplies The number of available power supplies that are operational on the chassis.

CPU 1 The name of the central processing unit (CPU 1) used by the message router.

CPU 2 The name of the central processing unit (CPU 2) used by the message router.

BIOS The basic input/output system used by the chassis.

Memory (KB)

Physical Lists the **Total** amount, the **Free** amount, the **Used** amount, and the **Used %** of physical memory.

Swap Lists the **Total** amount, the **Free** amount, the **Used** amount, and the **Used %** of swap memory.

Redundancy
These fields describe a fault tolerant pair of message routers.

Mate Router Name If redundancy is configured, this field lists the redundant router name (mate router name).

Configuration Status The status of the configuration for the backup message router.

Redundancy Status The status of the redundant message router.

Redundancy Mode Refer to Solace documentation for more information.

Primary Status The status of the primary message router.

Backup Status Refer to Solace documentation for more information.

Auto-Revert Refer to Solace documentation for more information.

ADB Link Up This check box is checked if a message router is set up to use guaranteed messaging and an Assured Delivery Blade (ADB) is set up and working correctly.

ADB Hello Up Refer to Solace documentation for more information.

Fabric

Slot	Displays the slot number on the network switch.
Card Type	The type of card connected to the particular slot.
Product	The product associated with the particular slot.
Serial #	The serial number of the product.
Fw-Version	The firmware version of the product.

Interface Summary

This display lists all network interfaces on a selected message router, the status of each network interface, as well as their throughput per second (bytes in/out and packets in/out).

Each row in the table is a different network interface. Click one to trace its current and historical performance data in the trend graph (bytes in/out and packets in/out per second).

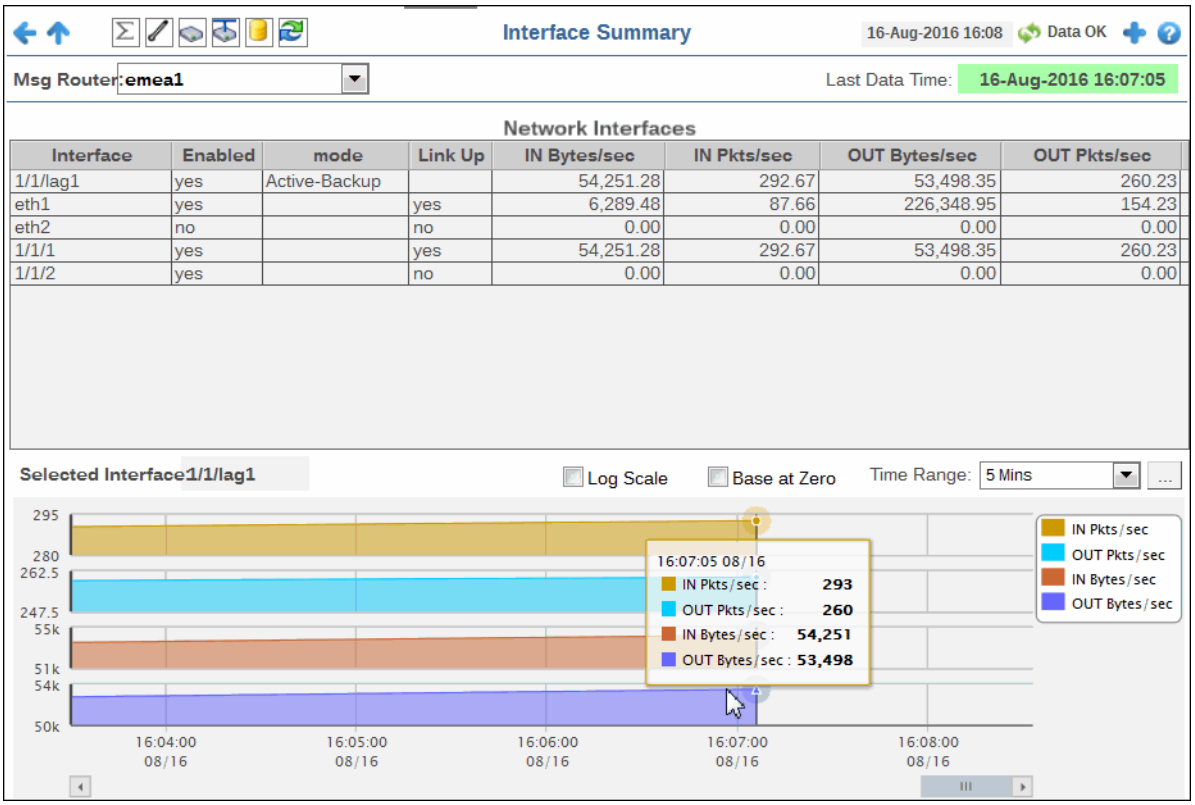
Interface Data Quality Indicators:

- When the display background color is (Red) the data for the selected network interface is stale.
- The Last Data Time shows the date and time the selected network interface was last updated.

If the **Last Data Time** background is:

(Red) the selected network interface is offline or expired.

(Green) the selected network interface is connected and receiving data



Title Bar: Indicators and functionality might include the following:

Open the previous and upper display.

Table Navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

Note: The upper icons ( ) also open displays within the **Message Routers** View.

Filter By:
The display might include these filtering options:

Message Router: Select the message router for which you want to show data in the display.

Fields and Data:

Last Data Time

Last Data Time: 15-Aug-2016 14:34:00

The date and time the selected network interface was last updated.

Red indicates the selected network interface is offline or expired.

Green indicates the selected network interface is connected and receiving data.

Interface The name of the network interface.

Enabled Displays whether or not the network interface is enabled.

mode Describes how the interface is configured to support networking operations.

Link Up Indicates whether the interface is electrically signaling on the transmission medium.

IN Bytes/sec The number of bytes per second contained in incoming messages.

IN Pkts/sec The number of incoming packets per second.

OUT Bytes/sec The number of bytes per second contained in the outgoing messages.

OUT Pkts/sec The number of outgoing packets per second.

Trend Graphs
Traces the sum of process metrics across all processes in all slices of the selected message router.

IN Pkts/sec Traces the number of incoming packets per second.

OUT Pkts/sec Traces the number of outgoing packets per second.

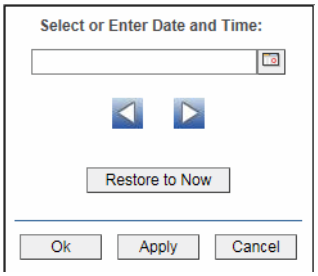
IN Bytes/sec Traces the number of bytes per second contained in the incoming messages.

OUT Bytes/sec Traces the number of bytes per second in the outgoing messages.

Log Scale Select to enable a logarithmic scale. Use **Log Scale** to see usage correlations for data with a wide range of values. For example, if a minority of your data is on a scale of tens, and a majority of your data is on a scale of thousands, the minority of your data is typically not visible in non-log scale graphs. **Log Scale** makes data on both scales visible by applying logarithmic values rather than actual values to the data.

Base at Zero Select to use zero (**0**) as the Y axis minimum for all graph traces.

Time Range Select a time range from the drop down menu varying from **2 Minutes** to **Last 7 Days**, or display **All Data**. To specify a time range, click Calendar ...



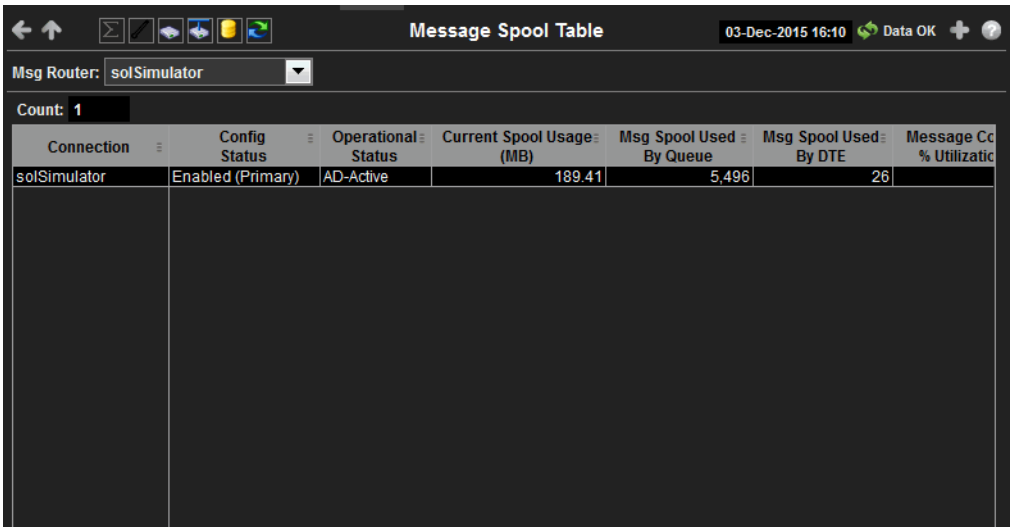
By default, the time range end point is the current time. To change the time range end point, click Calendar ... and select a date and time from the calendar or enter the date and time in the text field using the following format: **MMM dd, YYYY HH:MM**. For example, **Aug 21, 2011 12:24 PM**.

Use the navigation arrows to move forward or backward one time period. NOTE: The time period is determined by your selection from the **Time Range** drop-down menu.

Click **Restore to Now** to reset the time range end point to the current time.

Message Spool Table

This display shows operational status and message spool metrics (if spooling is enabled on the message router) for a selected message router. Refer to Solace documentation for details about data in this display.



Title Bar: Indicators and functionality might include the following:

Open the previous and upper display.

Table Navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

Note: The upper icons ( ) also open displays within the **Message Routers** View.

Filter By:
The display might include these filtering options:

Msg Router:	Select the message router for which you want to show data in the display.

Fields and Data:

Count	Lists the total number of message routers that are using spooling in the table.
Connection	The name of the message router.
Config Status	The status of the connection's configuration.
Operational Status	The operational status of the spool on the message router.
Current Spool Usage (MB)	The current amount of spool used in megabytes on the message router (calculated by summing spool used for each endpoint).
Msg Spool Used By Queue	The amount of spool used by the queue.

Msg Spool Used By DTE	The amount of spool used by DTE.
Message Count % Utilization	The percentage of total messages that use the message spool.
Delivered UnAcked Msgs % Utilization	The percentage of messages delivered via the spool that have not been acknowledged.
Ingress Flow Count	The current incoming flow count.
Ingress Flows Allowed	The total number of incoming flows allowed.
Queue/Topic Subscriptions Used	The number of queue/topic subscriptions used.
Max Queue/ Topic Subscriptions	The maximum number of queue/topic subscriptions available.
Sequenced Topics Used	The number of sequenced topics used.
Max Sequenced Topics	The maximum number of sequenced topics available.
Spool Files Used	The number of spool files used.
Spool Files Available	The maximum number of spool files available.
Spool Files % Utilization	The percentage of available spool files that have been used.
Active Disk Partition % Usage	The percentage of available active disk partition that has been used.
Standby Disk Partition % Usage	The percentage of available standby disk partition that has been used.
Disk Usage Current (MB)	The current amount of spool disk usage in megabytes.
Disk Usage Max (MB)	The maximum amount of available spool disk usage in megabytes.
Transacted Sessions Used	The current number of transacted sessions.
Transacted Sessions Max	The maximum number of transacted sessions allowed.
Transacted Session Count % Utilization	The percentage of allowable transacted sessions that have been used.

Transacted Session Resource % Utilization	The percentage of allowable transacted session resources that have been used.

Expired	When checked, performance data about the message router has not been received within the time specified (in seconds) in the **$solRowExpirationTime** field in the **conf\rtvapm_solmon.properties** file. The **$solRowExpirationTimeForDelete** field allows you to define the amount of time (in seconds) in which the row will be removed from the table if there is no response from the message router. To view/edit the current values, modify the following lines in the **.properties** file:
	`# Metrics data are considered expired after this number of seconds`
	`#`
	`collector.sl.rtview.sub=$solRowExpirationTime:45`
	`collector.sl.rtview.sub=$solRowExpirationTimeForDelete:3600`
	
	In the example above, the **Expired** check box would be checked after 45 seconds, and the row would be removed from the table after 3600 seconds.

Message Router VPN Activity

This display shows VPN activity metrics for a single message router. Choose a message router to see the number of client connections and the average in/out bytes per minute for each connected client. Use this display to compare metrics across VPNs.

Data Quality Indicators:

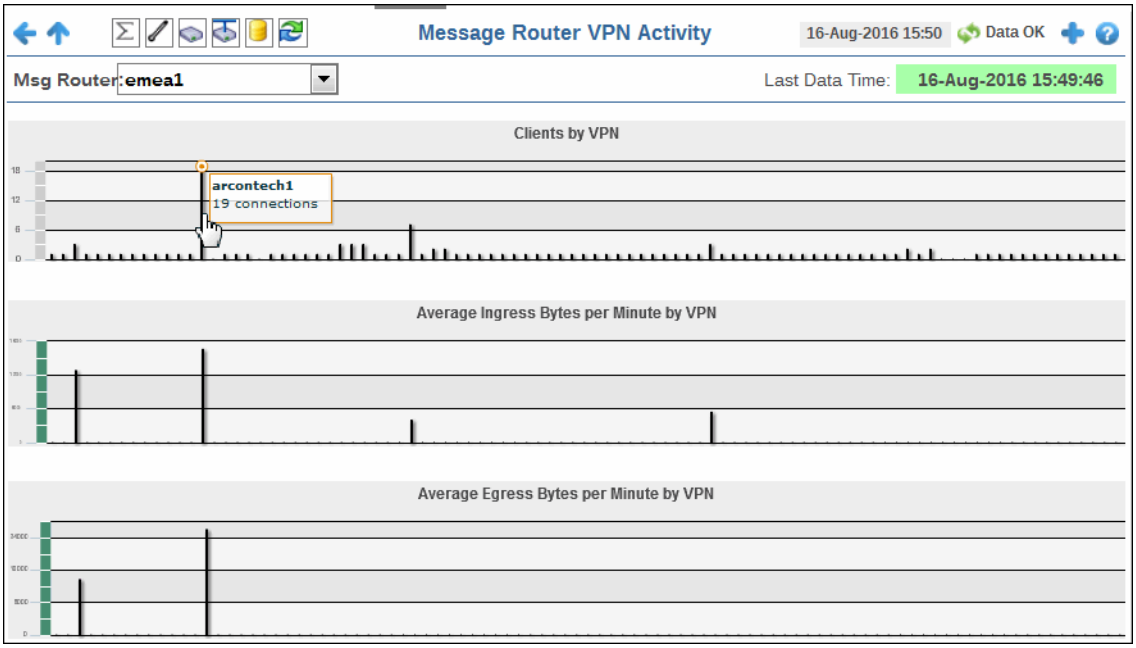
- When the display background color is (Red) the data is stale.
- The Last Data Time shows the date and time the selected message router was last updated.

If the **Last Data Time** background is:

(Red) the selected message router is offline or expired.

(Green) the selected message router is connected and receiving data.

Each column in the **Average Ingress Bytes per Minute** and **Average Egress Bytes per Minute** graphs refers to the same column in the **Client** graph. For example, the first column in the **Average Ingress Bytes per Minute** and **Average Egress Bytes per Minute** graphs refers to the first column in the **Clients** graph. You can hover over each of the graphs to view the exact number of connections and the average number of incoming and outgoing bytes for each client.



Title Bar: Indicators and functionality might include the following:

Open the previous and upper display.

Table Navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

Note: The upper icons ( ) also open displays within the **Message Routers** View.

Filter By:
The display might include these filtering options:

Msg Router: Select the message router for which you want to show data in the display.

Last Data Time

Last Data Time: 15-Aug-2016 14:34:00

The date and time the selected message router was last updated.

Red indicates the selected message router is offline or expired.

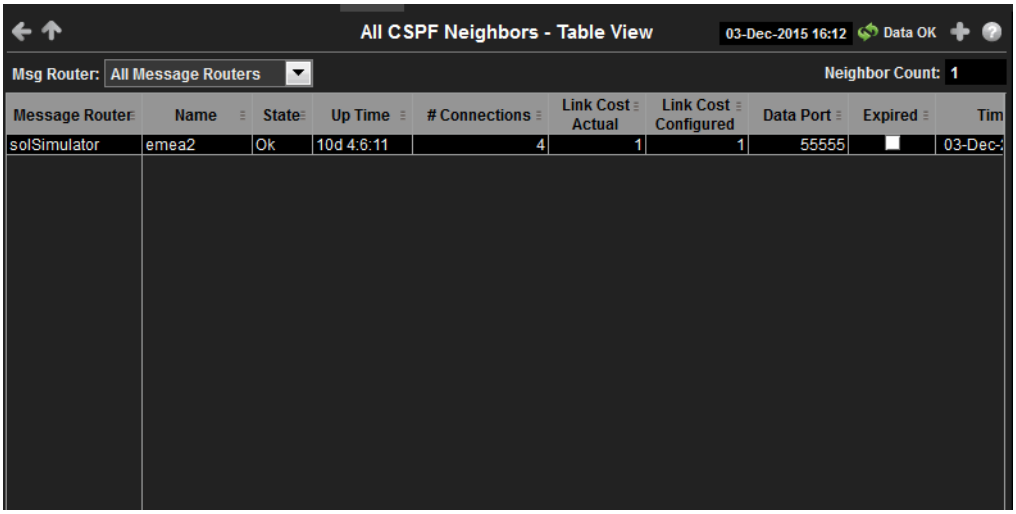
Green indicates the selected message router is connected and receiving data.

Fields and Data:

Clients	Lists the clients and the number of connections for each client for the selected message router. Hovering over each client in the graph displays the exact number of connections for the clients.
Average Ingress Bytes per Minute	Displays the average number of incoming bytes per minute for each of the clients in the message router. Hovering over each column in this graph provides the exact number of incoming bytes per minute for the associated client.
Average Egress Bytes per Minute	Displays the average number of outgoing bytes per minute for each of the clients in the message router. Hovering over each column in this graph provides the exact number of outgoing bytes per minute for the associated client.

CSPF Neighbors Table

This tabular display shows Content Shortest Path First (CSPF) “neighbor” metrics for a selected message router. View metrics for a Solace neighbor message router that uses the CSPF routing protocol to determine the least cost path in which to send messages from one message router to another message router in the Solace network.



Title Bar: Indicators and functionality might include the following:

Open the previous and upper display.

Table Navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

Filter By:
The display might include these filtering options:

Msg Router	Choose the message router for which you want to show data in the display.

Fields and Data:

Message Router	The name of the message router.
Name	The name of the “neighbor” message router.
State	The current state of the message router.
Up Time	The amount of time the message router has been up and running.
Connections	The number of connections.
Link Cost Actual	Refer to Solace documentation for more information.
Link Cost Configured	Refer to Solace documentation for more information.
Data Port	Refer to Solace documentation for more information.

Expired	When checked, performance data about the message router has not been received within the time specified (in seconds) in the **$solRowExpirationTime** field in the **conf\rtvapm_solmon.properties** file. The **$solRowExpirationTimeForDelete** field allows you to define the amount of time (in seconds) in which the row will be removed from the table if there is no response from the message router. To view/edit the current values, modify the following lines in the **.properties** file:
	`# Metrics data are considered expired after this number of seconds`
	`#`
	`collector.sl.rtview.sub=$solRowExpirationTime:45`
	`collector.sl.rtview.sub=$solRowExpirationTimeForDelete:3600`
	
	In the example above, the **Expired** check box would be checked after 45 seconds, and the row would be removed from the table after 3600 seconds.

Timestamp	The date and time the row data was last updated.

VPNs

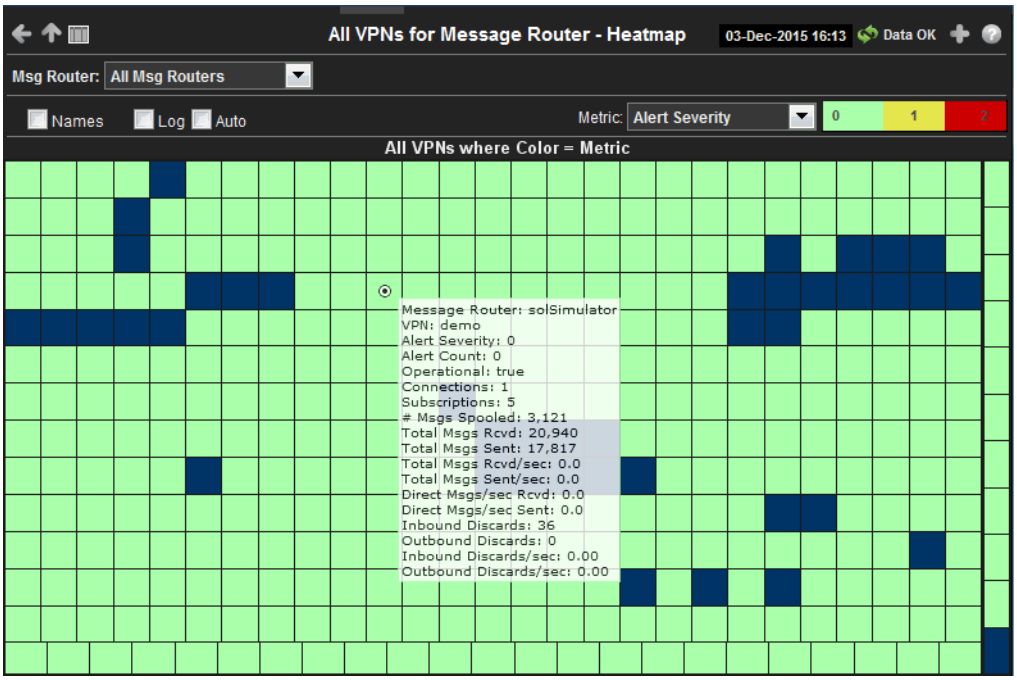
You can view data for all VPNs configured on a specific message router in heatmap, table, or grid formats, or you can view data for a single VPN. Displays in this View are:

- “All VPNs Heatmap” on page 59: A color-coded heatmap view of the current status of all VPNs configured on a specific message router.
- “All VPNs Table” on page 63: A tabular view of all available data for all VPNs configured on a specific router.
- “Top VPNs Grid” on page 67: Lists VPNs configured on a specific message router, in ascending or descending order, based on a selected metric.
- “Single VPN Summary” on page 69: Current and historical metrics for a single VPN.

All VPNs Heatmap

View the status of all VPNs configured on a specific message router in a heatmap format, which allows you to quickly identify VPNs with critical alerts. Each rectangle in the heatmap represents a VPN. The rectangle color indicates the alert state for each VPN.

Select a message router from the **Msg Router** drop-down menu and select a metric from the **Metric** drop-down menu. Use the **Names** check-box ☑ to include or exclude labels in the heatmap. By default, this display shows **Alert Severity**, but you can mouse over a rectangle to see additional metrics. Drill-down and investigate by clicking a rectangle in the heatmap to view details for the selected application in the "Single VPN Summary" display.



Title Bar: Indicators and functionality might include the following:

Open the previous and upper display.

Table Navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

Filter By:
The display might include these filtering options:

Msg Router Choose the message router for which you want to view data in the display.

Fields and Data:

Names Check the **Names** check box to include labels for each heatmap rectangle.

Log Select to enable a logarithmic scale. Use **Log Scale** to see usage correlations for data with a wide range of values. For example, if a minority of your data is on a scale of tens, and a majority of your data is on a scale of thousands, the minority of your data is typically not visible in non-log scale graphs. **Log Scale** makes data on both scales visible by applying logarithmic values rather than actual values to the data.

Auto Select to enable auto-scaling. When auto-scaling is activated, the color gradient bar's maximum range displays the highest value.

Note: Some metrics auto-scale automatically, even when **Auto** is not selected.

Metric Choose a metric to view in the display.

Alert Severity Visually displays the level at which the VPN has or has not exceeded its alarm level threshold. Values range from **0** - **2**, as indicated in the color gradient bar, where **2** is the highest Alert Severity:

Red indicates that one or more metrics exceeded their ALARM LEVEL threshold.

Yellow indicates that one or more metrics exceeded their WARNING LEVEL threshold.

Green indicates that no metrics have exceeded their alert thresholds.

Alert Count The total number of critical and warning alerts. The color gradient bar, populated by the current heatmap, shows the value/color mapping. The numerical values in the gradient bar range from **0** to the maximum count of alerts in the heatmap. The middle value in the gradient bar indicates the average alert count.

Connections The total number of connections. The color gradient bar, populated by the current heatmap, shows the value/color mapping. The numerical values in the gradient bar range from 0 to the defined alert threshold of **SolVpnConnectionCountHigh**. The middle value in the gradient bar indicates the middle value of the range.

When **Auto** is checked, the numeric values in the color gradient bar show the range of the data being displayed rather than the default values. The middle value changes accordingly to indicate the color of the middle value of the range.

Subscriptions The total number of subscriptions. The color gradient bar, populated by the current heatmap, shows the value/color mapping. The numerical values in the gradient bar range from 0 to the defined alert threshold of **SolVpnSubscriptionCountHigh**. The middle value in the gradient bar indicates the middle value of the range.

When **Auto** is checked, the numeric values in the color gradient bar show the range of the data being displayed rather than the default values. The middle value changes accordingly to indicate the color of the middle value of the range.

 # Msgs Spooled The total number of spooled messages. The color gradient bar, populated by the current heatmap, shows the value/color mapping. The numerical values in the gradient bar range from 0 to the defined alert threshold of **SolVpnEndpointSpoolUsageHigh**. The middle value in the gradient bar indicates the middle value of the range.

When **Auto** is checked, the numeric values in the color gradient bar show the range of the data being displayed rather than the default values. The middle value changes accordingly to indicate the color of the middle value of the range.

Total Msgs Rcvd The total number of received messages. The color gradient bar, populated by the current heatmap, shows the value/color mapping. The numerical values in the gradient bar range from **0** to the maximum count of messages received in the heatmap. The middle value in the gradient bar indicates the average count.

The **Auto** flag does not impact this metric.

Total Msgs Sent The total number of sent messages. The color gradient bar, populated by the current heatmap, shows the value/color mapping. The numerical values in the gradient bar range from **0** to the maximum count of messages sent in the heatmap. The middle value in the gradient bar indicates the average count.

The **Auto** flag does not impact this metric.

Total Msgs/ sec Rcvd

The number of messages received per second. The color gradient bar, populated by the current heatmap, shows the value/ color mapping. The numerical values in the gradient bar range from 0 to the defined alert threshold of **SolVpnInboundMsgRateHigh**. The middle value in the gradient bar indicates the middle value of the range.

When **Auto** is checked, the numeric values in the color gradient bar show the range of the data being displayed rather than the default values. The middle value changes accordingly to indicate the color of the middle value of the range.

Total Msgs/ sec Sent

The number of messages sent per second. The color gradient bar, populated by the current heatmap, shows the value/ color mapping. The numerical values in the gradient bar range from 0 to the defined alert threshold of **SolVpnOutboundMsgRateHigh**. The middle value in the gradient bar indicates the middle value of the range.

When **Auto** is checked, the numeric values in the color gradient bar show the range of the data being displayed rather than the default values. The middle value changes accordingly to indicate the color of the middle value of the range.

Total Bytes/ sec Rcvd

The number of bytes contained in messages received per second. The color gradient bar, populated by the current heatmap, shows the value/color mapping. The numerical values in the gradient bar range from 0 to the defined alert threshold of **SolVpnInboundByteRateHigh**. The middle value in the gradient bar indicates the middle value of the range.

When **Auto** is checked, the numeric values in the color gradient bar show the range of the data being displayed rather than the default values. The middle value changes accordingly to indicate the color of the middle value of the range.

Total Bytes/ sec Sent

The number of bytes contained in direct messages sent per second. The color gradient bar, populated by the current heatmap, shows the value/color mapping. The numerical values in the gradient bar range from 0 to the defined alert threshold of **SolMsgRouterOutboundByteRateHigh**. The middle value in the gradient bar indicates the middle value of the range.

When **Auto** is checked, the numeric values in the color gradient bar show the range of the data being displayed rather than the default values. The middle value changes accordingly to indicate the color of the middle value of the range.

Direct Msgs/ sec Rcvd

The number of direct messages received per second. The color gradient bar, populated by the current heatmap, shows the value/color mapping. The numerical values in the gradient bar range from **0** to the average number of direct messages received per second in the heatmap. The middle value in the gradient bar indicates the average count.

The **Auto** flag does not impact this metric.

Direct Msgs/ sec Sent

The number of direct messages sent per second in the heatmap rectangle. The color gradient bar, populated by the current heatmap, shows the value/color mapping. The numerical values in the gradient bar range from **0** to the average number of direct messages sent per second in the heatmap. The middle value in the gradient bar indicates the average count.

The **Auto** flag does not impact this metric.

Total Inbound Discards

The total number of discarded inbound messages in the heatmap rectangle. The color gradient bar, populated by the current heatmap, shows the value/color mapping. The numerical values in the gradient bar range from **0** to the maximum count of discarded inbound messages in the heatmap. The middle value in the gradient bar indicates the average count.

The **Auto** flag does not impact this metric.

Total Outbound Discards

The total number of discarded outbound messages in the heatmap rectangle. The color gradient bar, populated by the current heatmap, shows the value/color mapping. The numerical values in the gradient bar range from **0** to the maximum count of discarded outbound messages in the heatmap. The middle value in the gradient bar indicates the average count.

The **Auto** flag does not impact this metric.

Inbound Discard Rate

The number of discarded inbound messages per second in the heatmap rectangle. The color gradient bar, populated by the current heatmap, shows the value/color mapping. The numerical values in the gradient bar range from 0 to the defined alert threshold of **SolVpnInboundDiscardRateHigh**. The middle value in the gradient bar indicates the middle value of the range.

When **Auto** is checked, the numeric values in the color gradient bar show the range of the data being displayed rather than the default values. The middle value changes accordingly to indicate the color of the middle value of the range.

Outbound Discard Rate

The number of discarded outbound messages per second in the heatmap rectangle. The color gradient bar, populated by the current heatmap, shows the value/color mapping. The numerical values in the gradient bar range from 0 to the defined alert threshold of **SolVpnOutboundDiscardRateHigh**. The middle value in the gradient bar indicates the middle value of the range.

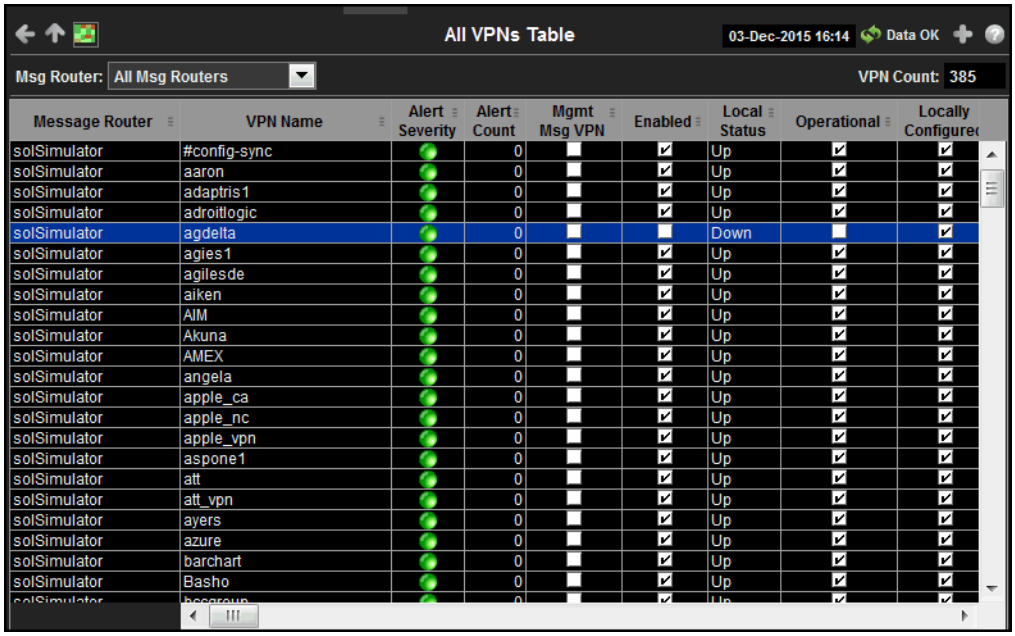
When **Auto** is checked, the numeric values in the color gradient bar show the range of the data being displayed rather than the default values. The middle value changes accordingly to indicate the color of the middle value of the range.

All VPNs Table

View data shown in the "All VPNs Heatmap" display, as well as additional details, in a tabular format. Use this display to view all available data for each VPN associated with a specific message router.

Choose a message router from the **Msg Router** drop-down menu to view a list of all associated VPNs. Click a column header to sort column data in numerical or alphabetical order.

Drill-down and investigate by clicking a row to view details for the selected VPN in the "Single VPN Summary" display.



Title Bar: Indicators and functionality might include the following:

Open the previous and upper display.

Table Navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

Filter By:
The display might include these filtering options:

Msg Router: Choose the message router for which you want view data in the display.

Fields and Data:

VPN Count: The total number of VPNs (rows) in the table.

Table:
Column values describe the message router and its associated VPN.

Message Router The name of the message router.

VPN Name The name of the VPN.

Alert Severity	The maximum level of alerts in the row. Values range from **0** - **2**, as indicated in the color gradient bar, where **2** is the highest Alert Severity: Red indicates that one or more metrics exceeded their ALARM LEVEL threshold. Yellow indicates that one or more metrics exceeded their WARNING LEVEL threshold. Green indicates that no metrics have exceeded their alert thresholds.
Alert Count	The total number of active alerts for the AppNode.
Is Mgmt Msg VPN	When checked, the VPN is used by the message router for management purposes.
Enabled	When checked, the VPN was enabled via the command line interface or via SolAdmin.
Local Status	Displays the status of the VPN.
Operational	When checked, this status indicates that the VPN is enabled and is operating normally.
Locally Configured	When checked, this status indicates that the VPN was configured locally using SolAdmin or the command line interface.
Dist Cache Mgmt Enabled	Refer to Solace documentation for more information.
Export Subscriptions	When checked, the export subscriptions policy allows subscriptions added locally to Message VPN to be advertised to the other message routers in the network.
Pending Messages	The current number of pending messages in the VPN.
# Connections	The total number of message routers connected to the VPN.
Total Unique Subscriptions	The total number of unique subscriptions to the VPN.
Total Client Messages Rcvd	The total number of messages received from clients connected to the VPN.
Total Client Messages Sent	The total number of messages sent to clients connected to the VPN.
Total Client Bytes Rcvd	The total number of bytes contained in messages received from clients connected to the VPN.
Total Client Bytes Sent	The total number of bytes contained in messages sent to clients connected to the VPN.
Total Client Msgs/sec Rcvd	The total number of messages received per second from clients connected to the VPN.
Total Client Msgs /sec Sent	The total number of messages sent per second to clients connected to the VPN.
Total Client Bytes/sec Rcvd	The total number of bytes contained in messages received per second from clients connected to the VPN.
Total Client Bytes/sec Sent	The total number of bytes contained in messages sent per second to clients connected to the VPN.
Client Direct Msgs Rcvd	The total number of direct messages received from clients connected to the VPN.
Client Direct Msgs Sent	The total number of direct messages sent to clients connected to the VPN.

Client Direct Bytes Rcvd	The total number of bytes contained in direct messages received from clients connected to the VPN.
Client Direct Bytes Sent	The total number of bytes contained in direct messages sent to clients connected to the VPN.
Client Direct Msgs/sec Rcvd	The total number of direct messages received per second from clients connected to the VPN.
Client Direct Msgs/sec Sent	The total number of direct messages sent per second to clients connected to the VPN.
Client Direct Bytes/sec Rcvd	The total number of bytes contained in the direct messages received per second from clients connected to the VPN.
Client Direct Bytes/sec Sent	The total number of bytes contained in the direct messages sent per second to clients connected to the VPN.
Client NonPersistent Msgs Rcvd	The total number of non-persistent messages received from clients connected to the VPN.
Client NonPersistent Msgs Sent	The total number of non-persistent messages sent to clients connected to the VPN.
Client NonPersistent Bytes Rcvd	The total number of bytes contained in the non-persistent messages received from clients connected to the VPN.
Client NonPersistent Bytes Sent	The total number of bytes contained in the non-persistent messages sent per second to clients connected to the VPN.
Client NonPersistant Msgs/sec Rcvd	The total number of non-persistent messages received per second from clients connected to the VPN.
Client NonPersistent Msgs/sec Sent	The total number of non-persistent messages sent per second to clients connected to the VPN.
Client NonPersistant Bytes/sec Rcvd	The total number of bytes contained in the non-persistent messages received per second from clients connected to the VPN.
Client NonPersistent Bytes/sec Sent	The total number of bytes contained in the non-persistent messages sent per second to clients connected to the VPN.
Client Persistent Msgs Rcvd	The total number of persistent messages received from clients connected to the VPN.
Client Persistent Msgs Sent	The total number of persistent messages sent to clients connected to the VPN.
Client Persistent Bytes Rcvd	The total number of bytes contained in persistent messages received from clients connected to the VPN.
Client Persistent Bytes Sent	The total number of bytes contained in persistent messages sent to clients connected to the VPN.

Client Persistent Msgs/sec Rcvd	The total number of persistent messages received per second from clients connected to the VPN.
Client Persistent Msgs/sec Sent	The total number of persistent messages sent per second to clients connected to the VPN.
Client Persistent Bytes/sec Rcvd	The total number of bytes contained in the persistent messages received per second from clients connected to the VPN.
Client Persistent Bytes/sec Sent	The total number of bytes contained in the persistent messages sent per second to clients connected to the VPN.
Total In Discards	The total number of discarded incoming messages.
Total In Discards/sec	The number of discarded incoming messages per second.
Total Out Discards	The total number of discarded outgoing messages.
Total Out Discards/sec	The number of discarded outgoing messages per second.
Max Spool Usage (MB)	The maximum amount of disk storage (in megabytes) that can be consumed by all spooled message on the VPN.
Authentication Type	The defined authentication type on the VPN.

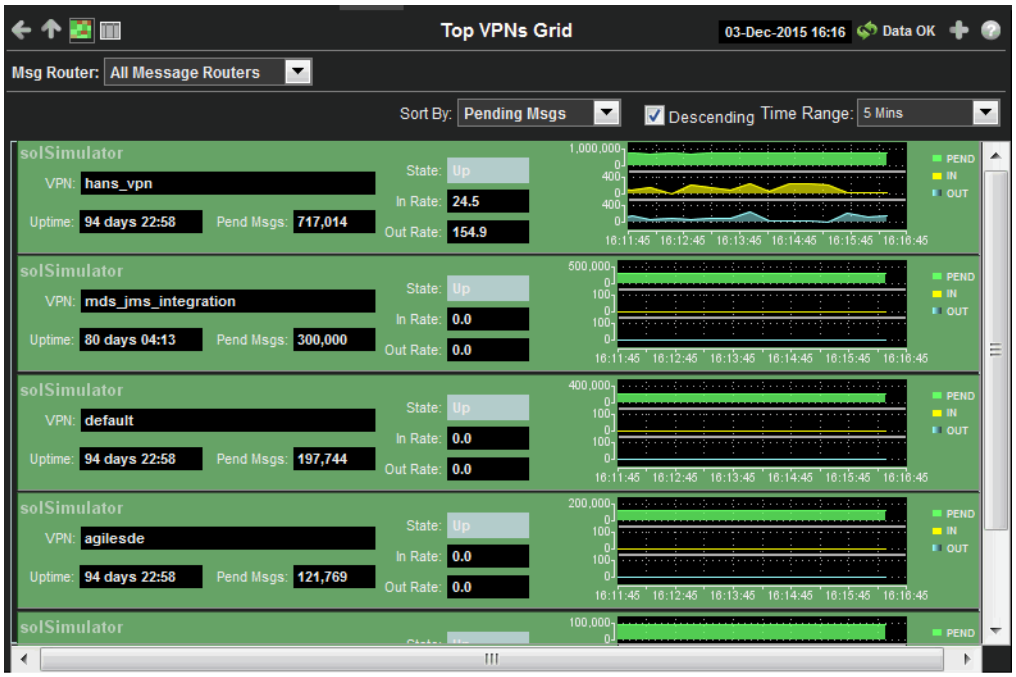
Expired	When checked, performance data about the VPN has not been received within the time specified (in seconds) in the **$solRowExpirationTime** field in the **conf\rtvapm_solmon.properties** file. The **$solRowExpirationTimeForDelete** field allows you to define the amount of time (in seconds) in which the row will be removed from the table if there is no response from the VPN. To view/edit the current values, modify the following lines in the **.properties** file:
	`# Metrics data are considered expired after this number of seconds`
	`#`
	`collector.sl.rtview.sub=$solRowExpirationTime:45`
	`collector.sl.rtview.sub=$solRowExpirationTimeForDelete:3600`
	
	In the example above, the **Expired** check box would be checked after 45 seconds, and the row would be removed from the table after 3600 seconds.

Time Stamp	The date and time the row data was last updated.

Top VPNs Grid

View the VPNs in ascending or descending order based on the number of pending messages, the number of incoming messages per second, or the number of outgoing messages per second.

Drill-down and investigate by clicking a row to view details for the selected VPN in the "Single VPN Summary" display.



Title Bar: Indicators and functionality might include the following:

Open the previous and upper display.

Table Navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

Filter By / Sort By:
The display includes these filtering/sorting options:

Msg Router: Choose the message router for which you want view data in the display.

Sort By: Select how you want to sort the data. You can select from **Pending Msgs**, **Msgs IN / sec**, and **Msgs OUT / sec**.

Descending: Select this check box to view the data in descending order based on the option selected in the **Sort By** drop down list. For example, select **Pending Msgs** in the **Sort By** drop down and select this toggle to view the VPNs (for the selected message router) with the most pending messages at the top of the display. Deselect this toggle to view the data in ascending order (for example, VPNs with the least pending messages at the top of the display).

Time Range: Select the length of time for which you want to view past data in the trend graphs. You can select from the last **2 Mins** up to the last **7 Days**, or you can view **All Data**.

Fields and Data:

VPN Displays the name of the VPN.

Uptime	Displays the length of time the VPN has been up and running.
Pend Msgs	Displays the number of pending messages for the VPN.
State	Displays the current status of the VPN.
In Rate	Displays the current Incoming Message Rate (per second) for the VPN.
Out Rate	Displays the current Outgoing Message Rate (per second) for the VPN.
Trend Graph	Displays, in graph form, the Pending Messages, In Message Rate/sec, and Out Message Rate/sec based on the selected **Time Range**. For example, if **20 Mins** was selected in the **Time Range** drop down, the graph displays the total pending messages (**Pend**), the incoming message rates (**IN**), and the outgoing message rates (**OUT**) over the last 20 minutes.

Single VPN Summary

View alert, connection/destination, incoming message, outgoing message, and pending message information for a VPN.

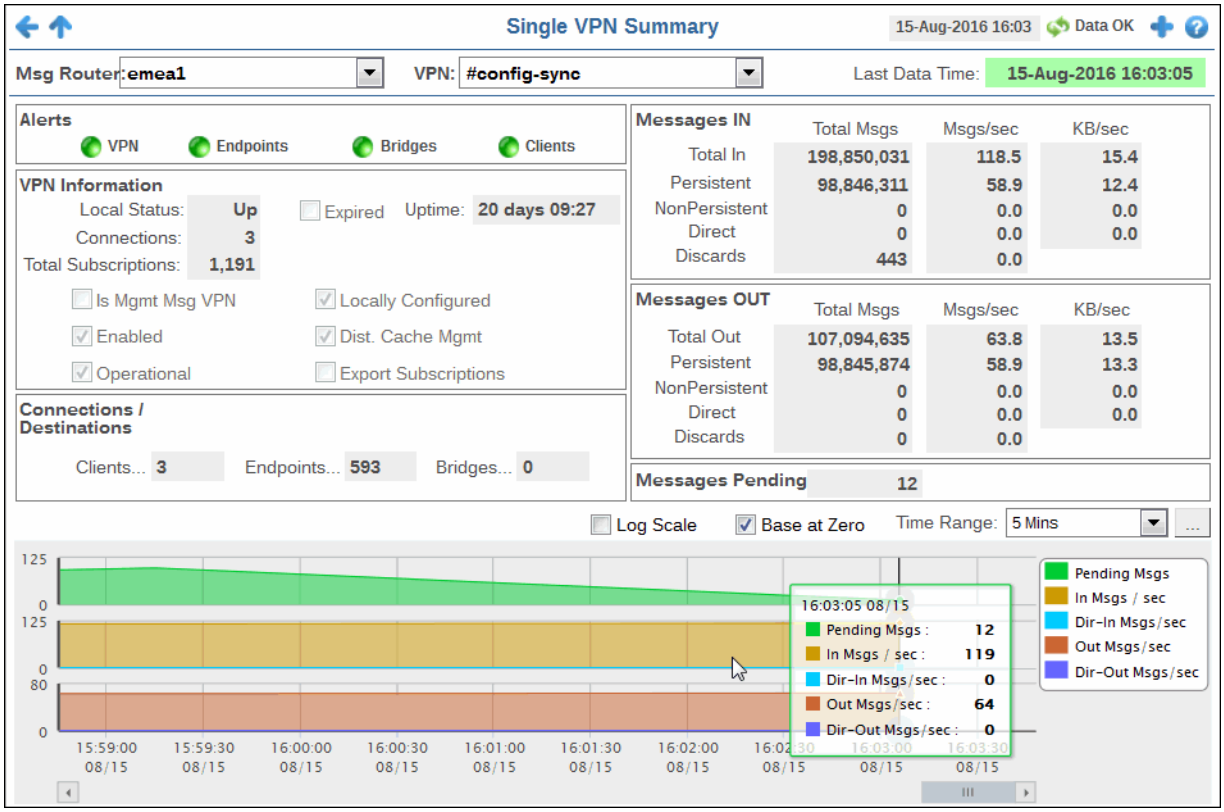
Data Quality Indicators:

- When the display background color is (Red) the data is stale.
- The Last Data Time shows the date and time the selected message router was last updated.

If the **Last Data Time** background is:

(Red) the selected message router is offline or expired.

(Green) the selected message router is connected and receiving data.



Title Bar: Indicators and functionality might include the following:

Open the previous and upper display.

Table Navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

Filter By:
The display might include these filtering options:

Msg Router: Choose the message router for which you want to view data.

VPN Choose the VPN associated with the selected message router for which you want to view data.

Last Data Time

Last Data Time: 15-Aug-2016 14:34:00

The date and time the selected message router was last updated.

Red indicates the selected message router is offline or expired.

Green indicates the selected message router is connected and receiving data.

Fields and Data:

Alerts

Red indicates that one or more metrics exceeded their ALARM LEVEL threshold.

Yellow indicates that one or more metrics exceeded their WARNING LEVEL threshold.

Green indicates that no metrics have exceeded their alert thresholds.

VPN	The current alert status for the VPN.
Endpoints	The current alert status for the endpoints associated with the VPN.
Bridges	The current alert status for the bridges associated with the VPN.
Clients	The current alert status for the clients associated with the VPN.

VPN Information

Local Status	The current status of the VPN.
Connections	The total number of connections for the VPN.
Total Subscriptions	The total number of subscriptions to the VPN.

Expired	When checked, performance data about the VPN has not been received within the time specified (in seconds) in the **$solRowExpirationTime** field in the **conf\rtvapm_solmon.properties** file. The **$solRowExpirationTimeForDelete** field allows you to define the amount of time (in seconds) in which the row will be removed from the table if there is no response from the VPN. To view/edit the current values, modify the following lines in the **.properties** file:
	`# Metrics data are considered expired after this number of seconds`
	`#`
	`collector.sl.rtview.sub=$solRowExpirationTime:45`
	`collector.sl.rtview.sub=$solRowExpirationTimeForDelete:3600`
	
	In the example above, the **Expired** check box would be checked after 45 seconds, and the row would be removed from the table after 3600 seconds.

Uptime	If the VPN's **Local Status** is **Up**, this field displays the length of time that the VPN has been up and running.
Is Mgmt Msg VPN	Displays whether or not the VPN is used by the message router for management purposes.
Enabled	When checked, the VPN was enabled via the command line interface or SolAdmin.
Operational	When checked, this status indicates that the VPN has been enabled and is operating normally.
Locally Configured	When checked, the VPN was configured locally using the command line interface or SolAdmin. If unchecked, the VPN received configuration instructions from another message router.
Dist. Cache Mgmt	Refer to Solace documentation for more information.
Export Subscriptions	When checked, the export subscriptions policy allows subscriptions added locally to the Message VPN to be advertised to the other message routers in the network.

Connections / Destinations

Clients	The total number of connected clients.
Endpoints	The total number of endpoints.

	Bridges	The total number of bridges connected to the VPN.
Messages IN		
	Total In	Displays the total incoming messages (**Total Msgs**), the total incoming message rate (**Msgs/sec**), and the total incoming kilobytes per second (**KB/sec**).
	Persistent	Displays the total number of incoming persistent messages (**Total Msgs**), the incoming persistent message rate (**Msgs/sec**), and the total incoming kilobytes per second (**KB/sec**) for the persistent messages.
	NonPersistent	Displays the total number of incoming non-persistent messages (**Total Msgs**), the incoming non-persistent message rate (**Msgs/sec**), and the total incoming kilobytes per second (**KB/sec**) for the non-persistent messages.
	Direct	Displays the total number of incoming direct messages (**Total Msgs**), the incoming direct message rate (**Msgs/sec**), and the total incoming kilobytes per second (**KB/sec**) for the direct messages.
	Discards	Displays the total number of incoming messages (**Total Msgs**) that were discarded, the incoming message rate (**Msgs/sec**) for the discarded messages, and the total kilobytes per second (**KB/sec**) of discarded incoming messages.
Messages OUT		
	Total In	Displays the total outgoing messages (**Total Msgs**), the total outgoing message rate (**Msgs/sec**), and the total outgoing kilobytes per second (**KB/sec**).
	Persistent	Displays the total number of outgoing persistent messages (**Total Msgs**), the outgoing persistent message rate (**Msgs/sec**), and the total outgoing kilobytes per second (**KB/sec**) for the persistent messages.
	NonPersistent	Displays the total number of outgoing non-persistent messages (**Total Msgs**), the outgoing non-persistent message rate (**Msgs/sec**), and the total outgoing kilobytes per second (**KB/sec**) for the non-persistent messages.
	Direct	Displays the total number of outgoing direct messages (**Total Msgs**), the outgoing direct message rate (**Msgs/sec**), and the total outgoing kilobytes per second (**KB/sec**) for the direct messages.
	Discards	Displays the total number of outgoing messages (**Total Msgs**) that were discarded, the outgoing message rate (**Msgs/sec**) for the discarded messages, and the total kilobytes per second (**KB/sec**) of discarded outgoing messages.
Messages Pending	The total number of pending messages for the VPN.	

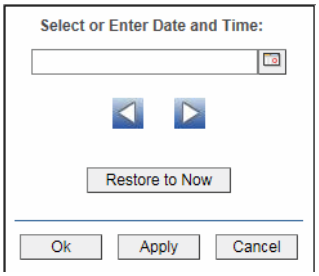
Trend Graphs
Traces the sum of process metrics for the VPN associated with the selected message router.

- **Pending Msgs**: The number of pending messages for the VPN.
- **In Msgs/sec**: The rate of incoming messages (per second) into the VPN.
- **Dir-In Msgs/sec**: The rate of direct incoming messages (per second) into the VPN.
- **Out Msgs/sec**: The rate of outgoing messages (per second) from the VPN.
- **Dir-Our Msgs/sec**: The rate of direct outgoing messages (per second) from the VPN.

Log Scale Select to enable a logarithmic scale. Use **Log Scale** to see usage correlations for data with a wide range of values. For example, if a minority of your data is on a scale of tens, and a majority of your data is on a scale of thousands, the minority of your data is typically not visible in non-log scale graphs. **Log Scale** makes data on both scales visible by applying logarithmic values rather than actual values to the data.

Base at Zero Select to use zero (**0**) as the Y axis minimum for all graph traces.

Time Range Select a time range from the drop down menu varying from **2 Minutes** to **Last 7 Days**, or display **All Data**. To specify a time range, click Calendar ...



By default, the time range end point is the current time. To change the time range end point, click Calendar ... and select a date and time from the calendar or enter the date and time in the text field using the following format: **MMM dd, YYYY HH:MM**. For example, **Aug 21, 2011 12:24 PM**.

Use the navigation arrows to move forward or backward one time period. NOTE: The time period is determined by your selection from the **Time Range** drop-down menu.

Click **Restore to Now** to reset the time range end point to the current time.

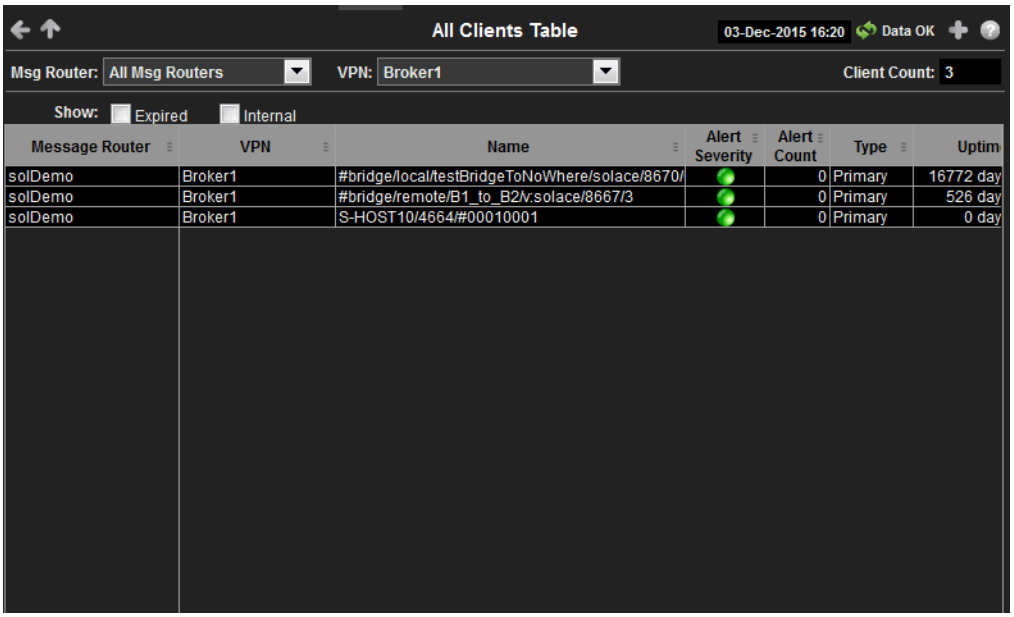
Clients

These displays allow you to view the current and historical metrics for clients configured on a VPN.Displays in this View are:

- "All Clients" on page 74: A color-coded heatmap view of data for all clients configured on a VPN.
- "Single Client Summary" on page 79: This display allows you to view the current and historical metrics for a single client configured on a VPN in a table format.

All Clients

This display allows you to view data for all clients configured on a VPN. Select the **Show: Expired** check box to include clients in the table that have been marked as expired because polls of the message router for client status data have not refreshed the data for the specific client ID. Select the **Internal** check box to include processes that run on the message router under the Solace OS. You can drill-down and view the details in the "Single Client Summary" display for a specific client by clicking on a row in the resulting table.



Title Bar: Indicators and functionality might include the following:

Open the previous and upper display.

Table Navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

Filter By:
The display includes these filtering options:

Msg Router:	Choose the message router for which you want to view data.
VPN:	Select the VPN associated with the message router for which you want to view data.
Client Count	The number of clients listed in the display.
Show: Expired	Select to display client connections to the message router that are not currently active.
Show: Internal	Select to display processes that run on the message router under the Solace OS.

Fields and Data:

Message Router	Lists the name of the selected message router.
VPN	Lists the name of the selected VPN.
Name	The name of the client.
Alert Severity	The maximum level of alerts in the row. Values range from **0** - **2**, as indicated in the color gradient bar, where **2** is the highest Alert Severity: Red indicates that one or more metrics exceeded their ALARM LEVEL threshold. Yellow indicates that one or more metrics exceeded their WARNING LEVEL threshold. Green indicates that no metrics have exceeded their alert thresholds.
Alert Count	Total number of alerts for the client.
Type	Lists the type of alert.
Uptime	Lists the amount of time the client has been up and running.
Client ID	Lists the client ID.
Client UserName	Lists the user name for the client.
Client Address	The IP Address of the client.
Profile	The client profile that is assigned to the client.
ACL Profile	The access control list profile to which the client is assigned.
Description	Lists a description of the client.
Platform	Lists the platform of the client.
Software Version	The version of the platform.
Slow Subscriber	This check box will be checked if the client consistently fails to consume their messages at the offered rate (which causes their egress queues to fill up).
Total Flows Out	The total number of outbound message flows for the client.
Total Flows In	The total number of inbound message flows for the client.
Bind Requests	The number of bind requests made by the client.
# Subscriptions	The number of subscribers connected to the client.
Add Sub Msgs Rcvd	The number of Add Subscription messages received.
Add Sub Msgs Sent	The number of Add Subscription Messages sent.
Already Exists Msgs Sent	Refer to Solace documentation for more information.
Assured Ctrl Msgs Rcvd	Refer to Solace documentation for more information.
Assured Ctrl Msgs Sent	Refer to Solace documentation for more information.

Total Client Msgs Rcvd	The total number of messages received by the client.
Total Client Msgs Sent	The total number of messages sent by the client.
Total Client Bytes Rcvd	The total number of bytes contained within the messages received by the client.
Total Client Bytes Sent	The total number of bytes contained within the messages sent by the client.
Total Client Msgs Rcvd / sec	The total number of messages received per second by the client.
Total Client Msgs Sent / sec	The total number of messages sent per second by the client.
Total Client Bytes Rcvd / sec	The total number of bytes contained within the messages received per second by the client.
Total Client Bytes Sent / sec	The total number of bytes contained within the messages sent per second by the client.
Ctl Bytes Rcvd	The number of control data bytes received by the client.
CTL Bytes Sent	The number of control data bytes sent by the client.
Ctl Msgs Rcvd	The number of control data messages received by the client.
Ctl Msgs Sent	The number of control data messages sent by the client.
Client Data Bytes Rcvd	The number of bytes contained within the data messages received by the client.
Client Data Bytes Sent	The number of bytes contained within the data messages sent by the client.
Client Data Msgs Rcvd	The number of data messages received by the client.
Client Data Msgs Sent	The number of data messages sent by the client.
Client Direct Msgs Rcvd	The number of direct messages received by the client.
Client Direct Msgs Sent	The number of direct messages sent by the client.
Client Direct Bytes Rcvd	The number of bytes contained within direct messages received by the client.
Client Direct Bytes Sent	The number of bytes contained within direct messages sent by the client.
Client Direct Msgs Rcvd / sec	The number of direct messages received per second by the client.
Client Direct Msgs Sent / sec	The number of direct messages sent per second by the client.
Client Direct Bytes Rcvd / sec	The number of bytes contained within the messages received per second by the client.

Client Direct Bytes Sent/sec	The number of bytes contained within the messages sent per second by the client.
Client NonPersistent Msgs Rcvd	The number of non-persistent messages received by the client.
Client NonPersistent Msgs Sent	The number of non-persistent messages sent by the client.
Client NonPersistent Bytes Rcvd	The number of bytes contained within the non-persistent messages received by the client.
Client NonPersistent Bytes Sent	The number of bytes contained within the non-persistent messages sent by the client.
Client NonPersistent Msgs Rcvd/sec	The number of non-persistent messages received per second by the client.
Client NonPersistent Msgs Sent/sec	The number of non-persistent messages sent per second by the client.
Client NonPersistent Bytes Rcvd/sec	The number of bytes contained within the non-persistent messages received per second by the client
Client NonPersistent Bytes Sent/sec	The number of bytes contained within the non-persistent messages sent per second by the client
Client Persistent Msgs Rcvd	The number of persistent messages received by the client.
Client Persistent Msgs Sent	The number of persistent messages sent by the client.
Client Persistent Bytes Rcvd	The number of bytes contained within the persistent messages received by the client.
Client Persistent Bytes Sent	The number of bytes contained within the persistent messages sent by the client.
Client Persistent Msgs Rcvd/sec	The number of persistent messages received per second by the client.
Client Persistent Msgs Sent/sec	The number of persistent messages sent per second by the client.
Client Persistent Bytes Rcvd/sec	The number of bytes contained within the persistent messages received per second by the client.

Client Persistent Bytes Sent/sec	The number of bytes contained within the persistent messages sent per second by the client.
Denied Dup Clients	Refer to Solace documentation for more information.
Denied Subscribe Permission	The number of denied subscription requests due to improper permissions.
Denied Subscribe Topic-ACL	The number of denied subscriptions to topics due to the fact that the client requesting was not on the Access Control List.
Denied Unsubscribe Permission	The number of denied unsubscribe requests due to improper permissions.
Denied Unsubscribe Topic-ACL	The number of denied unsubscribe requests to topics due to the fact that the client requesting was not on the Access Control List.
DTO Msgs Rcvd	The number of Deliver-To-One messages received by the client.
Egress Compressed Bytes	The number of compressed bytes contained within outgoing messages.
Ingress Compressed Bytes	The number of compressed bytes contained within incoming messages.
Total Ingress Discards	The total number of discarded incoming messages.
Total Egress Discards	The total number of discarded outgoing messages.
Total Ingress Discards/sec	The total number of discarded incoming messages per second.
Total Egress Discards/sec	The total number of discarded outgoing messages per second.
Keepalive Msgs Rcvd	The number of Keepalive messages received by the client.
Keepalive Msgs Sent	The number of Keepalive messages sent by the client.
Large Msgs Rcvd	The number of large messages received by the client.
Login Msgs Rcvd	The number of login message received by the client.
Max Exceeded Msgs Sent	The number of responses sent by the client informing the connected message router(s) that the number of the message(s) sent exceeded the maximum allowed.
Not Enough Space Msgs Sent	The number of responses sent by the client informing the connected message router(s) that the size of the message(s) sent exceeded the maximum allowable size, or that the message caused the client's Local Spool Quota to exceed the maximum amount of space.

Not Found Msgs Sent	Refer to Solace documentation for more information.
Parse Error on Add Msgs Sent	Refer to Solace documentation for more information.
Parse Error on Remove Msgs Sent	Refer to Solace documentation for more information.
Remove Subscription Msgs Rcvd	The number of remove subscription requests received by the client.
Remove Subscription Msgs Sent	The number of remove subscription requests sent by the client.
Subscribe Client Not Found	The number of subscription requests for clients that were not found.
Unsubscribe Client Not Found	The number of unsubscribe requests for clients that were not found.
Update Msgs Rcvd	Refer to Solace documentation for more information.
Update Msgs Sent	Refer to Solace documentation for more information.

Expired	When checked, performance data about the client has not been received within the time specified (in seconds) in the **$solRowExpirationTime** field in the **conf\rtvapm_solmon.properties** file. The **$solRowExpirationTimeForDelete** field allows you to define the amount of time (in seconds) in which the row will be removed from the table if there is no response from the client. To view/edit the current values, modify the following lines in the **.properties** file:
	`# Metrics data are considered expired after this number of seconds #`
	`collector.sl.rtview.sub=$solRowExpirationTime:45`
	`collector.sl.rtview.sub=$solRowExpirationTimeForDelete:3600`
	
	In the example above, the **Expired** check box would be checked after 45 seconds, and the row would be removed from the table after 3600 seconds.

Timestamp	The date and time the row data was last updated.

Single Client Summary

This display allows you to view the current and historical metrics for a single VPN client. You can view the **Client Type**, the **User Name**, the **Client ID**, the associated **Platform**, the current **Up Time**, and additional information specific to the client. You can also view the total number of incoming and outgoing messages, as well as the number of incoming and outgoing persistent, non-persistent, direct, and discarded messages.

Data Quality Indicators:

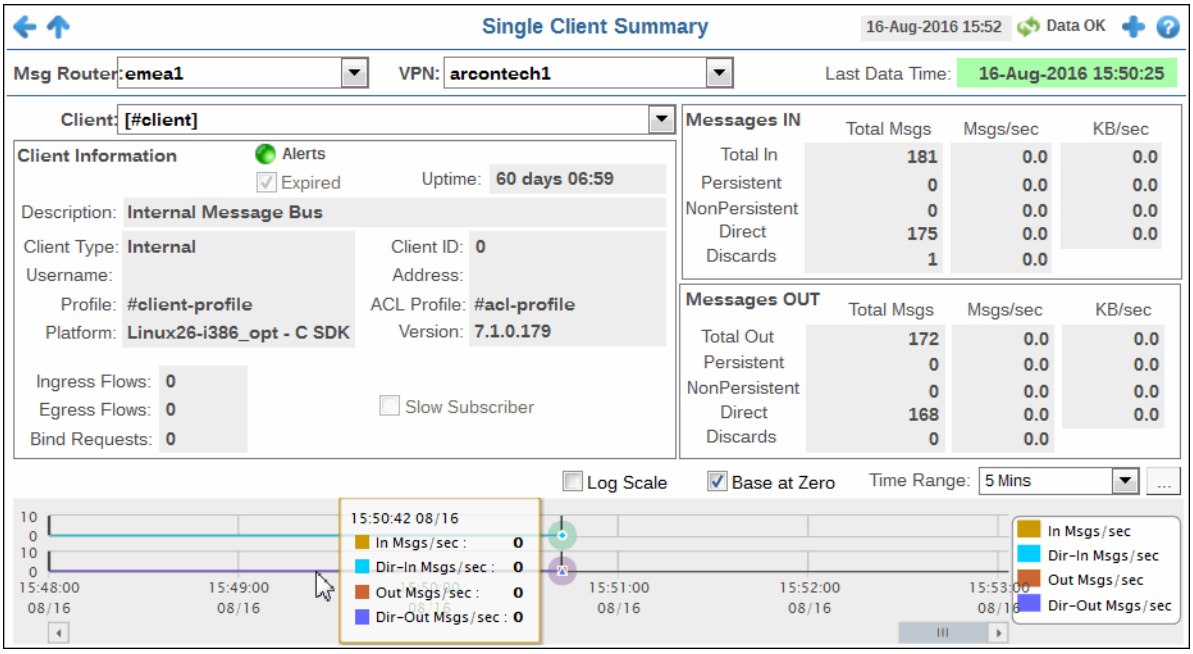
- When the display background color is (Red) the data is stale.
- The Last Data Time shows the date and time the selected message router was last updated.

Last Data Time: **15-Aug-2016 14:34:00**

If the **Last Data Time** background is:

- (Red) the selected message router is offline or expired.
- (Green) the selected message router is connected and receiving data.

This display also includes a trend graph containing the current and historical incoming messages per second, outgoing messages per second, incoming direct messages per second, and outgoing direct messages per second.



Title Bar: Indicators and functionality might include the following:

Open the previous and upper display.

Table Navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

Filter By:
The display might include these filtering options:

Msg Router:	Select the message router containing the VPN and client for which you want to view data.
VPN	Select the VPN associated with the selected message router and containing the client for which you want to view data.
Client	Select the client associated with the message router and VPN for which you want to view data.

Fields and Data:

Last Data Time

Last Data Time: **15-Aug-2016 14:34:00**

The date and time the selected message router was last updated.

Red indicates the selected message router is offline or expired.

Green indicates the selected message router is connected and receiving data.

Client Information

Alerts	The current status of the Alerts. Red indicates that one or more metrics exceeded their ALARM LEVEL threshold. Yellow indicates that one or more metrics exceeded their WARNING LEVEL threshold. Green indicates that no metrics have exceeded their alert thresholds.

Expired	When checked, performance data about the client has not been received within the time specified (in seconds) in the **$solRowExpirationTime** field in the **conf\rtvapm_solmon.properties** file. The **$solRowExpirationTimeForDelete** field allows you to define the amount of time (in seconds) in which the row will be removed from the table if there is no response from the client. To view/edit the current values, modify the following lines in the **.properties** file:
	`# Metrics data are considered expired after this number of seconds`
	`#`
	`collector.sl.rtview.sub=$solRowExpirationTime:45`
	`collector.sl.rtview.sub=$solRowExpirationTimeForDelete:3600`
	
	In the example above, the **Expired** check box would be checked after 45 seconds, and the row would be removed from the table after 3600 seconds.

Uptime	If the VPN's **Local Status** is **Up**, this field displays the length of time that the VPN has been up and running.
Description	The description of the client.
Client Type	The client type.
Username	The client's user name.
Profile	The client's profile.
Platform	The client's platform
Client ID	The client ID.
Address	The client's IP address.
ACL Profile	The access control list profile to which the client is assigned.
Version	The client's version number.
Ingress Flows	The number of message flows coming into the client.
Egress Flows	The number of message flows going out of the client.
Bind Requests	The number of bind requests received by the client.
Slow Subscriber	This check box will be checked if the client consistently fails to consume their messages at the offered rate (which causes their egress queues to fill up).

Messages IN	**Total In**	Displays the total incoming messages (**Total Msgs**), the total incoming message rate (**Msgs/sec**), and the total incoming kilobytes per second (**KB/sec**).
	Persistent	Displays the total number of incoming persistent messages (**Total Msgs**), the incoming persistent message rate (**Msgs/sec**), and the total incoming kilobytes per second (**KB/sec**) for the persistent messages.
	NonPersistent	Displays the total number of incoming non-persistent messages (**Total Msgs**), the incoming non-persistent message rate (**Msgs/sec**), and the total incoming kilobytes per second (**KB/sec**) for the non-persistent messages.
	Direct	Displays the total number of incoming direct messages (**Total Msgs**), the incoming direct message rate (**Msgs/sec**), and the total incoming kilobytes per second (**KB/sec**) for the direct messages.
	Discards	Displays the total number of incoming messages (**Total Msgs**) that were discarded, the incoming message rate (**Msgs/sec**) for the discarded messages, and the total kilobytes per second (**KB/sec**) of discarded incoming messages.
Messages OUT	**Total Out**	Displays the total outgoing messages (**Total Msgs**), the total outgoing message rate (**Msgs/sec**), and the total outgoing kilobytes per second (**KB/sec**).
	Persistent	Displays the total number of outgoing persistent messages (**Total Msgs**), the outgoing persistent message rate (**Msgs/sec**), and the total outgoing kilobytes per second (**KB/sec**) for the persistent messages.
	NonPersistent	Displays the total number of outgoing non-persistent messages (**Total Msgs**), the outgoing non-persistent message rate (**Msgs/sec**), and the total outgoing kilobytes per second (**KB/sec**) for the non-persistent messages.
	Direct	Displays the total number of outgoing direct messages (**Total Msgs**), the outgoing direct message rate (**Msgs/sec**), and the total outgoing kilobytes per second (**KB/sec**) for the direct messages.
	Discards	Displays the total number of outgoing messages (**Total Msgs**) that were discarded, the outgoing message rate (**Msgs/sec**) for the discarded messages, and the total kilobytes per second (**KB/sec**) of discarded outgoing messages.
Messages Pending	The total number of pending messages for the VPN.	

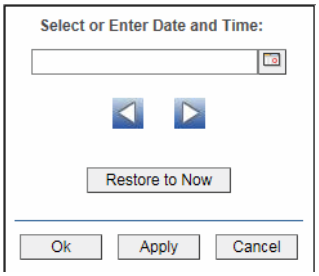
Trend Graphs
Traces the sum of process metrics for the client associated with the selected message router and VPN.

- **In Msgs/sec**: The rate of incoming messages (per second) into the client.
- **Dir-In Msgs/sec**: The rate of direct incoming messages (per second) into the client.
- **Out Msgs/sec**: The rate of outgoing messages (per second) from the client.
- **Dir-Out Msgs/sec**: The rate of direct outgoing messages (per second) from the client.

Log Scale	Select to enable a logarithmic scale. Use **Log Scale** to see usage correlations for data with a wide range of values. For example, if a minority of your data is on a scale of tens, and a majority of your data is on a scale of thousands, the minority of your data is typically not visible in non-log scale graphs. **Log Scale** makes data on both scales visible by applying logarithmic values rather than actual values to the data.

Base at Zero Select to use zero (**0**) as the Y axis minimum for all graph traces.

Time Range Select a time range from the drop down menu varying from **2 Minutes** to **Last 7 Days**, or display **All Data**. To specify a time range, click Calendar ...



By default, the time range end point is the current time. To change the time range end point, click Calendar ... and select a date and time from the calendar or enter the date and time in the text field using the following format: **MMM dd, YYYY HH:MM**. For example, **Aug 21, 2011 12:24 PM**.

Use the navigation arrows to move forward or backward one time period. NOTE: The time period is determined by your selection from the **Time Range** drop-down menu.

Click **Restore to Now** to reset the time range end point to the current time.

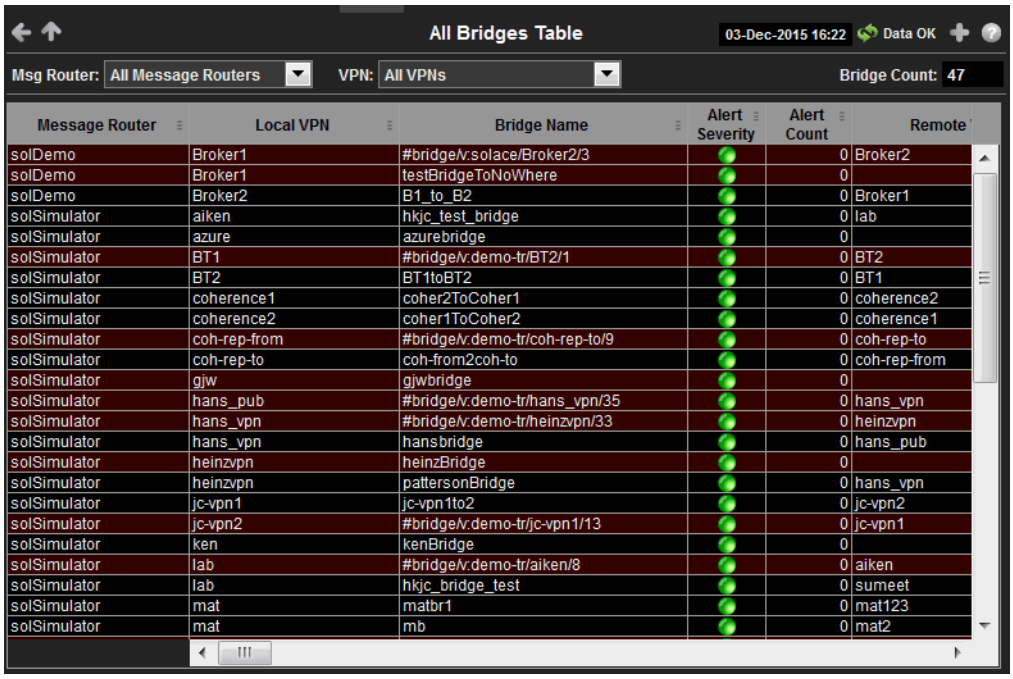
Bridges

These displays provide process data for bridges configured on a VPN. Displays in this View are:

- "All Bridges" on page 84: A tabular view of all available process performance data for all bridges configured on a VPN.
- "Single Bridge Summary" on page 88: Current and historical metrics for a single bridge.

All Bridges

This display allows you to view data for all bridges configured for a VPN. Rows listing bridges that are disabled or expired display with a shaded background. You can drill-down and view the details in the "Single Bridge Summary" display for a specific bridge by clicking on a row in the resulting table.



Message Router	Local VPN	Bridge Name	Alert Severity	Alert Count	Remote
solDemo	Broker1	#bridge/v:solace/Broker2/3		0	Broker2
solDemo	Broker1	testBridgeToNoWhere		0	
solDemo	Broker2	B1_to_B2		0	Broker1
solSimulator	aiken	hkjc_test_bridge		0	lab
solSimulator	azure	azurebridge		0	
solSimulator	BT1	#bridge/v:demo-tr/BT2/1		0	BT2
solSimulator	BT2	BT1toBT2		0	BT1
solSimulator	coherence1	coher2ToCoher1		0	coherence2
solSimulator	coherence2	coher1ToCoher2		0	coherence1
solSimulator	coh-rep-from	#bridge/v:demo-tr/coh-rep-to/9		0	coh-rep-to
solSimulator	coh-rep-to	coh-from2coh-to		0	coh-rep-from
solSimulator	gjw	gjwbridge		0	
solSimulator	hans_pub	#bridge/v:demo-tr/hans_vpn/35		0	hans_vpn
solSimulator	hans_vpn	#bridge/v:demo-tr/heinzvpn/33		0	heinzvpn
solSimulator	hans_vpn	hansbridge		0	hans_pub
solSimulator	heinzvpn	heinzBridge		0	
solSimulator	heinzvpn	pattersonBridge		0	hans_vpn
solSimulator	jc-vpn1	jc-vpn1to2		0	jc-vpn2
solSimulator	jc-vpn2	#bridge/v:demo-tr/jc-vpn1/13		0	jc-vpn1
solSimulator	ken	kenBridge		0	
solSimulator	lab	#bridge/v:demo-tr/aiken/8		0	aiken
solSimulator	lab	hkjc_bridge_test		0	sumeet
solSimulator	mat	matbr1		0	mat123
solSimulator	mat	mb		0	mat2

Title Bar: Indicators and functionality might include the following:

Open the previous and upper display.

Table Navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

Filter By:
The display might include these filtering options:

Msg Router: Select the message router for which you want to view data.

VPN Select the VPN associated with the selected message router for which you want to view data.

Fields and Data:

Bridge Count: The total number of bridges found that were configured on the VPN and are displayed in the table.

Message Router Displays the name of the message router

Local VPN	The name of the local VPN.
Bridge Name	The name of the bridge.
Alert Severity	The current level of alerts in the row. Red indicates that one or more metrics exceeded their ALARM LEVEL threshold. Yellow indicates that one or more metrics exceeded their WARNING LEVEL threshold. Green indicates that no metrics have exceeded their alert thresholds.
Alert Count	The total number of active alerts for the process.
Remote VPN	The name of the remote VPN that is connected to the local VPN via the bridge.
Remote Router	The name of the remote router.
Admin State	Indicates whether the bridge has been administratively enabled (via SolAdmin or the command line interface).
Inbound Operational State	The current inbound operational status of the bridge. (The administrator can turn off a bridge's input or output for maintenance or other reasons.)
Outbound Operational State	The current outbound operational status of the bridge. (The administrator can turn off a bridge's input or output for maintenance or other reasons.)
Queue Operational State	The current operational status of the queue.
Connection Establisher	Indicates whether the administrator created and configured the bridge directly on the message router using SolAdmin or the command line interface, or indirectly from another message router.
Redundancy	Displays whether the bridge is the **primary** bridge, the **backup** bridge, the **static** bridge (default bridge used when no other bridge is available), or whether it is the only bridge available (**none**).
Uptime	The current amount of time in which the bridge has been up and running.
Client Name	The name of the client.
Connected Via Addr	The local IP address and port used for the bridge.
Connected Via Interface	The name of the network interface used for the bridge.
Client Direct Bytes Rcvd	The number of bytes contained within direct messages received by the client via the bridge.
Client Direct Bytes/sec Rcvd	The number of bytes contained within direct messages received per second by the client via the bridge.
Client Direct Bytes Sent	The number of bytes contained within direct messages sent by the client via the bridge.
Client Direct Bytes/sec Sent	The number of bytes contained within direct messages sent per second by the client via the bridge.
Client Direct Msgs/sec Rcvd	The number of bytes contained within direct messages received per second by the client via the bridge.

Client Direct Msgs Sent	The number of direct messages sent by the client via the bridge.
Client Direct Msgs/sec Sent	The number of direct messages sent per second by the client via the bridge.
Client NonPersistent Bytes Rcvd	The number of bytes contained within non-persistent messages received by the client via the bridge.
Client NonPersistent Bytes/sec Rcvd	The number of bytes contained within non-persistent messages received per second by the client via the bridge.
Client NonPersistent Bytes Sent	The number of bytes contained within non-persistent messages sent by the client via the bridge.
Client NonPersistent Bytes/sec Sent	The number of bytes contained within non-persistent messages sent per second by the client via the bridge.
Client NonPersistent Msgs Rcvd	The number of non-persistent messages received by the client via the bridge.
Client NonPersistent Msgs/sec Rcvd	The number of non-persistent messages received per second by the client via the bridge.
Client NonPersistent Msgs Sent	The number of non-persistent messages sent by the client via the bridge.
Client NonPersistent Msgs/sec Sent	The number of non-persistent messages sent per second by the client via the bridge.
Client Persistent Bytes Rcvd	The number of bytes contained within persistent messages received by the client via the bridge.
Client Persistent Bytes/sec Rcvd	The number of bytes contained within persistent messages received per second by the client via the bridge.
Client Persistent Bytes Sent	The number of bytes contained within persistent messages sent by the client via the bridge.
Client Persistent Bytes/sec Sent	The number of bytes contained within persistent messages sent per second by the client via the bridge.
Client Persistent Msgs Rcvd	The number of persistent messages received by the client via the bridge.
Client Persistent Msgs /sec Rcvd	The number of persistent messages received per second by the client via the bridge.

Client Persistent Msgs Sent	The number of persistent messages sent by the client via the bridge.
Client Persistent Msgs/sec Sent	The number of persistent messages sent per second by the client via the bridge.
Total Client Bytes Rcvd	The number of bytes contained within all messages received by the client via the bridge.
Total Client Bytes/sec Rcvd	The number of bytes contained within all messages received per second by the client via the bridge.
Total Client Bytes Sent	The number of bytes contained within all messages sent by the client via the bridge.
Total Client Bytes/sec Sent	The number of bytes contained within all messages sent per second by the client via the bridge.
Total Client Msgs Rcvd	The total number of all messages received by the client via the bridge.
Total Client Msgs/sec Rcvd	The total number of all messages received per second by the client via the bridge.
Total Client Msgs Sent	The total number of all messages sent by the client via the bridge.
Total Client Msgs/sec Sent	The total number of all messages sent per second by the client via the bridge.
Total Out Discards	The total number of discarded outgoing messages sent by the client via the bridge.
Total Out Discards/sec	The total number of discarded outgoing messages sent per second by the client via the bridge.
Total In Discards	The total number of discarded incoming messages received by the client via the bridge.
Total In Discards/sec	The total number of discarded incoming messages received per second by the client via the bridge.

Expired	When checked, performance data about the bridge has not been received within the time specified (in seconds) in the **$solRowExpirationTime** field in the **conf\rtvapm_solmon.properties** file. The **$solRowExpirationTimeForDelete** field allows you to define the amount of time (in seconds) in which the row will be removed from the table if there is no response from the bridge. To view/edit the current values, modify the following lines in the **.properties** file:
	`# Metrics data are considered expired after this number of seconds #`
	`collector.sl.rtview.sub=$solRowExpirationTime:45`
	`collector.sl.rtview.sub=$solRowExpirationTimeForDelete:3600`
	
	In the example above, the **Expired** check box would be checked after 45 seconds, and the row would be removed from the table after 3600 seconds.

Timestamp	The date and time the row data was last updated.

Single Bridge Summary

This display allows you to view data for a specific bridge configured on a VPN.

Data Quality Indicators:

- When the display background color is (Red) the data is stale.
- The Last Data Time shows the date and time the selected message router was last updated.

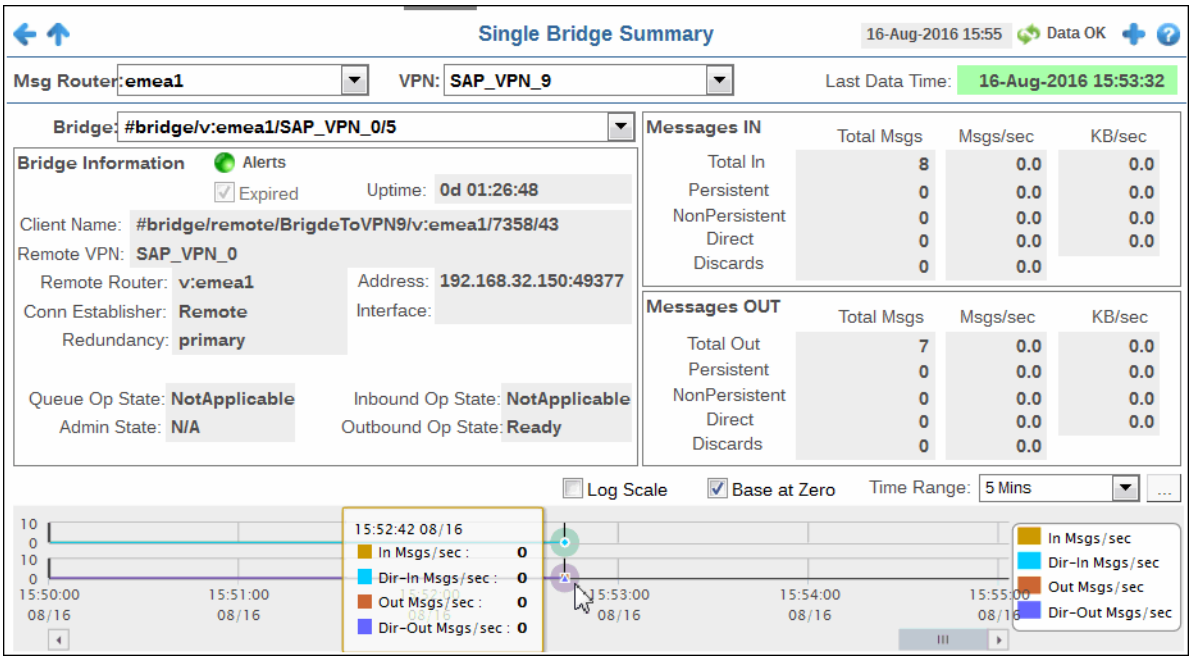
Last Data Time: 15-Aug-2016 14:34:00

If the **Last Data Time** background is:

(Red) the selected message router is offline or expired.

(Green) the selected message router is connected and receiving data.

Choose a message router, VPN, and a bridge from the drop-down menus, and use the **Time-Range** to "zoom-in" or "zoom-out" on a specific time frame in the trend graph.



Title Bar: Indicators and functionality might include the following:

Open the previous and upper display.

Table Navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

Filter By:
The display might include these filtering options:

Msg Router:	Select the message router containing the VPN and client for which you want to view data.
VPN	Select the VPN associated with the selected message router and containing the client for which you want to view data.
Bridge	Select the bridge associated with the message router and VPN for which you want to view data.

Fields and Data:

Last Data Time

Last Data Time: **15-Aug-2016 14:34:00**

The date and time the selected message router was last updated.
Red indicates the selected message router is offline or expired.
Green indicates the selected message router is connected and receiving data.

Bridge Information

Alerts	The current status of the Alerts. Red indicates that one or more metrics exceeded their ALARM LEVEL threshold. Yellow indicates that one or more metrics exceeded their WARNING LEVEL threshold. Green indicates that no metrics have exceeded their alert thresholds.

Expired	When checked, performance data about the bridge has not been received within the time specified (in seconds) in the **$solRowExpirationTime** field in the **conf\rtvapm_solmon.properties** file. The **$solRowExpirationTimeForDelete** field allows you to define the amount of time (in seconds) in which the row will be removed from the table if there is no response from the bridge. To view/edit the current values, modify the following lines in the **.properties** file:
	`# Metrics data are considered expired after this number of seconds`
	`#`
	`collector.sl.rtview.sub=$solRowExpirationTime:45`
	`collector.sl.rtview.sub=$solRowExpirationTimeForDelete:3600`
	
	In the example above, the **Expired** check box would be checked after 45 seconds, and the row would be removed from the table after 3600 seconds.

Uptime	Displays the length of time that the bridge has been up and running.
Client Name	The name of the client.
Remote VPN	The name of the remote VPN that is connected to the local VPN via the bridge.
Remote Router	The name of the remote router.
Conn Establisher	Refer to Solace documentation for more information.
Redundancy	Indicates whether the bridge is the **primary** bridge, the **backup** bridge, the **static** bridge (default bridge used when no other bridge is available), or whether it is the only bridge available (**none**).
Address	The IP address.

	Interface	The interface ID.
	Queue Op State	Refer to Solace documentation for more information.
	Admin State	Indicates whether the bridge has been administratively enabled (via SolAdmin or the command line interface).
	Inbound Op State	The current inbound operational status of the bridge. (The administrator can turn off a bridge's input or output for maintenance or other reasons.)
	Outbound Op State	The current outbound operational status of the bridge. (The administrator can turn off a bridge's input or output for maintenance or other reasons.)
Messages IN	**Total In**	Displays the total incoming messages (**Total Msgs**), the total incoming message rate (**Msgs/sec**), and the total incoming kilobytes per second (**KB/sec**).
	Persistent	Displays the total number of incoming persistent messages (**Total Msgs**), the incoming persistent message rate (**Msgs/sec**), and the total incoming kilobytes per second (**KB/sec**) for the persistent messages.
	NonPersistent	Displays the total number of incoming non-persistent messages (**Total Msgs**), the incoming non-persistent message rate (**Msgs/sec**), and the total incoming kilobytes per second (**KB/sec**) for the non-persistent messages.
	Direct	Displays the total number of incoming direct messages (**Total Msgs**), the incoming direct message rate (**Msgs/sec**), and the total incoming kilobytes per second (**KB/sec**) for the direct messages.
	Discards	Displays the total number of incoming messages (**Total Msgs**) that were discarded, the incoming message rate (**Msgs/sec**) for the discarded messages, and the total kilobytes per second (**KB/sec**) of discarded incoming messages.
Messages OUT	**Total Out**	Displays the total outgoing messages (**Total Msgs**), the total outgoing message rate (**Msgs/sec**), and the total outgoing kilobytes per second (**KB/sec**).
	Persistent	Displays the total number of outgoing persistent messages (**Total Msgs**), the outgoing persistent message rate (**Msgs/sec**), and the total outgoing kilobytes per second (**KB/sec**) for the persistent messages.
	NonPersistent	Displays the total number of outgoing non-persistent messages (**Total Msgs**), the outgoing non-persistent message rate (**Msgs/sec**), and the total outgoing kilobytes per second (**KB/sec**) for the non-persistent messages.
	Direct	Displays the total number of outgoing direct messages (**Total Msgs**), the outgoing direct message rate (**Msgs/sec**), and the total outgoing kilobytes per second (**KB/sec**) for the direct messages.
	Discards	Displays the total number of outgoing messages (**Total Msgs**) that were discarded, the outgoing message rate (**Msgs/sec**) for the discarded messages, and the total kilobytes per second (**KB/sec**) of discarded outgoing messages.

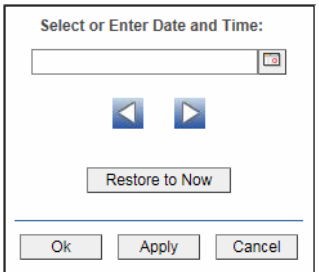
Trend Graphs
Traces the sum of process metrics for the client associated with the selected message router and VPN.

- **In Msgs/sec**: The rate of incoming messages (per second) into the client.
- **Dir-In Msgs/sec**: The rate of direct incoming messages (per second) into the client.
- **Out Msgs/sec**: The rate of outgoing messages (per second) from the client.
- **Dir-Out Msgs/sec**: The rate of direct outgoing messages (per second) from the client.

Log Scale Select to enable a logarithmic scale. Use **Log Scale** to see usage correlations for data with a wide range of values. For example, if a minority of your data is on a scale of tens, and a majority of your data is on a scale of thousands, the minority of your data is typically not visible in non-log scale graphs. **Log Scale** makes data on both scales visible by applying logarithmic values rather than actual values to the data.

Base at Zero Select to use zero (**0**) as the Y axis minimum for all graph traces.

Time Range Select a time range from the drop down menu varying from **2 Minutes** to **Last 7 Days**, or display **All Data**. To specify a time range, click Calendar ...



By default, the time range end point is the current time. To change the time range end point, click Calendar ... and select a date and time from the calendar or enter the date and time in the text field using the following format: **MMM dd, YYYY HH:MM**. For example, **Aug 21, 2011 12:24 PM**.

Use the navigation arrows to move forward or backward one time period. NOTE: The time period is determined by your selection from the **Time Range** drop-down menu.

Click **Restore to Now** to reset the time range end point to the current time.

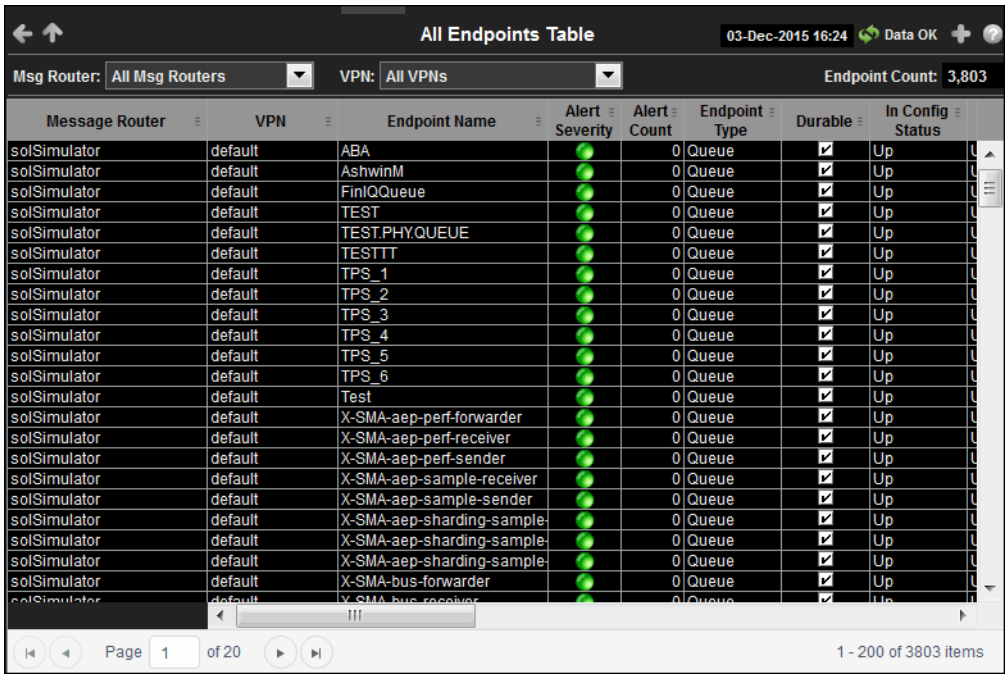
Endpoints

These displays list data for one or more endpoints configured on a VPN. Displays in this View are:

- "All Endpoints" on page 92
- "Single Endpoint Summary" on page 94
- "Single Endpoint Summary Rates" on page 97

All Endpoints

This display lists data in a table for all endpoints configured on a VPN. Each row in the table lists the details for a specific endpoint. You can click a column header to sort column data in numerical or alphabetical order, or drill-down and view details for a specific endpoint in the "Single Endpoint Summary" display by clicking on a row in the table.



Message Router	VPN	Endpoint Name	Alert Severity	Alert Count	Endpoint Type	Durable	In Config Status
solSimulator	default	ABA		0	Queue	✓	Up
solSimulator	default	AshwinM		0	Queue	✓	Up
solSimulator	default	FinIQQueue		0	Queue	✓	Up
solSimulator	default	TEST		0	Queue	✓	Up
solSimulator	default	TEST.PHY.QUEUE		0	Queue	✓	Up
solSimulator	default	TESTTT		0	Queue	✓	Up
solSimulator	default	TPS_1		0	Queue	✓	Up
solSimulator	default	TPS_2		0	Queue	✓	Up
solSimulator	default	TPS_3		0	Queue	✓	Up
solSimulator	default	TPS_4		0	Queue	✓	Up
solSimulator	default	TPS_5		0	Queue	✓	Up
solSimulator	default	TPS_6		0	Queue	✓	Up
solSimulator	default	Test		0	Queue	✓	Up
solSimulator	default	X-SMA-aep-perf-forwarder		0	Queue	✓	Up
solSimulator	default	X-SMA-aep-perf-receiver		0	Queue	✓	Up
solSimulator	default	X-SMA-aep-perf-sender		0	Queue	✓	Up
solSimulator	default	X-SMA-aep-sample-receiver		0	Queue	✓	Up
solSimulator	default	X-SMA-aep-sample-sender		0	Queue	✓	Up
solSimulator	default	X-SMA-aep-sharding-sample-		0	Queue	✓	Up
solSimulator	default	X-SMA-aep-sharding-sample-		0	Queue	✓	Up
solSimulator	default	X-SMA-aep-sharding-sample-		0	Queue	✓	Up
solSimulator	default	X-SMA-bus-forwarder		0	Queue	✓	Up

Title Bar: Indicators and functionality might include the following:

Open the previous and upper display.

Table Navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

Filter By:
The display might include these filtering options:

Msg Router: Select the message router for which you want to view data.

VPN Select the VPN associated with the selected message router for which you want to view data.

Fields and Data:

Endpoint Count: The total number of endpoints configured on the VPN and displayed in the table.

Message Router Displays the name of the message router

VPN	The name of the VPN.
Endpoint Name	The name of the endpoint.
Alert Severity	The current alert severity in the row. Red indicates that one or more metrics exceeded their ALARM LEVEL threshold. Yellow indicates that one or more metrics exceeded their WARNING LEVEL threshold. Green indicates that no metrics have exceeded their alert thresholds.
Alert Count	The total number of active alerts for the endpoint.
Endpoint Type	The type of endpoint (either queue or topic).
Durable	Displays whether or not the endpoint is durable (checked) or non-durable (unchecked). Durable endpoints remain after an message router restart and are automatically restored as part of an message router's backup and restoration process.
In Config Status	Refer to Solace documentation for more information.
Out Config Status	Refer to Solace documentation for more information.
Type	Refer to Solace documentation for more information.
Access Type	Refer to Solace documentation for more information.
Bind Count	The total number of binds connected to the endpoint.
Pending Messages	The total number of pending messages on the endpoint.
Spool Usage (MB)	The total spool usage consumed on the endpoint (in megabytes).
High Water Mark (MB)	The highest level of spool usage on the endpoint (in megabytes).
In Selector	Refer to Solace documentation for more information.
Out Selector	Refer to Solace documentation for more information.

Expired	When checked, performance data about the endpoint has not been received within the time specified (in seconds) in the **$solRowExpirationTime** field in the **conf\rtvapm_solmon.properties** file. The **$solRowExpirationTimeForDelete** field allows you to define the amount of time (in seconds) in which the row will be removed from the table if there is no response from the endpoint. To view/edit the current values, modify the following lines in the **.properties** file:
	`# Metrics data are considered expired after this number of seconds #`
	`collector.sl.rtview.sub=$solRowExpirationTime:45`
	`collector.sl.rtview.sub=$solRowExpirationTimeForDelete:3600`
	
	In the example above, the **Expired** check box would be checked after 45 seconds, and the row would be removed from the table after 3600 seconds.

Time Stamp	The date and time the data was last updated.

Single Endpoint Summary

This display allows you to view endpoint information, message data, and a trend graph for pending and spool messages for a specific endpoint configured on a VPN. Choose a message router, VPN, and an endpoint from the drop-down menus, and use the **Time Range** to "zoom-in" or "zoom-out" on a specific time frame in the trend graph.

Data Quality Indicators:

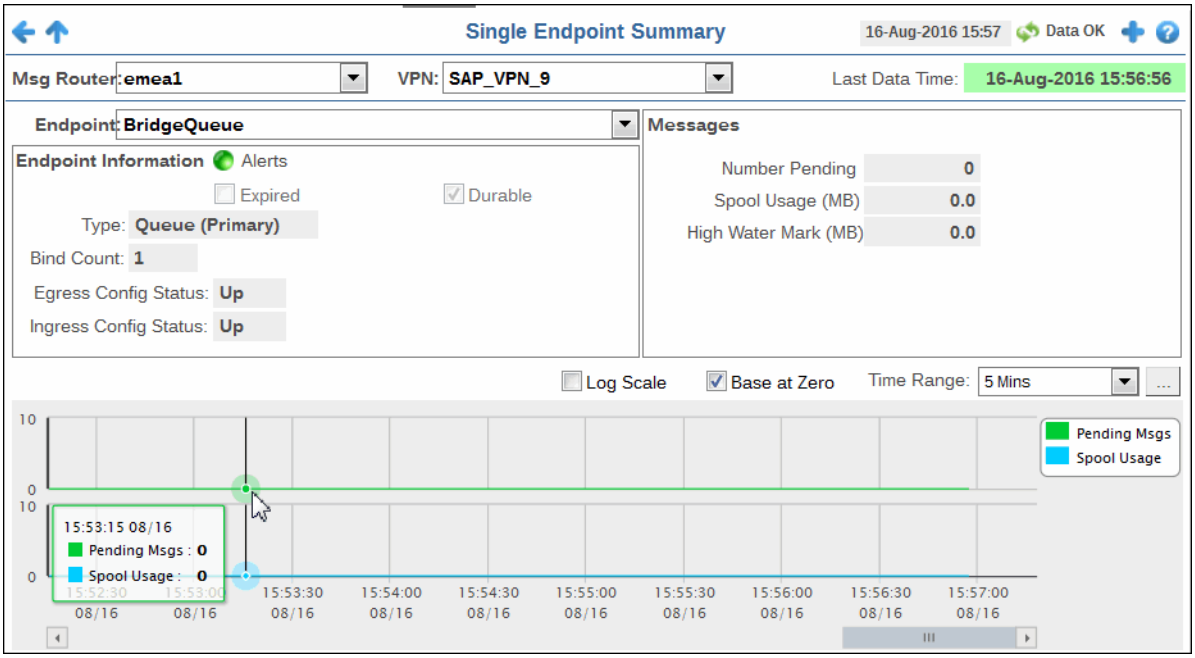
- When the display background color is (Red) the data is stale.
- The Last Data Time shows the date and time the selected message router was last updated.

If the **Last Data Time** background is:

(Red) the selected message router is offline or expired.

(Green) the selected message router is connected and receiving data.

This display is provided by default and should be used if you do not want to collect message spool data for specific VPNs. However, if you do want to configure message spool monitoring for specific VPNs, then you should use the **Single Endpoint Summary Rates** display instead, which is not included in the navigation tree by default. See "Single Endpoint Summary Rates" for more information on disabling the **Single Endpoint Summary** display and enabling the **Single Endpoint Summary Rates** display.



Title Bar: Indicators and functionality might include the following:

Open the previous and upper display.

Table Navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

Filter By:
The display might include these filtering options:

Msg Router: Select the message router containing the VPN and client for which you want to view data.

VPN Select the VPN associated with the selected message router and containing the client for which you want to view data.

Endpoint Select the endpoint associated with the message router and VPN for which you want to view data.

Fields and Data:

Last Data Time

Last Data Time: 15-Aug-2016 14:34:00

The date and time the selected message router was last updated.

Red indicates the selected message router is offline or expired.

Green indicates the selected message router is connected and receiving data.

Endpoint Information

Alerts The current status of the Alerts.

Red indicates that one or more metrics exceeded their ALARM LEVEL threshold.

Yellow indicates that one or more metrics exceeded their WARNING LEVEL threshold.

Green indicates that no metrics have exceeded their alert thresholds.

Expired When checked, performance data about the endpoint has not been received within the time specified (in seconds) in the **$solRowExpirationTime** field in the **conf\rtvapm_solmon.properties** file. The **$solRowExpirationTimeForDelete** field allows you to define the amount of time (in seconds) in which the row will be removed from the table if there is no response from the endpoint. To view/edit the current values, modify the following lines in the **.properties** file:

```
# Metrics data are considered expired after this number of
seconds
#
collector.sl.rtview.sub=$solRowExpirationTime:45
collector.sl.rtview.sub=$solRowExpirationTimeForDelete:3600
```

In the example above, the **Expired** check box would be checked after 45 seconds, and the row would be removed from the table after 3600 seconds.

Durable Displays whether or not the endpoint is durable (checked) or non-durable (unchecked). Durable endpoints remain after an message router restart and are automatically restored as part of an message router's backup and restoration process.

	Type	The type of endpoint (either queue or topic).
	Bind Count	The total number of binds connected to the endpoint.
	Egress Config Status	The status of the egress configuration.
	Ingress Config Status	The status of the ingress configuration.
Messages	**Number Pending**	The total number of pending messages on the endpoint.
	Spool Usage (MB)	The current spool usage consumed on the endpoint (in megabytes).
	High Water Mark (MB)	The highest level of spool usage on the endpoint (in megabytes).

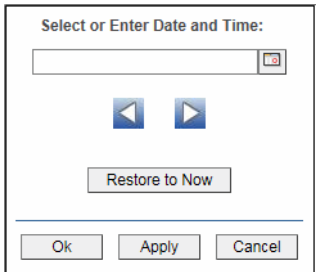
Trend Graphs
Traces the sum of process metrics for the endpoint associated with the selected message router and VPN.

- **Pending Msgs**: The number of pending messages.
- **Spool Usage**: The total spool usage consumed on the endpoint (in megabytes).

Log Scale Select to enable a logarithmic scale. Use **Log Scale** to see usage correlations for data with a wide range of values. For example, if a minority of your data is on a scale of tens, and a majority of your data is on a scale of thousands, the minority of your data is typically not visible in non-log scale graphs. **Log Scale** makes data on both scales visible by applying logarithmic values rather than actual values to the data.

Base at Zero Select to use zero (**0**) as the Y axis minimum for all graph traces.

Time Range Select a time range from the drop down menu varying from **2 Minutes** to **Last 7 Days**, or display **All Data**. To specify a time range, click Calendar ...



By default, the time range end point is the current time. To change the time range end point, click Calendar ... and select a date and time from the calendar or enter the date and time in the text field using the following format: **MMM dd, YYYY HH:MM**. For example, **Aug 21, 2011 12:24 PM**.

Use the navigation arrows to move forward or backward one time period. NOTE: The time period is determined by your selection from the **Time Range** drop-down menu.

Click **Restore to Now** to reset the time range end point to the current time.

Single Endpoint Summary Rates

This display allows you to view endpoint information, message data, and a trend graph for pending messages, spool messages, incoming message rates, and outgoing message rates for a specific endpoint configured on a VPN. Choose a message router, VPN, and an endpoint from the drop-down menus, and use the **Time Range** to “zoom-in” or “zoom-out” on a specific time frame in the trend graph.

Data Quality Indicators:

- When the display background color is (Red) the data is stale.
- The Last Data Time shows the date and time the selected message router was last updated.

If the **Last Data Time** background is:

(Red) the selected message router is offline or expired.

(Green) the selected message router is connected and receiving data.

The “Single Endpoint Summary” display is provided by default and should be used if you do not want to collect message spool data for specific VPNs. However, if you do want to configure message spool monitoring for specific VPNs, then you should use this display instead, which is not included in the navigation tree by default.To collect message spool data for specific VPNs, disable the **Single Endpoint Summary** display, and enable the **Single Endpoint Summary Rates** display in the navigation tree, perform the following steps:

1. Uncomment and copy the following line in your **sample.properties** file to configure message spool monitoring for each VPN:

   ```
   #collector.sl.rtview.cache.config=sol_cache_source_msg_spool.rtv
   $solConn:UNIQUE_APPLIANCE_NAME $solVpnName:VPN_NAME
   ```

2. To edit the navigation tree, extract **solmon.navtree.xml** from the **rtvapm\solmon\lib\rtvapm_solmon.jar** file and save it in the **emsample\servers\central** directory.

3. In the **solmon.navtree.xml** file, comment out the following line (enclose with **<!--** and **-->**):

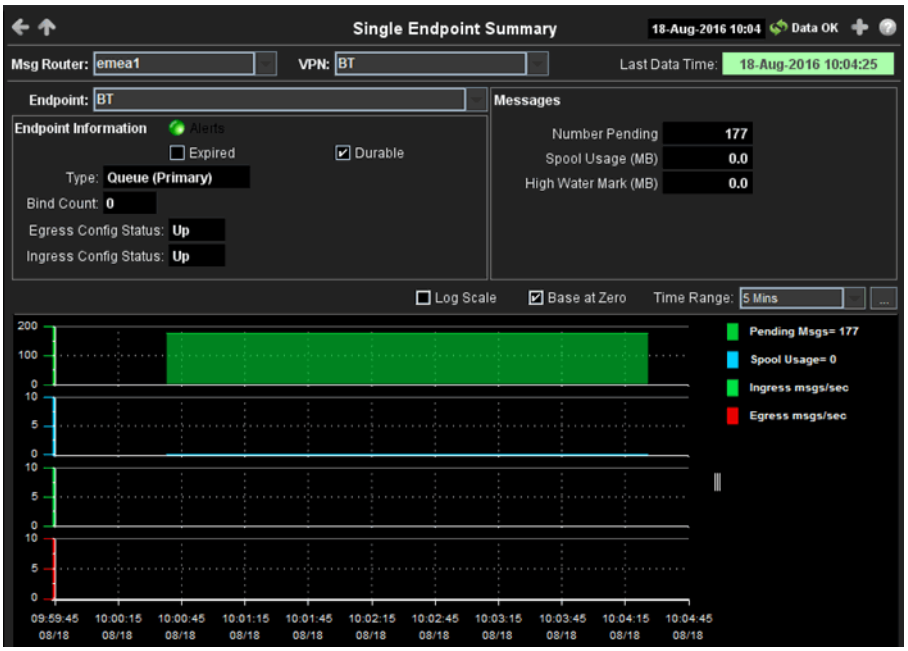
   ```
   <node label="Single Endpoint Summary" display="sol_endpoint_summary"></node>
   ```

   and add/uncomment this line:

   ```
   <node label="Single Endpoint Summary Rates" display="sol_endpoint_summaryWithRates"></node>
   ```

Once the file is edited and saved in **emsample\servers\central** directory, it will get picked up automatically during startup.

Note: Collecting data for a large number of VPNs might impair the performance of the message router.



Title Bar: Indicators and functionality might include the following:

Open the previous and upper display.

Table Navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

Filter By:
The display might include these filtering options:

Msg Router:	Select the message router containing the VPN and client for which you want to view data.
VPN	Select the VPN associated with the selected message router and containing the client for which you want to view data.
Endpoint	Select the endpoint associated with the message router and VPN for which you want to view data.

Fields and Data:

Last Data Time

Last Data Time: **15-Aug-2016 14:34:00**

The date and time the selected message router was last updated.

Red indicates the selected message router is offline or expired.

Green indicates the selected message router is connected and receiving data.

Endpoint Information

Alerts The current status of the Alerts.

Red indicates that one or more metrics exceeded their ALARM LEVEL threshold.

Yellow indicates that one or more metrics exceeded their WARNING LEVEL threshold.

Green indicates that no metrics have exceeded their alert thresholds.

Expired When checked, performance data about the endpoint has not been received within the time specified (in seconds) in the **$solRowExpirationTime** field in the **conf\rtvapm_solmon.properties** file. The **$solRowExpirationTimeForDelete** field allows you to define the amount of time (in seconds) in which the row will be removed from the table if there is no response from the endpoint. To view/edit the current values, modify the following lines in the **.properties** file:

```
# Metrics data are considered expired after this number of
seconds
#
collector.sl.rtview.sub=$solRowExpirationTime:45
collector.sl.rtview.sub=$solRowExpirationTimeForDelete:3600
```

In the example above, the **Expired** check box would be checked after 45 seconds, and the row would be removed from the table after 3600 seconds.

Durable Displays whether or not the endpoint is durable (checked) or non-durable (unchecked). Durable endpoints remain after an message router restart and are automatically restored as part of an message router's backup and restoration process.

Type The type of endpoint (either queue or topic).

Bind Count The total number of binds connected to the endpoint.

Egress Config Status The status of the egress configuration.

Ingress Config Status The status of the ingress configuration.

Messages

Number Pending The total number of pending messages on the endpoint.

Spool Usage (MB) The current spool usage consumed on the endpoint (in megabytes).

High Water Mark (MB) The highest level of spool usage on the endpoint (in megabytes).

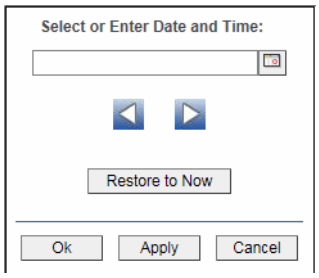
Trend Graphs
Traces the sum of process metrics for the endpoint associated with the selected message router and VPN.

- **Pending Msgs**: The number of pending messages.
- **Spool Usage**: The total spool usage consumed on the endpoint (in megabytes).
- **Ingress msgs/sec**: The number of incoming messages per second.
- **Egress msgs/sec**: The number of outgoing messages per second.

Log Scale Select to enable a logarithmic scale. Use **Log Scale** to see usage correlations for data with a wide range of values. For example, if a minority of your data is on a scale of tens, and a majority of your data is on a scale of thousands, the minority of your data is typically not visible in non-log scale graphs. **Log Scale** makes data on both scales visible by applying logarithmic values rather than actual values to the data.

Base at Zero Select to use zero (**0**) as the Y axis minimum for all graph traces.

Time Range Select a time range from the drop down menu varying from **2 Minutes** to **Last 7 Days**, or display **All Data**. To specify a time range, click Calendar ...



By default, the time range end point is the current time. To change the time range end point, click Calendar ... and select a date and time from the calendar or enter the date and time in the text field using the following format: **MMM dd, YYYY HH:MM**. For example, **Aug 21, 2011 12:24 PM**.

Use the navigation arrows to move forward or backward one time period. NOTE: The time period is determined by your selection from the **Time Range** drop-down menu.

Click **Restore to Now** to reset the time range end point to the current time.

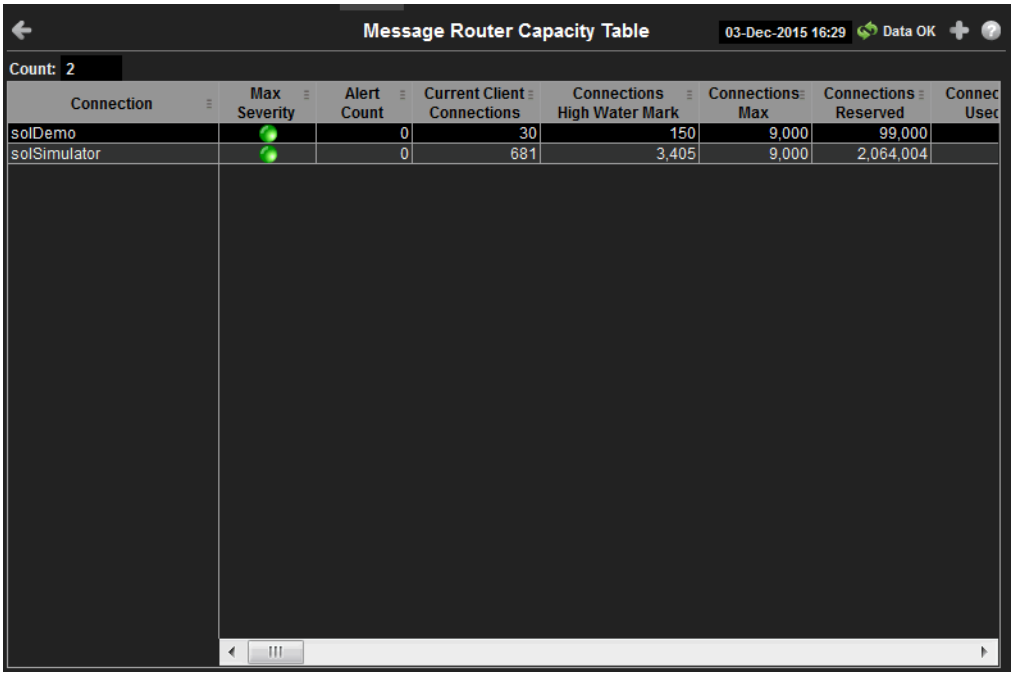
Capacity Analysis

These displays provide current metrics, alert count and severity at the message router level. Displays in this View are:

- "All Message Router Capacity" on page 101: View client, spool usage, incoming messages, outgoing messages, incoming bytes, and outgoing bytes data for all message routers.
- "Message Router Capacity" on page 104: View client, spool usage, incoming messages, outgoing messages, incoming bytes, and outgoing bytes data for a specific message router.
- "Message Router Capacity Trends" on page 108: View the message router capacity data for a specific message router in a trend graph format.

All Message Router Capacity

This display allows you to view the message router capacity data for all message routers in a table format. You can view client, spool usage, incoming message, outgoing message, incoming bytes, and outgoing bytes data for the message router. Clicking on a row in the table displays the selected message router data in the "Message Router Capacity" display.



Title Bar: Indicators and functionality might include the following:

Open the previous and upper display.

Table Navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

Fields and Data:

Count	The total number of message routers listed in the table.
Connection	The name of the message router.
Max Severity	The maximum level of all alerts on the message router
Alert Count	The total number of alerts on the message router.
Current Client Connections	The current number of clients connected to the message router.

Connections High Water Mark	The highest number of clients connected to the message router on a particular day in the past 30 days.
Connections Max	The maximum number of clients allowed to connect to the message router.
Connections Reserved	The sum over all VPNs of connections allowed for each VPN.
Connections Used %	The number of current clients divided by the maximum number of clients.
Connections Used HWM %	The highest utilization level in the last 30 days (in percent).
Current Spool Usage (MB)	The current spool usage, in megabytes, on the message router.
Current Spool Usage High Water Mark	The most megabytes used by messages spools on the message router on a particular day in the past 30 days.
Spool Disk Allocated	The maximum number of megabytes allowed to be used by message spools on the message router.
Spool Reserved	The sum over all VPNs of max spool allowed for each VPN.
Current Spool Usage %	The current spool usage in megabytes divided by the maximum allowed spool usage on the message router.
Current Spool Usage HWM %	The highest utilization level in the last 30 days (in percent).
Delivered Unacked Msgs Utilization %	The current number of delivered messages that were not acknowledged divided by the maximum number of delivered messages that were not acknowledged allowed on the message router.
Ingress Flow Count	The current number of flows coming into the message router.
Ingress Flow High Water Mark	The highest number of flows coming into the message router on a particular day in the past 30 days.
Ingress Flows Allowed	The maximum number of incoming flows allowed to come into the message router.
Ingress Flow Count %	The current number of flows divided by the maximum number of flows allowed to come into the message router.
Ingress Flow Count HWM %	The highest utilization level in the last 30 days (in percent).
Ingress Msgs/sec	The current number of messages coming into the message router per second.
Ingress Msgs/sec High Water Mark	The highest number of messages coming into the message router per second on a particular day in the past 30 days.
Ingress Msgs/sec Max	The maximum number of messages (per second) allowed to come into the message router.
Ingress Msgs/sec %	The current number of incoming messages per second divided by the maximum number of messages allowed per second to come into the message router.

Egress Msgs/sec	The current number of messages going out of the message router per second.
Egress Msgs/sec HWM	The highest number of messages going out of the message router per second on a particular day in the past 30 days.
Egress Msgs/sec Max	The maximum number of messages (per second) allowed to go out of the message router.
Egress Msgs/sec %	The current number of outgoing messages divided by the maximum number of messages allowed go out of the message router.
Egress Msgs/sec HWM %	The highest utilization level in the last 30 days (in percent).
Ingress Bytes/sec	The current number of bytes coming into the message router per second.
Ingress Bytes/sec High Water Mark	The highest number of bytes coming into the message router per second on a particular day in the past 30 days.
Ingress Bytes/sec Max	The maximum number of bytes (per second) allowed to come into the message router.
Ingress Bytes/sec %	The current number of incoming bytes divided by the maximum number of bytes allowed to come into the message router.
Ingress Bytes/sec HWM %	The highest utilization level in the last 30 days (in percent).
Egress Bytes/sec	The current number of bytes going out of the message router per second.
Egress Bytes/sec High Water Mark	The highest number of bytes going out of the message router per second on a particular day in the past 30 days.
Egress Bytes/sec Max	The maximum number of bytes (per second) allowed to go out of the message router.
Egress Bytes/sec %	The current number of outgoing bytes divided by the maximum number of bytes allowed go out of the message router.
Egress Bytes/sec HWM %	The highest utilization level in the last 30 days (in percent).
Queue/Topic Subscriptions Used	The current number of queue/topic subscriptions on the message router.
Subscriptions High Water Mark	The highest number of subscriptions on the message router on a particular day in the past 30 days.
Subscriptions Max	The maximum number of subscriptions allowed on the message router.
Subscriptions Reserved	The sum over all VPNs of connections allowed for each VPN.
Queue/Topic Subscriptions Used %	The number of current subscriptions divided by the maximum number of subscriptions.
Queue/Topic Subscriptions Used HWM %	The highest utilization level in the last 30 days (in percent).

Spool Files Used	The current number of spool files on the message router.
Spool Files High Water Mark	The highest number of spool files on the message router on a particular day in the past 30 days.
Spool Files Available	The maximum number of spool files allowed to be on the message router.
Spool Files Used %	The current number of spool files divided by the maximum number of spool files allowed on the message router.
Spool Files Used HWM %	The highest utilization level in the last 30 days (in percent).
Transacted Sessions Used	The current number of transacted sessions on the message router.
Transacted Sessions High Water Mark	The highest number of transacted sessions on the message router on a particular day in the past 30 days.
Transacted Sessions Max	The maximum number of incoming transacted sessions allowed on the message router.
Transacted Sessions % Utilization	The current number of transacted sessions divided by the maximum number of transacted sessions allowed on the message router.
Transacted Sessions HWM % Utilization	The highest utilization level in the last 30 days (in percent).

Expired	When checked, performance data about the message router has not been received within the time specified (in seconds) in the **$solRowExpirationTime** field in the **conf\rtvapm_solmon.properties** file. The **$solRowExpirationTimeForDelete** field allows you to define the amount of time (in seconds) in which the row will be removed from the table if there is no response from the message router. To view/edit the current values, modify the following lines in the **.properties** file:
	`# Metrics data are considered expired after this number of seconds`
	`#`
	`collector.sl.rtview.sub=$solRowExpirationTime:45`
	`collector.sl.rtview.sub=$solRowExpirationTimeForDelete:3600`
	In the example above, the **Expired** check box would be checked after 45 seconds, and the row would be removed from the table after 3600 seconds.

Timestamp	The date and time the data was last updated.

Message Router Capacity

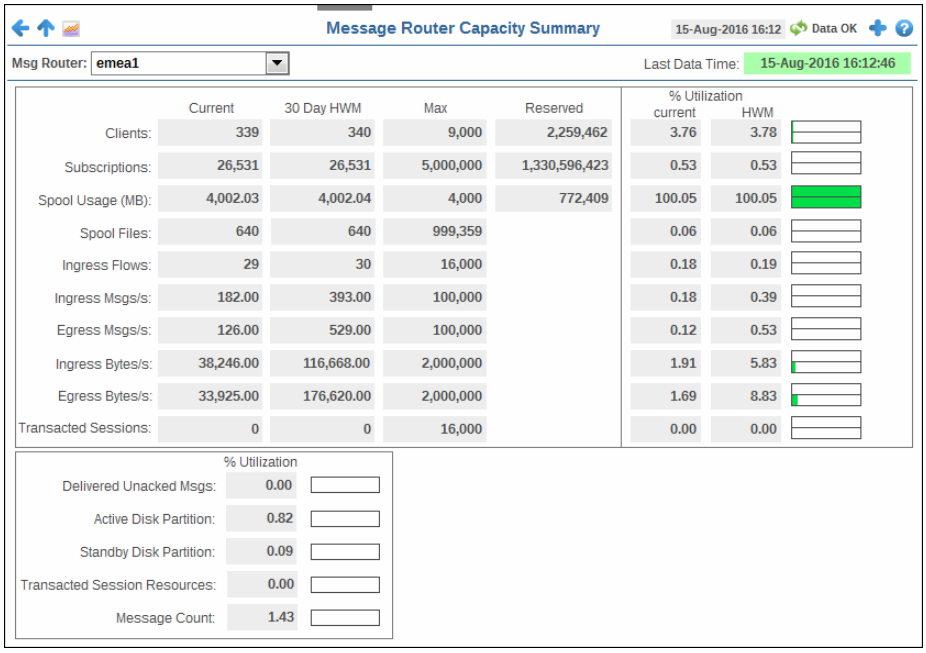
This display, a pivoted view of the **All Message Routers Capacity** table, allows you to view the message router capacity data for a specific message router. You can view client, spool usage, incoming message, outgoing message, incoming bytes, and outgoing bytes data for the message router.

Data Quality Indicators:

- When the display background color is (Red) the data is stale.
- The Last Data Time shows the date and time the selected message router was last updated.

If the **Last Data Time** background is:

- (Red) the selected message router is offline or expired.
- (Green) the selected message router is connected and receiving data.



Title Bar: Indicators and functionality might include the following:

Open the previous and upper display.

Table Navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

Note: Clicking the Capacity Trends button displays the message router's capacity metrics in the "Message Router Capacity Trends" display.

Filter By:
The display might include these filtering options:

Msg Router: Select the message router for which you want to view data.

Last Data Time

Last Data Time: 15-Aug-2016 14:34:00

The date and time the selected message router was last updated.

- Red indicates the selected message router is offline or expired.
- Green indicates the selected message router is connected and receiving data.

Fields and Data:

Count	The total number of message routers listed in the table.	
Clients	**Current**	The current number of clients connected to the message router.
	30 Day HWM	The highest number of clients connected to the message router on a particular day in the past 30 days.
	Max	The maximum number of clients allowed to connect to the message router.
	Reserved	The sum over all VPNs of connections allowed for each VPN.
	% Utilization	**Current**: The number of current clients divided by the maximum number of clients. **HWM**: The highest utilization level in the last 30 days (in percent).
Subscriptions	**Current**	The current number of subscriptions on the message router.
	30 Day HWM	The highest number of subscriptions on the message router on a particular day in the past 30 days.
	Max	The maximum number of subscriptions allowed on the message router.
	Reserved	The sum over all VPNs of connections allowed for each VPN.
	% Utilization	**Current**: The number of current subscriptions divided by the maximum number of subscriptions. **HWM**: The highest utilization level in the last 30 days (in percent).
Spool Usage (MB)	**Current**	The current spool usage, in megabytes, on the message router.
	30 Day HWM	The most megabytes used by messages spools on the message router on a particular day in the past 30 days.
	Max	The maximum number of megabytes allowed to be used by message spools on the message router.
	Reserved	The sum over all VPNs of connections allowed for each VPN.
	% Utilization	**Current**: The current spool usage in megabytes divided by the maximum allowed spool usage on the message router. **HWM**: The highest utilization level in the last 30 days (in percent).
Spool Files	**Current**	The current number of spool files on the message router.
	30 Day HWM	The highest number of spool files on the message router on a particular day in the past 30 days.
	Max	The maximum number of spool files allowed to be on the message router.
	% Utilization	**Current**: The current number of spool files divided by the maximum number of spool files allowed on the message router. **HWM**: The highest utilization level in the last 30 days (in percent).
Ingress Flows	**Current**	The current number of flows coming into the message router.
	30 Day HWM	The highest number of flows coming into the message router on a particular day in the past 30 days.
	Max	The maximum number of incoming flows allowed to come into the message router.
	% Utilization	**Current**: The current number of flows divided by the maximum number of flows allowed to come into the message router. **HWM**: The highest utilization level in the last 30 days (in percent).
Ingress Msgs/s	**Current**	The current number of messages coming into the message router per second.

	30 Day HWM	The highest number of messages coming into the message router per second on a particular day in the past 30 days.
	Max	The maximum number of messages (per second) allowed to come into the message router.
	% Utilization	**Current**: The current number of incoming messages divided by the maximum number of messages allowed to come into the message router. **HWM**: The highest utilization level in the last 30 days (in percent).
Egress Msgs/s	**Current**	The current number of messages going out of the message router per second.
	30 Day HWM	The highest number of messages going out of the message router per second on a particular day in the past 30 days.
	Max	The maximum number of messages (per second) allowed to go out of the message router.
	% Utilization	**Current**: The current number of outgoing messages divided by the maximum number of messages allowed go out of the message router. **HWM**: The highest utilization level in the last 30 days (in percent).
Ingress Bytes/s	**Current**	The current number of bytes coming into the message router per second.
	30 Day HWM	The highest number of bytes coming into the message router per second on a particular day in the past 30 days.
	Max	The maximum number of bytes (per second) allowed to come into the message router.
	% Utilization	**Current**: The current number of incoming bytes divided by the maximum number of bytes allowed to come into the message router. **HWM**: The highest utilization level in the last 30 days (in percent).
Egress Bytes/s	**Current**	The current number of bytes going out of the message router per second.
	30 Day HWM	The highest number of bytes going out of the message router per second on a particular day in the past 30 days.
	Max	The maximum number of bytes (per second) allowed to go out of the message router.
	% Utilization	**Current**: The current number of outgoing bytes divided by the maximum number of bytes allowed go out of the message router. **HWM**: The highest utilization level in the last 30 days (in percent).
Transacted Sessions	**Current**	The current number of transacted sessions on the message router.
	30 Day HWM	The highest number of transacted sessions on the message router on a particular day in the past 30 days.
	Max	The maximum number of incoming transacted sessions allowed on the message router.
	% Utilization	**Current**: The current number of transacted sessions divided by the maximum number of transacted sessions allowed on the message router. **HWM**: The highest utilization level in the last 30 days (in percent).
Delivered Unacked Msgs	**% Utilization**	The current number of delivered messages that were not acknowledged divided by the maximum number of delivered messages that were not acknowledged allowed on the message router.
Active Disk Partition	**% Utilization**	The percentage of available active disk partition that has been used.

Standby Disk Partition	**% Utilization**	The percentage of available standby disk partition that has been used.
Transacted Session Resource	**% Utilization**	The current amount of transacted session resources divided by the maximum number of transaction session resources allowed on the message router.
Message Count	**% Utilization**	The current number messages divided by the maximum number of messages allowed on the message router.

Message Router Capacity Trends

This display allows you to view the message router capacity data for a specific message router in a trend graph format. You can view client, spool usage, incoming message, outgoing message, incoming bytes, and outgoing bytes data for the message router.

Data Quality Indicators:

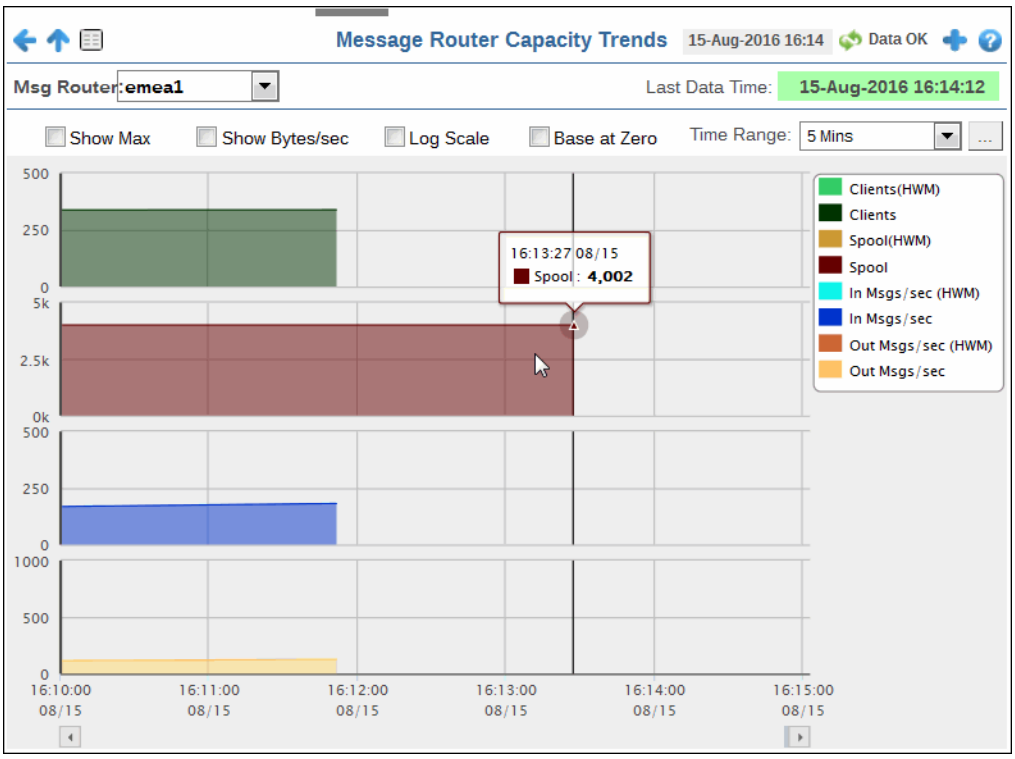
- When the display background color is (Red) the data is stale.
- The Last Data Time shows the date and time the selected message router was last updated.

Last Data Time: **15-Aug-2016 14:34:00**

If the **Last Data Time** background is:

(Red) the selected message router is offline or expired.

(Green) the selected message router is connected and receiving data.



Title Bar: Indicators and functionality might include the following:

Open the previous and upper display.

Table Navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

Filter By:
The display might include these filtering options:

Msg Router: Select the message router for which you want to view data.

Last Data Time

Last Data Time: 15-Aug-2016 14:34:00

The date and time the selected message router was last updated.

Red indicates the selected message router is offline or expired.

Green indicates the selected message router is connected and receiving data.

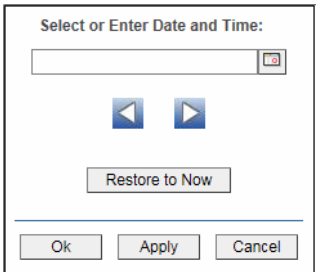
Trend Graphs
Traces the sum of process metrics for the selected message router.

- **Clients (HWM)**: The highest number of clients connected to the message router on a particular day in the past 30 days.
- **Clients (Max):** The maximum number of clients allowed to connect to the message router. This option only displays when the **Show Max** check box is selected.
- **Clients**: The current number of clients connected to the message router.
- **Spool (HWM)**: The most megabytes used by messages spools on the message router on a particular day in the past 30 days.
- **Spool (Max):** The maximum number of megabytes allowed to be used by message spools on the message router. This option only displays when the **Show Max** check box is selected.
- **Spool**: The current spool usage, in megabytes, on the message router.
- **In Msgs/sec (HWM)**: The current number of messages coming into the message router per second.
- **In Msgs/sec (Max):** The maximum number of messages (per second) allowed to come into the message router. This option only displays when the **Show Max** check box is selected.
- **In Msgs/sec**: The rate of incoming messages into the client.
- **In Bytes/sec (HWM):**The highest number of bytes coming into the message router per second on a particular day in the past 30 days. This option only displays when the **Show Bytes/sec** check box is selected.
- **In Bytes/sec (Max):** The maximum number of bytes (per second) allowed to come into the message router. This option only displays when the **Show Max** and **Show Bytes/sec** check boxes are selected.
- **In Bytes/sec:** The current number of bytes coming into the message router per second. This option only displays when the **Show Bytes/sec** check box is selected.
- **Out Msgs/sec (HWM)**: The highest number of messages going out of the message router per second on a particular day in the past 30 days.
- **Out Msgs/sec (Max)**: The maximum number of messages (per second) allowed to go out of the message router. This option only displays when the **Show Max** check box is selected.
- **Out Msgs/sec**: The current number of messages going out of the message router per second.
- **Out Bytes/sec (HWM)**: The highest number of bytes going out of the message router per second on a particular day in the past 30 days. This option only displays when the **Show Bytes/sec** check box is selected.
- **Out Bytes/sec (Max):** The maximum number of messages allowed to go out of the message router. This option only displays when the **Show Max** and **Show Bytes/sec** check boxes are selected.
- **Out Bytes/sec**: The current number of bytes going out of the message router per second. This option only displays when the **Show Bytes/sec** check box is selected.

Show Max	Selecting this toggle changes metrics using **HWM** (high water mark) to **Max** (maximum value). For example, **Clients (HWM)** becomes **Clients (Max)** and the values in the graph are updated accordingly.
Show Bytes/sec	Selecting this toggle changes metrics using **Messages/sec** to **Bytes/sec**. For example, **In Msgs/sec** becomes **In Bytes/sec** and the values in the graph are updated accordingly.
Log Scale	Select to enable a logarithmic scale. Use **Log Scale** to see usage correlations for data with a wide range of values. For example, if a minority of your data is on a scale of tens, and a majority of your data is on a scale of thousands, the minority of your data is typically not visible in non-log scale graphs. **Log Scale** makes data on both scales visible by applying logarithmic values rather than actual values to the data.

Base at Zero Select to use zero (**0**) as the Y axis minimum for all graph traces.

Time Range Select a time range from the drop down menu varying from **2 Minutes** to **Last 7 Days**, or display **All Data**. To specify a time range, click Calendar ...



By default, the time range end point is the current time. To change the time range end point, click Calendar ... and select a date and time from the calendar or enter the date and time in the text field using the following format: **MMM dd, YYYY HH:MM**. For example, **Aug 21, 2011 12:24 PM**.

Use the navigation arrows to move forward or backward one time period. NOTE: The time period is determined by your selection from the **Time Range** drop-down menu.

Click **Restore to Now** to reset the time range end point to the current time.

Syslog

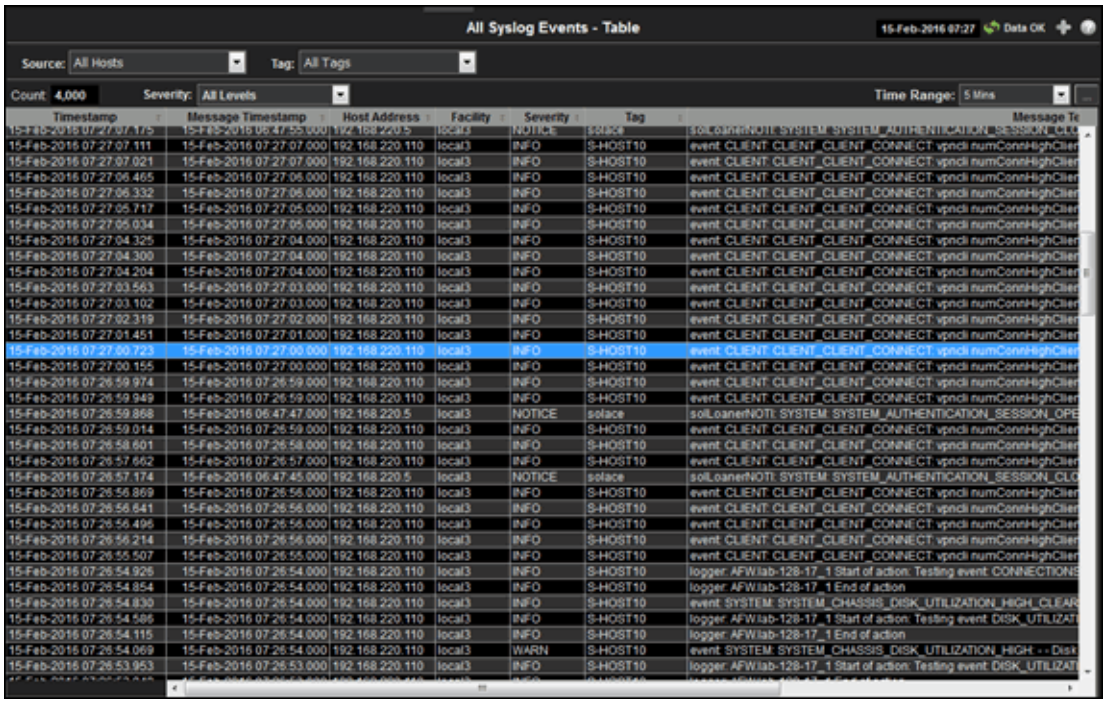
The display in this View provides a tabular list of all Syslog events:

- "All Syslog Events Table" on page 111: View all Syslog events for all your Solace message routers.

All Syslog Events Table

This table lists all Syslog events collected from one or all Solace message routers. Each row in the table is a different message. Filter messages per single Solace message router or all message routers (choose **All Hosts** from the **Source** drop-down menu), a single tag or **All Tags**, a single severity level or all levels (choose **All Levels** from the **Severity** drop-down menu), and specify a **Time Range**.

Click a column header to sort column data in numerical, alphabetical or chronological order.



Title Bar: Indicators and functionality might include the following:

Open the previous and upper display.

Table Navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

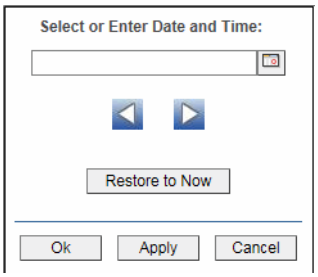
Open the online help page for this display.

Source: Select the host for which you want to view data, or **All Hosts**.

Tag: Select the message tag for which you want to view data, or **All Tags**.

Severity: Select the message severity level for which you want to view data, or **All Levels**.

Time Range: Select a time range from the drop down menu varying from **2 Minutes** to **Last 7 Days**, or display **All Data**. To specify a time range, click Calendar ...



By default, the time range end point is the current time. To change the time range end point, click Calendar ... and select a date and time from the calendar or enter the date and time in the text field using the following format: **MMM dd, YYYY HH:MM**. For example, **Aug 21, 2011 12:24 PM**.

Use the navigation arrows to move forward or backward one time period. NOTE: The time period is determined by your selection from the **Time Range** drop-down menu.

Click **Restore to Now** to reset the time range end point to the current time.

Timestamp The date and time the row data was last updated.

Message Timestamp The date and time the message was sent.

Host Address The host IP address. Refer to Solace documentation for more information.

Facility The message facility code. Refer to Solace documentation for more information.

Severity The message severity level. Refer to Solace documentation for more information.

- **INFO**
- **NOTICE**
- **NOTICE or higher**
- **WARN**
- **WARN or higher**
- **ERROR**
- **ERROR or higher**
- **CRITICAL**
- **ALERT**
- **EMERGENCY**

Tag The host name. Refer to Solace documentation for more information.

Message Text The content of the message.

Alert Views

These displays present detailed information about all alerts that have occurred in your RTView Enterprise Monitor system (all Owners and all Areas). The type of alerts that appear in these displays depends on the Solution Packages installed on your RTView Enterprise Monitor system. Displays in this View are:

- "Alert Detail Table," next: Shows current alert data. Use this time-ordered tabular view to track, manage and assign alerts.

Alert Detail Table

Use this display to track and manage all alerts that have occurred in the system, add comments, acknowledge or assign Owners to alerts.

Each row in the table is a different active alert. Select one or more rows, right-click and choose **Alert** to see all actions that you can perform on the selected alert(s). Choose **Alert / Set Filter Field** to apply the selected cell data to the **Field Filter** and **Search Text** fields. Or enter filter criteria directly in the **Field Filter** and **Search Text** fields. Click **Clear** to clear the **Field Filter** and **Search Text** fields.

Click a column heading to sort the table on that column data.

If the RTVMGR Solution Package and the RTVRULES Solution Package (which come with RTView Enterprise Monitor) are installed on your system you might see the following alert types for RTView Servers (Data Servers, Display Servers and Historian Servers).

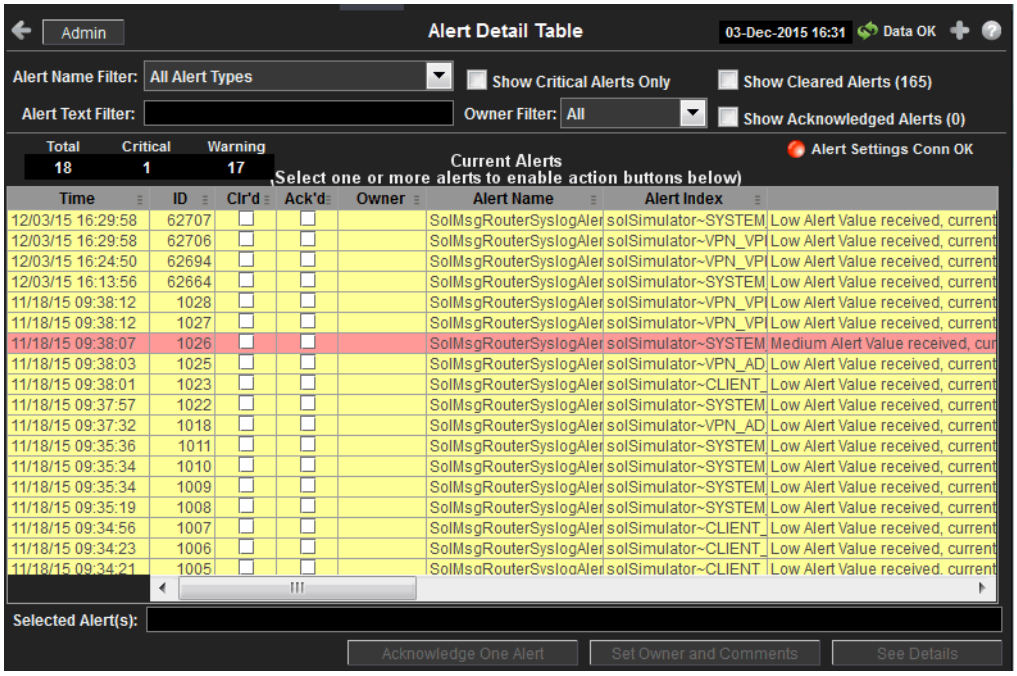
RTVMGR Solution Package Alert Types

JvmCpuPercentHigh	The percent JVM CPU usage exceeded the specified threshold.
JvJvmGcDutyCycleHigh	The JVM garbage collection contains an item that exceeded the specified duty cycle threshold (the percent of time spent in Garbage Collection).
JvmMemoryUsedAfterGCHigh	The percentage of the memory used after garbage collection exceeded the specified threshold.
JvmMemoryUsedHigh	The percent JVM memory used exceeded the specified threshold.
JvmNotConnected	The JVM is not connected.
JvmStaleData	The JVM stopped receiving data.
TomcatAccessRateHigh	The Access Rate of a Tomcat application deployed on a Tomcat server exceeded the specified threshold.
TomcatActiveSessionsHigh	The number of active Tomcat Server sessions exceeded the specified threshold.
TomcatAppAccessRateHigh	The application deployed on a Tomcat Server exceeded the specified threshold.
TomcatAppActiveSessionsHigh	The number of active Tomcat application sessions exceeded the specified threshold.

RTVRULES Solution Package Alert Types

RtvEmServiceAlert	This discrete alert is generated when a Service has one or more alerts on any associated CIs.
RtvEmServiceAlertImpactHigh	This limits alert is generated when a Service has an Alert Impact value that exceeds the specified threshold on any associated CI.

Optionally, you can use the **$rtvUserShowDualTables** substitution to add a table that lists alerts owned by the logged in user.



Title Bar: Indicators and functionality might include the following:

Open the previous and upper display.

Table Navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

The row color indicates the following:

Row Color Code:
Tables with colored rows indicate the following:

Red indicates that one or more alerts exceeded their ALARM LEVEL threshold in the table row.

Yellow indicates that one or more alerts exceeded their WARNING LEVEL threshold in the table row.

Green indicates that no alerts exceeded their WARNING or ALARM LEVEL threshold in the table row.

Gray indicates that the alert engine that is hosting the alert is not connected, not enabled or not initialized. When you select a gray row the **Own**, **Suppress**, **Unsuppress**, **Close**, **Annotate**, **Options** and **Details** options are disabled.

Fields and Data
This display includes:

Field Filter Select a table column from the drop-down menu to perform a search in: **Alert Name**, **Alert Text**, **Alert Class**, **Service**, **CI**, **Closed Reason**, **Closed**, **CompId**, **Count**, **First Occ**, **ID**, **Last Occ**, **Owner**, **Primary Service**, **Sup**, **TicketGroup**, **TicketID**.

Filters limit display content and drop-down menu selections to only those items that pass through the selected filter's criteria. If no items match the filter, you might have zero search results (an empty table).

Clear Clears the **Field Filter** and **Search Text** entries.

Search Text Enter the (case-sensitive) string to search for in the selected **Field Filter.**

CMDB Filter Shows the selected Owner, Area, Group, Service and Environment filters. By default, all components of the CMDB (*) are included in the search.

These **CMDB Filter** fields are populated when you click Open Alerts Table , which is accessible from the **Multi Area Service Views** displays, to open the **Alerts Table** in a new window. The filters selected in the **All Management Areas** and **Multi Area Service Views** displays are applied to the **Alerts Table** (that opens in the new window). NOTE: When you use the navigation tree (in the left panel) to open the **Alerts Table** display, the **Environment** filter is applied to the display if it has a value other than ***** (asterisk).

Clear CMDB Filter Clears all of the values in the **CMDB Filter** (**Owner**, **Area**, **Group**, **Service** and **Environment** filters). NOTE: This action is not applied to any other display.

RegEx Toggles the **Search Text** field to accept Regular Expressions for filtering.

All Click to show all alerts in the table: **Open** and **Closed** alerts.

Open Click to only show **Open** alerts in the table.

Closed Click to only show **Closed** alerts in the table.

Owner Filter Select the alert **Owner** to show alerts for in the table.

- **All** Shows alerts for all Owners in the table: **Not Owned** and **Owned By Me** alerts.
- **Not Owned** Shows only alerts without Owners in the table.
- **Owned By Me** Shows only alerts for the current user in the table.

Alert Settings Conn OK The Alert Server connection state:
Disconnected.
Connected.

Total **X/Y** where **X** is the total number of alerts in the table with all selected filters applied. **Y** is the number of alerts in the table with only the **CMDB** and **Cleared** filters applied.

Critical Check to show alerts in the table that are currently in a critical state. NOTE: You must check **Critical** to see alerts that are in a critical state.

X/Y where **X** is the total number of critical alerts in the table with all selected filters applied. **Y** is the number of alerts in the table with only the **CMDB Filter** and **Cleared** filters applied.

Warning Check to show alerts in the table that are currently in a warning state. NOTE: You must check **Warning** to see alerts that are in a warning state.

X/Y where **X** is the total number of warning alerts in the table with all selected filters applied. **Y** is the number of alerts in the table with only the **CMDB** and **Cleared** filters applied.

Suppressed Check to show alerts in the table that are suppressed. The **Suppressed** count is not impacted by the **Critical** and **Warning** filters. It is impacted only by the **CMDB Filter** and the **Owner Filter**. NOTE: You must check **Suppressed** to see Suppressed alerts in the table.

Own Click to assign an Owner for the alert. This option is only visible when logged in as one of the following roles: event, full, admin, super. This option is disabled when you select a gray row. For details, see "Configure User and Role Management" on page 44.

Suppress Click to suppress the alert. This option is only visible when logged in as one of the following roles: event, full, admin, super. This option is disabled when you select a gray row. For details, see "Configure User and Role Management" on page 44.

UnSuppress Click to unsuppress the alert. This option is only visible when logged in as one of the following roles: event, full, admin, super. This option is disabled when you select a gray row or when you select a row. For details, see "Configure User and Role Management" on page 44.

Close Click to close the alert. This option is only visible to users with Administrator privileges. This option is disabled when you select a gray row or you select a row where the Primary Service is not in the $rtvManageableCompID list for the logged in user. For details, see "Configure User and Role Management" on page 44.

Alerts Table
This table lists all active alerts for the current filters. The table is empty unless you check **Critical**, **Warning**, or both. Filter the list using the search fields and drop-down menus (in the upper portion of the display). To view details about an alert, select an alert and click **Details** (in the bottom right portion of the display) to open the **Alert Detail** dialog. To view details about the CI source of the alert, select an alert and click **Go To CI** (in the bottom right portion of the display) to open its Summary display.

	First Occ	The date and time the alert first occurred.
	Last Occ	The date and time the alert last occurred.
	Count	The number of times the alert was generated.
	Sup	When checked, the alert has been suppressed by a user.
	Owner	The named owner assigned by the administrator.
	Alert Name	The name of the alert.
	Primary Service	The name of the Service with which the alert is associated.
	CI	The CI alert source.
	Alert Text	Description of the alert.
	AlertClass	An optional alert field which can be used when integrating with other alerting systems.
	CompID	An optional alert field which can be used when integrating with other alerting systems.
	TicketID	An optional alert field which can be used when integrating with other alerting systems.
	TicketGroup	An optional alert field which can be used when integrating with other alerting systems.
Columns	**Id**	When checked, shows the **ID** column in the table.
	Closed	When checked, shows the **Closed** column in the table.
	Closed Reason	When checked, shows the **Closed Reason** column in the table.
	Alert Index	When checked, shows the **Alert Index** column in the table.

Go To CI Select an alert from the **Alerts Table**, then click **Go To CI** to view details for the selected CI in the Summary display.

Annotate Select one or more alerts from the **Alerts Table**, then click **Annotate** to open the **Set Owner and Comments** dialog and enter comments or change alert owner. This option is only visible when logged in as one of the following roles: event, full, admin, super. This option is disabled when you select a gray row or when you select a row where the Primary Service is not in the $rtvManageableCompID list for the logged in user. For details, see "Configure User and Role Management" on page 44.

- **ID** Lists the alert IDs, separated by semicolons, for the alerts selected from the **Alert Table**.
- **Source** Lists the name of the back-end Data Server reporting the alert, separated by semicolons.
- **Enter Owner** Enter the name of the owner for one or more alerts, click **Set Owner of One Alert** to assign the Owner, then click **Close**. By default, this field displays the current user name.
- **Enter Comment** Enter a comment for one or more alerts, click **Add Comment on One Alert** to apply the Comment, then click **Close**. By default, this field displays previously entered comments. The text appears in the **Comments** field for the alert.
- **Set Owner** Applies the name of the alert owner in the **Enter Owner** field for one or more alerts.
- **Add Comment** Applies the comment in the **Enter Comment** field for one or more alerts.
- **Clear Comments** Removes all comments for one or more alerts.
- **Close** Closes the dialog.

Options Select a single alert from the **Alerts Table**, then click **Options** to open the **Alert Options** dialog. This dialog is provided for customizing your own alert options. This option is disabled when you select a gray row or more than one row.

Details Select a single alert from the **Alerts Table**, then click **Details** to open the **Alert Detai**l window and view alert details. This option is disabled when you select a gray row or more than one row.

Administration

These displays enable you to set alert thresholds, observe how alerts are managed, and view internal data gathered and stored by RTView (used for troubleshooting with SL Technical Support). Displays in this View are:

- "Alert Administration" on page 119: Displays active alerts and provides interface to modify and manage alerts.
- "Alert Administration Audit" on page 124: View cached data that RTView is capturing and maintaining, and use this data use this for debugging with SL Technical Support.
- "RTView Cache Tables" on page 126: Display information about RTView Agent data servers.
- "RTView Agent Admin" on page 127: Display information about RTView Agent data servers.

Alert Administration

This section includes:

- "Tabular Alert Administration" on page 122
- "Setting Override Alerts" on page 123

Set global or override alert thresholds. Alert settings are global by default.

The table describes the global settings for all alerts on the system. To filter the alerts listed in the table, enter a string in the **Alert Filter** field and press **<enter>** or click elsewhere in the display. Filters are case sensitive and no wildcard characters are needed for partial strings. For example, if you enter Server in the **Alert Filter** field, it filters the table to show only alerts with **Server** in the name. Choose **Clear** to clear the filter.

Global Thresholds

To set a global alert, select an alert from the **Active Alert Table**. The name of the selected alert populates the **Settings for Selected Alert Name** field. Edit the **Settings for Selected Alert** and click **Save Settings** when finished.

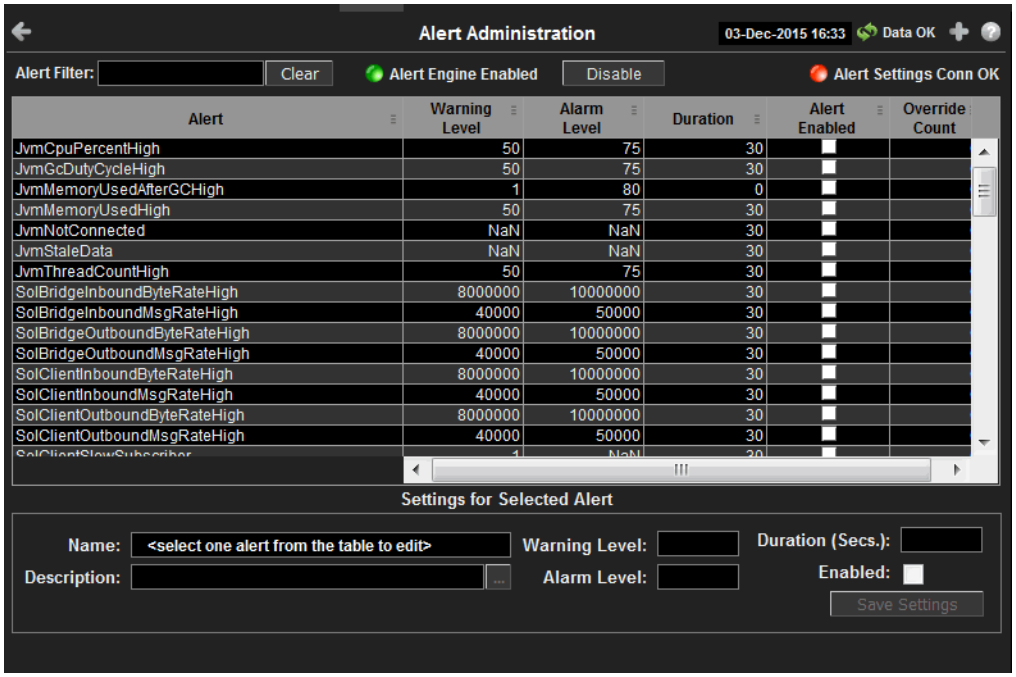
The manner in which global alerts are applied depends on the Solution Package. For example, the EMS Monitor Solution Package has queue alerts, topic alerts and server alerts. When a queue alert is applied globally, it is applied to all queues on all servers. Likewise, a server alert applies to all servers, and a topic alert applies to all topics on all servers.

Override Thresholds

Setting override alerts allows you to set thresholds for a single resource (for example, a single server). Override alerts are useful if the majority of your alerts require the same threshold setting, but there are other alerts that require a different threshold setting. For example, you might not usually be concerned with execution time at a process level, but perhaps certain processes are critical. In this case, you can apply alert thresholds to each process individually.

To apply an individual alert you Index the Monitored Instance or resource. The Index Types available are determined by the Solution Package installed. For example, the EMS Monitor package lets you set an alert for a specific *topic* on a specific *server* (such as the PerServerTopic Index option), rather than for all topics on all servers.

For details about alerts for Solace, see **Appendix A, Alert Definitions**.



Title Bar: Indicators and functionality might include the following:

Open the previous and upper display.

Table Navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

Fields and Data
This display includes:

Alert Filter	Enter the (case-sensitive) string to filter the table by the **Alert** table column value. **NOTE:** Partial strings can be used without wildcard characters. Press **<enter>** or click elsewhere in the display to apply the filter.
Clear	Clears the **Alert Filter** entry.
Alert Engine Enabled	Alerting is disabled. Alerting is enabled (by default).
Disable	Suspends all alerting.
Alert Settings Conn OK	The Alert Server connection state: Disconnected. Connected.

Active Alert Table
This table describes the global settings for all alerts on the system. Select an alert. The name of the selected alert populates the **Settings for Selected Alert Name** field (in the lower panel). Edit **Settings for Selected Alert** fields and click **Save Settings**.

NOTE: To filter the alerts shown in the table by Solution Package, use the **$rtvAlertPackageMask** substitution.

Alert	The name of the alert.
Warning Level	The global warning threshold for the selected alert. When the specified value is exceeded a warning is executed.
Alarm Level	The global alarm threshold for the selected alert. When the specified value is exceeded an alarm is executed.
Duration (Secs)	The amount of time (in seconds) that the value must be above the specified Warning Level or Alarm Level threshold before an alert is executed. **0** is for immediate execution.
Alert Enabled	When checked, the alert is enabled globally.
Override Count	The number of times thresholds for this alert have been defined individually in the **Tabular Alert Administration** display.

Settings for Selected Alert
To view or edit global settings, select an alert from the **Active Alert Table**. Edit the **Settings for Selected Alert** fields and click **Save Settings** when finished.

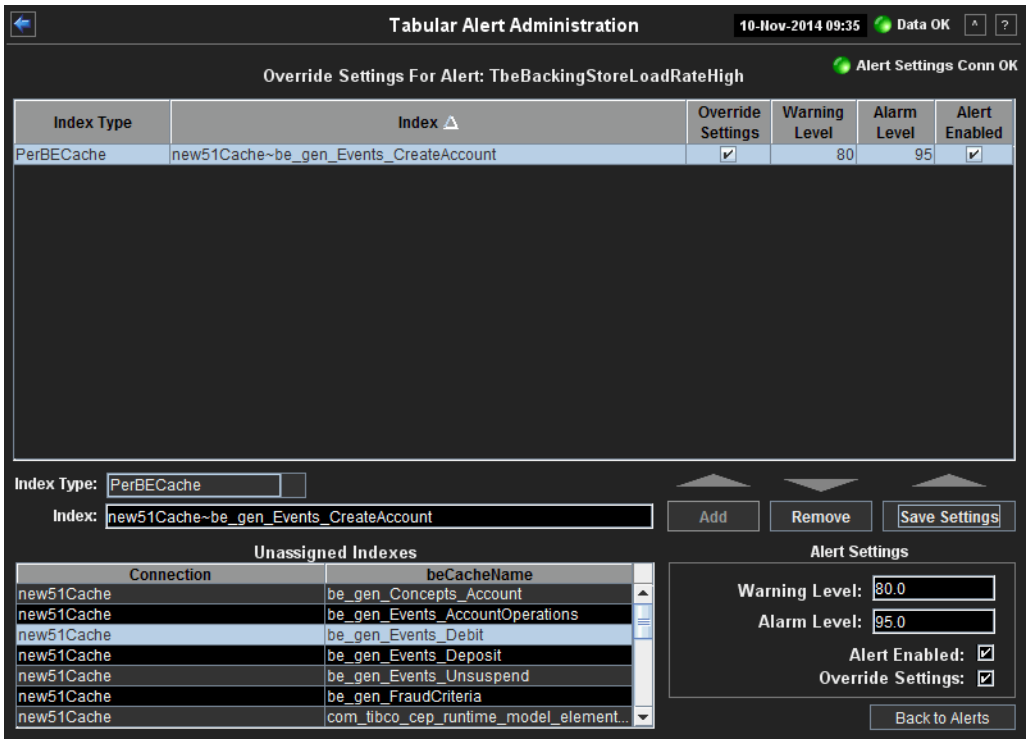
To set override alerts, click on **Override Settings** to open the **Tabular Alert Administration** display.

Name	The name of the alert selected in the **Active Alert Table**.
Description	Description of the selected alert. Click Calendar ... for more detail.
Warning Level	Set the Global warning threshold for the selected alert. When the specified value is exceeded a warning is executed. To set the warning to occur sooner, reduce the Warning Level value. To set the warning to occur later, increase the Warning Level value. **NOTE:** For low value-based alerts (such as **EmsQueuesConsumerCountLow**), to set the warning to occur sooner, increase the Warning Level value. To set the warning to occur later, reduce the Warning Level value.
Alarm Level	Set the Global alarm threshold for the selected alert. When the specified value is exceeded an alarm is executed. To set the alarm to occur sooner, reduce the Alarm Level value. To set the warning to occur later, increase the Alarm Level value. **NOTE:** For low value-based alerts (such as **EmsQueuesConsumerCountLow**), to set the alarm to occur sooner, increase the Alarm Level value. To set the alarm to occur later, reduce the Alarm Level value.
Duration	Set the amount of time (in seconds) that the value must be above the specified Warning Level or Alarm Level threshold before an alert is executed. **0** is for immediate execution. This setting is global.
Enabled	Check to enable alert globally.
Save Settings	Click to apply alert settings.
Override Settings	Click to open the **Tabular Alert Administration** display to set override alerts on the selected alert.

Tabular Alert Administration

Set override alerts (override global alert settings). This display opens when you select an alert in the **Alert Administration** display and then select **Override Settings**.

For step-by-step instructions setting thresholds for individual alerts, see **Setting Override Alerts**.



Fields and Data

This display includes:

Alert Settings Conn OK

The connection state.

- No servers are found.
- One or more servers are delivering data.

Override Settings For Alert:(name)

This table lists and describes alerts that have override settings for the selected alert. Select a row to edit alert thresholds. The selected item appears in the **Index** field. Edit settings in the **Alert Settings** fields, then click **Save** Settings.

Index Type

Select the type of alert index to show in the **Values** table. Options in this drop-down menu are populated by the type of alert selected, which are determined by the Package installed. For example, with the EMS Monitor package the following Index Types are available:

- PerServer: Alert settings are applied to a specific server.
- PerQueue: Alert settings are applied to the queue on each server that has the queue defined.
- PerServerQueue: Alert settings are applied to a single queue on a specific server.
- PerTopic: Alert settings are applied to the topic on each server that has the topic defined.
- PerServerTopic: Alert settings are applied to a single topic on a specific server.

	Index	The value of the index column.
	Override Settings	When checked, the override settings are applied.
	Alert Enabled	When checked, the alert is enabled.
Index Type	Select the index type. The index type specifies how to apply alert settings. For example, to a queue (topic or JVM, and so forth) across all servers, or to a queue on a single server. **NOTE:** Options in this drop-down menu are populated by the type of alert selected from the **Alert Administration** display. Index Types available depend on the Package installed.	
Index	The selected index column to be edited. This field is populated by the selection made in the **Unassigned Indexes** table.	
Unassigned Indexes	This table lists all possible indexes corresponding to the Index Type chosen in the drop-down list. Select a row to apply individual alert thresholds. The selected item appears in the **Index** field. Edit settings in the **Alert Settings** fields, then click **Add**.	
Add	Click to add changes made in **Alert Settings**, then click **OK** to confirm.	
Remove	Click to remove an alert selected in the **Index Alert Settings** table, then click **OK** to confirm.	
Save Settings	Click to save changes made to alert settings.	

Alert Settings
Select a topic, server or queue from the **Unassigned Indexes** table and edit the following settings.

	Warning Level	Set the warning threshold for the selected alert. When the specified value is exceeded a warning is executed. To set the warning to occur sooner, reduce the Warning Level value. To set the warning to occur later, increase the Warning Level value. **NOTE:** For low value-based alerts (such as **EmsQueuesConsumerCountLow**), to set the warning to occur sooner, increase the Warning Level value. To set the warning to occur later, reduce the Warning Level value. Click **Save Settings** to save settings.
	Alarm Level	Set the alarm threshold for the selected alert. When the specified value is exceeded an alarm is executed. To set the alarm to occur sooner, reduce the Alarm Level value. To set the warning to occur later, increase the Alarm Level value. NOTE: For low value-based alerts (such as **EmsQueuesConsumerCountLow**), to set the alarm to occur sooner, increase the Alarm Level value. To set the alarm to occur later, reduce the Alarm Level value. Click **Save Settings** to save settings.
	Alert Enabled	Check to enable the alert, then click **Save Settings**.
	Override Settings	Check to enable override global setting, then click **Save Settings**.
Back to Alerts	Returns to the **Administration** - **Alert Administration** display.	

Setting Override Alerts

Perform the following steps to set an override alert. Index Types available depend on the Solution Package installed. In this example, we use the EMS Monitor Package to illustrate.

NOTE: To turn on an alert, both Alert Enabled and Levels Enabled must be selected.

To turn on/off, change threshold settings, enable/disable or remove an alert on a single resource:

1. In the **Alert Administration** display, select an alert in the **Active Alert Table** and click **Edit Index Levels**. The **Tabular Alert Administration** display opens.

2. In the **Tabular Alert Administration** display, from the **Index Type** drop-down menu, select the Index type (options are populated by the type of alert you previously selected). For example, with the EMS Monitor package, select PerServerQueue, PerServerTopic or PerServer. **NOTE:** If you select PerServerQueue or PerServerTopic, the alert settings are applied to the queue or topic on a single server.

3. In the **Values** table, select the server to apply alert settings and click **Add**. In a few moments the server appears in the **Index Alert Settings** table.

4. In the **Index Alert Settings** table select the server.

5. In the **Alert Settings** panel (lower right), if needed, modify the **Warning Level** and **Alarm Level** settings.

6. In the **Alert Settings** panel, set the following as appropriate.

   To turn on the alert for this index with the given thresholds:

   Alert Enabled Select this option.

   Levels Enabled Select this option.

   To turn off the alert for only this index (global alert thresholds will no longer apply to this index):

   Alert Enabled Deselect this option.

   Levels Enabled Select this option.

   To no longer evaluate this indexed alert and revert to global settings (or, optionally, Remove it if it is never to be used again):

   Alert Enabled Not used.

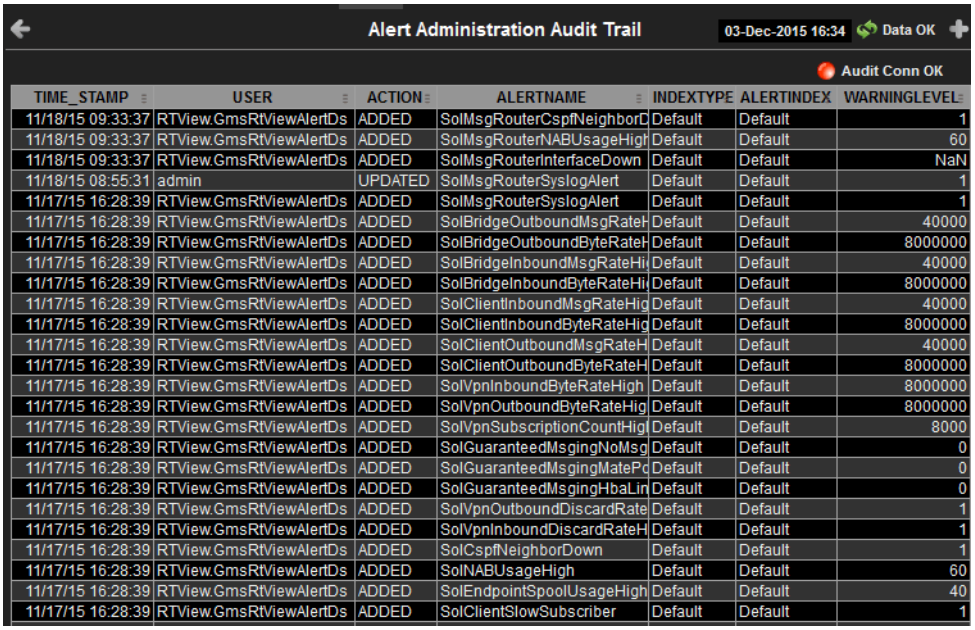
   Levels Enabled Deselect this option.

7. Click **Save Settings**. In a few moments the modifications are updated in the **Index Alert Settings** table.

Alert Administration Audit

View alert management details such as alert threshold modifications.

Each table row is a single modification made to an alert. To view modifications for a single alert in a group, click Sort to order the ALERTNAME column.



TIME_STAMP	USER	ACTION	ALERTNAME	INDEXTYPE	ALERTINDEX	WARNINGLEVEL
11/18/15 09:33:37	RTView.GmsRtViewAlertDs	ADDED	SolMsgRouterCspfNeighborD	Default	Default	1
11/18/15 09:33:37	RTView.GmsRtViewAlertDs	ADDED	SolMsgRouterNABUsageHigh	Default	Default	60
11/18/15 09:33:37	RTView.GmsRtViewAlertDs	ADDED	SolMsgRouterInterfaceDown	Default	Default	NaN
11/18/15 08:55:31	admin	UPDATED	SolMsgRouterSyslogAlert	Default	Default	1
11/17/15 16:28:39	RTView.GmsRtViewAlertDs	ADDED	SolMsgRouterSyslogAlert	Default	Default	1
11/17/15 16:28:39	RTView.GmsRtViewAlertDs	ADDED	SolBridgeOutboundMsgRateH	Default	Default	40000
11/17/15 16:28:39	RTView.GmsRtViewAlertDs	ADDED	SolBridgeOutboundByteRateH	Default	Default	8000000
11/17/15 16:28:39	RTView.GmsRtViewAlertDs	ADDED	SolBridgeInboundMsgRateHi	Default	Default	40000
11/17/15 16:28:39	RTView.GmsRtViewAlertDs	ADDED	SolBridgeInboundByteRateHi	Default	Default	8000000
11/17/15 16:28:39	RTView.GmsRtViewAlertDs	ADDED	SolClientInboundMsgRateHig	Default	Default	40000
11/17/15 16:28:39	RTView.GmsRtViewAlertDs	ADDED	SolClientInboundByteRateHig	Default	Default	8000000
11/17/15 16:28:39	RTView.GmsRtViewAlertDs	ADDED	SolClientOutboundMsgRateH	Default	Default	40000
11/17/15 16:28:39	RTView.GmsRtViewAlertDs	ADDED	SolClientOutboundByteRateH	Default	Default	8000000
11/17/15 16:28:39	RTView.GmsRtViewAlertDs	ADDED	SolVpnInboundByteRateHigh	Default	Default	8000000
11/17/15 16:28:39	RTView.GmsRtViewAlertDs	ADDED	SolVpnOutboundByteRateHig	Default	Default	8000000
11/17/15 16:28:39	RTView.GmsRtViewAlertDs	ADDED	SolVpnSubscriptionCountHigh	Default	Default	8000
11/17/15 16:28:39	RTView.GmsRtViewAlertDs	ADDED	SolGuaranteedMsgingNoMsg	Default	Default	0
11/17/15 16:28:39	RTView.GmsRtViewAlertDs	ADDED	SolGuaranteedMsgingMatePc	Default	Default	0
11/17/15 16:28:39	RTView.GmsRtViewAlertDs	ADDED	SolGuaranteedMsgingHbaLin	Default	Default	0
11/17/15 16:28:39	RTView.GmsRtViewAlertDs	ADDED	SolVpnOutboundDiscardRate	Default	Default	1
11/17/15 16:28:39	RTView.GmsRtViewAlertDs	ADDED	SolVpnInboundDiscardRateH	Default	Default	1
11/17/15 16:28:39	RTView.GmsRtViewAlertDs	ADDED	SolCspfNeighborDown	Default	Default	1
11/17/15 16:28:39	RTView.GmsRtViewAlertDs	ADDED	SolNABUsageHigh	Default	Default	60
11/17/15 16:28:39	RTView.GmsRtViewAlertDs	ADDED	SolEndpointSpoolUsageHigh	Default	Default	40
11/17/15 16:28:39	RTView.GmsRtViewAlertDs	ADDED	SolClientSlowSubscriber	Default	Default	1

Title Bar: Indicators and functionality might include the following:

Open the previous and upper display.

Table Navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

Fields and Data
This display includes:

Audit Conn OK	The Alert Server connection state. Disconnected. Connected.
TIME_STAMP	The date and time of the modification.
USER	The user name of the administrator who made the modification.
ACTION	The type of modification made to the alert, such as **UPDATED**.
ALERTNAME	The name of the alert modified.
INDEXTYPE	The type of alert Index. Index Type refers to the manner in which alert settings are applied and vary among Packages. For example, JVMs have a PerJvm Index Type and the EMS Monitor package PerServer, PerTopic and PerQueue Index Types, which apply alerts to servers, topics and queues, respectively.
ALERTINDEX	The index of the alert that identifies its source.

WARNINGLEVEL The warning threshold value for the alert at the time this modification was made, as indicated in the **TIME_STAMP** column.

The warning level is a threshold that, when exceeded, a warning is executed.

ALARMLEVEL The alarm threshold value for the alert at the time this modification was made, as indicated in the **TIME_STAMP** column.

The alarm level is a threshold that, when exceeded, an alarm is executed.

DURATION The duration value for the alert at the time this modification was made, as indicated in the **TIME_STAMP** column.

The alert duration is the amount of time (in seconds) that a value must be above the specified Warning Level or Alarm Level threshold before an alert is executed. **0** is for immediate execution.

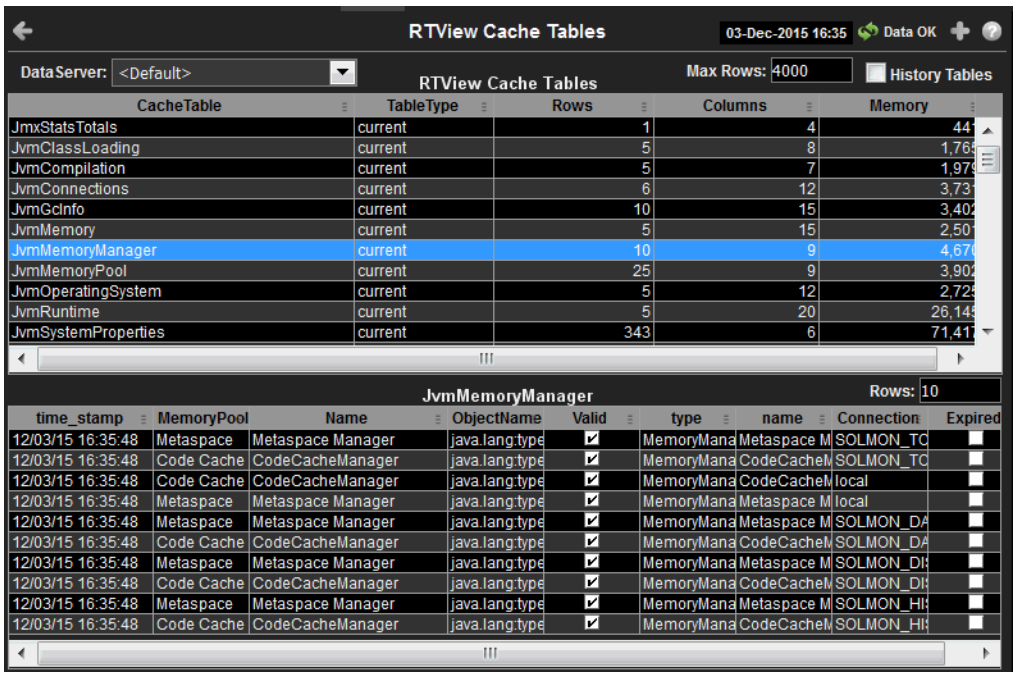
ENABLED When checked, indicates the alert was enabled at the time this modification was made, as indicated in the **TIME_STAMP** column.

USEINDEX When checked, indicates the alert override was enabled at the time this modification was made, as indicated in the **TIME_STAMP** column. For details about alert overrides, see **Alert Administration**.

RTView Cache Tables

View data that RTView is capturing and maintaining. Drill down and view details of RTView Cache Tables. Use this data for debugging. This display is typically used for troubleshooting with Technical Support.

Choose a cache table from the upper table to see cached data.



Title Bar: Indicators and functionality might include the following:

Open the previous and upper display.

Table Navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

DataServer	Select a data server from the drop down menu.
Max Rows	Enter the maximum number of rows to display in RTView Cache Tables.
History Tables	Select to include all defined history tables in RTView Cache Tables.

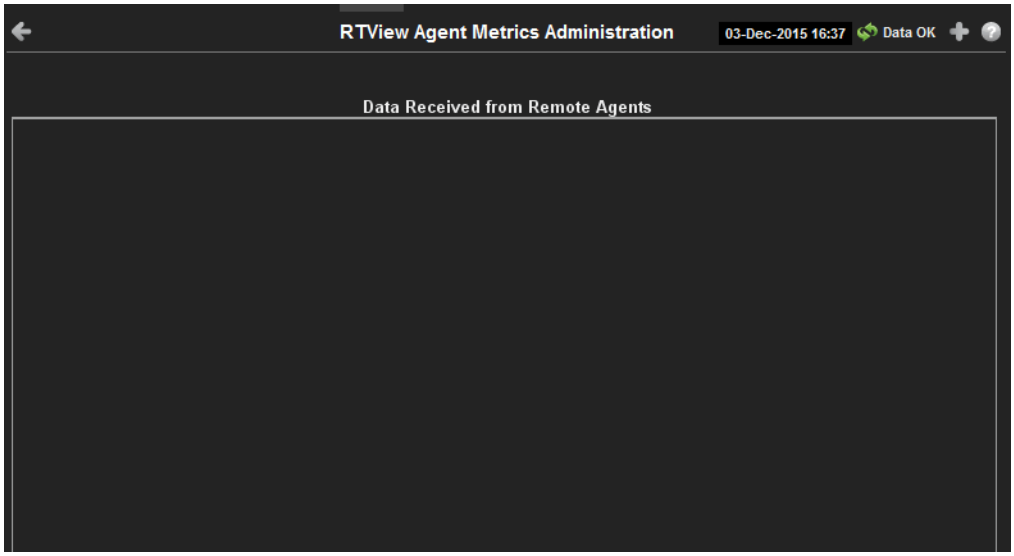
RTView Cache Tables
This table lists and describes all defined RTView Cache Tables for your system. Cache tables gather Monitor data and are the source that populate the Monitor displays.

NOTE: When you click on a row in RTView Cache Tables a supplemental table will appear that gives more detail on the selected Cache Table.

CacheTable	The name of the cache table.	
TableType	The type of cache table:	
	current	Current table which shows the current values for each index.
	current_condensed	Current table with primary compaction configured.
	history	History table.
	history_condensed	History table with primary compaction configured.
Rows	Number of rows currently in the table.	
Columns	Number of columns currently in the table.	
Memory	Amount of space, in bytes, used by the table.	

RTView Agent Admin

Verify when agent metrics were last queried by the Monitor. The data in this display is predominantly used for debugging by Technical Support.



Title Bar: Indicators and functionality might include the following:

Open the previous and upper display.

Table Navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

Data Received from Remote Agents Table	
AgentName	Name of the agent.
AgentClass	Class of the agent.
Client ID	Unique client identifier
Total Rows Rcvd	Total number of rows of data received.
Rows Rcvd/sec	Number of rows of data received per second.
Last Receive Time	Last time data was received from the agent.

RTView Servers

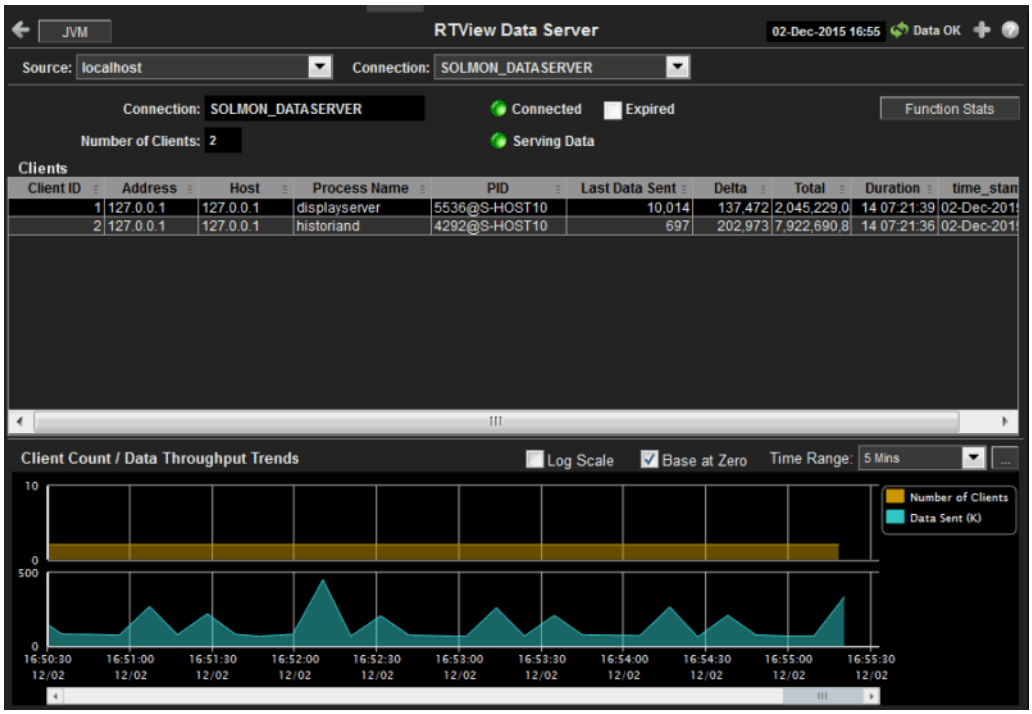
These displays enable you to monitor performance of all RTView Servers.

- "Data Server Metrics" on page 129: Shows metrics for RTView Data Servers.
- "Display Server Metrics" on page 133: Shows metrics for RTView Display Servers.
- "Historian Servers" on page 134: Shows metrics for RTView Historian Servers.
- "Tomcat Server Summary" on page 136: Shows metrics for Tomcat application sessions, including Tomcat hosting and connection details.
- "Tomcat Modules Summary" on page 139: Shows metrics for Tomcat application modules and utilization details.
- "JVM CPU/Mem Summary" on page 142: Shows Java Virtual Machine memory and CPU usage, JVM system information, application performance metrics, and input arguments for a single connection.
- "JVM Mem Pool Trends" on page 146: Shows Java Virtual Machine heap and non-heap memory usage for a single connection.
- "JVM Mem GC Trends" on page 149: Shows Java Virtual Machine garbage collection memory usage for a single connection.
- "JVM System Properties" on page 151: Shows Java Virtual Machine input arguments and system properties for a single connection.
- "Version Info" on page 152: Shows the version information of each jar used in each connected RTView application.
- "About" on page 154: Shows Monitor version information.

Data Server Metrics

Track data transfer metrics for RTView Data Servers, client count and throughput trends.

Use the available drop-down menus or right-click to filter data shown in the display.



Title Bar:
Indicators and functionality might include the following:

Open the previous and upper display.

CMDB and Table navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Cls: 3,047 The number of items in the display.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

Source	Select the type of connection to the RTView Server.
Connection	Select an RTView Server from the drop-down menu. Names can be modified in the RTView Server configuration properties file.
Connection	The connection selected from the **Connection** drop-down menu.
Number of Clients	The number of clients currently server on this Data Server.
Connected	The Data Server connection state: Disconnected. Connected.
Serving Data	The Data Server is not currently serving data. The Data Server is currently serving data.
Expired	This server has been marked as expired after no activity.

Function Stats Opens the **RTView Function Stats** display which shows detailed performance statistics for RTView functions in the selected Data Server. This button is only enabled if the RTVMGR has a JMX connection defined for the selected Data Server.

Clients
This table describes all clients on the selected server.

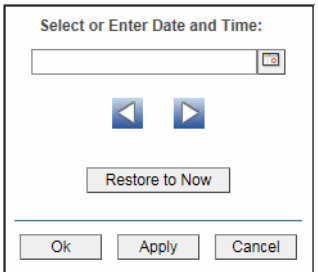
Address	The client IP address.
Client ID	The unique client identifier.
Duration	The amount of time for this client session. Format: **dd HH:MM:SS** **<days> <hours>:<minutes>:<seconds>** **For example:** **10d 08:41:38**
Host	The client host name.
Last Data Sent	The amount of data, in bytes, last sent to the client.
Delta	The amount of data, in bytes, sent since the last update.
Total	The total amount of data, in bytes, sent to the client.
TIME_STAMP	The date and time this row of data was last updated.

Client Count / Data Throughput Trends
Shows throughput metrics for all clients on the selected server.

Log Scale Enable to use a logarithmic scale for the Y axis. Use Log Scale to see usage correlations for data with a wide range of values. For example, if a minority of your data is on a scale of tens, and a majority of your data is on a scale of thousands, the minority of your data is typically not visible in non-log scale graphs. Log Scale makes data on both scales visible by applying logarithmic values rather than actual values to the data.

Base at Zero Use zero as the Y axis minimum for all graph traces.

Time Range Select a time range from the drop down menu varying from **2 Minutes** to **Last 7 Days**, or display **All Data**. To specify a time range, click Calendar ... .



By default, the time range end point is the current time. To change the time range end point, click Calendar ... and select a date and time from the calendar or enter the date and time in the text field using the following format: **MMM dd, YYYY HH:MM**. For example, **Aug 21, 2011 12:24 PM**.

Use the navigation arrows to move forward or backward one time period. NOTE: The time period is determined by your selection from the **Time Range** drop-down menu.

Click **Restore to Now** to reset the time range end point to the current time.

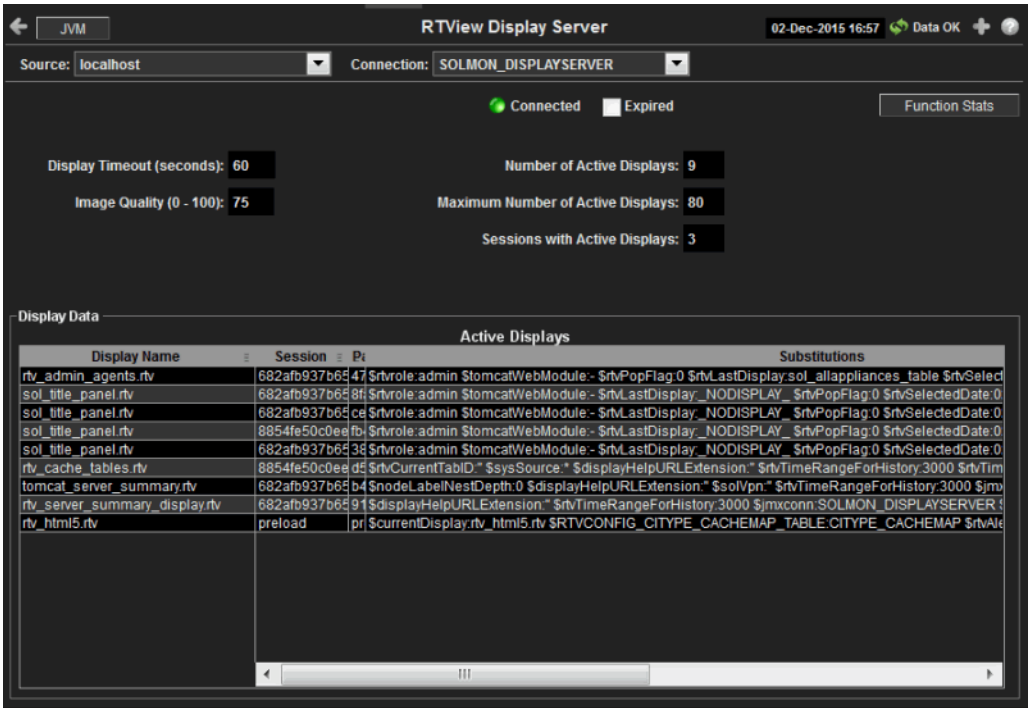
Number of Clients Traces the number of clients being served by the Data Server.

Data Sent Traces the total amount of data, in Kilobytes, sent to all clients.

Display Server Metrics

Track display utilization metrics for RTView Display Servers.

Use the available drop-down menus or right-click to filter data shown in the display.



Title Bar:
Indicators and functionality might include the following:

Open the previous and upper display.

CMDB and Table navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Cls: 3,047 The number of items in the display.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

Fields and Data
This display includes:

Source	Select the type of connection to the RTView Server.
Connection	Select an RTView Server from the drop-down menu. Names can be modified in the RTView Server configuration properties file.
Connected	The Display Server connection state: Disconnected. Connected.
Expired	This server has been marked as expired after no activity.

Function Stats	Opens the **RTView Function Stats** display which shows detailed performance statistics for RTView functions in the selected Display Server. This button is only enabled if the RTVMGR has a JMX connection defined for the selected Display Server.
Display Timeout (seconds)	The amount of time, in seconds, that a display can be kept in memory after the Display Servlet has stopped requesting it. The default is **60** seconds (to allow faster load time when switching between displays).
Image Quality (0-100)	A value between **0** and **100**, which controls the quality of the generated images. If the value is **100**, the Display Server outputs the highest quality image with the lowest compression. If the value is **0**, the Display Server outputs the lowest quality image using the highest compression. The default is **75**.
Number of Active Displays	The total number of displays currently being viewed by a user.
Maximum Number of Active Displays	The maximum number of displays kept in memory. The default is **20** (to optimize memory used by the Display Server).
Sessions with Active Displays	Number of clients accessing the Display Server.

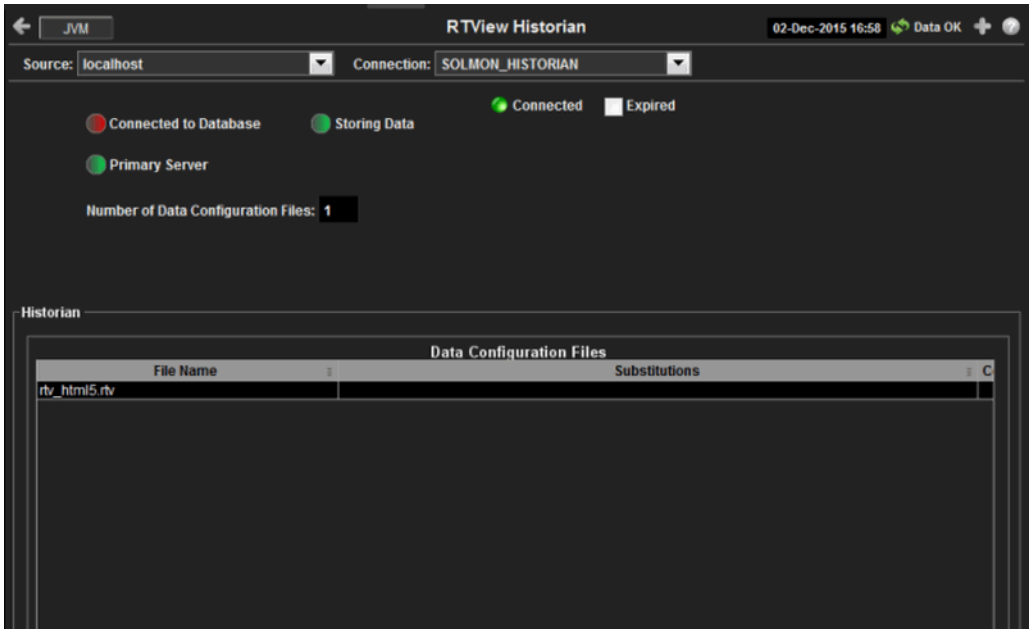
Display Data / Active Displays

Display Name	The name of the currently open display.
Session	A unique string identifier assigned to each session.
Panel ID	A unique string identifier assigned to each panel. The Display Server loads each display requested by each client into a panel. This ID can be useful in troubleshooting.
Substitutions	Lists the substitutions used for the display.
Last Ref	The amount of time that has elapsed since the display was last requested by a client.
ID	The client ID.
Preloaded	When checked, indicates that the display (**.rtv**) file is configured in the **DISPLAYSERVER.ini** file to be preloaded. The **history_config** option is used to configure display preloading. Preloading a display makes data immediately available. Preloaded displays are not unloaded unless the Display Server is restarted or the display cache is cleared via JMX. This option can be used multiple times to specify multiple displays to preload.

Historian Servers

Track the status of RTView Historian Servers and data configuration file usage. View the caches that are archived by the Historian application, substitution variables associated with the history cache configuration file, as well as the history cache status. You can also stop and start the Historian, and purge data.

Use the available drop-down menus or right-click to filter data shown in the display.



Title Bar:
Indicators and functionality might include the following:

Open the previous and upper display.

CMDB and Table navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Cls: 3,047 The number of items in the display.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

Fields and Data
This display includes:

Source	Select the type of connection to the RTView Server.
Connection	Select an RTView Server from the drop-down menu. Names can be modified in the RTView Server configuration properties file.
Connected	The Historian Server connection state: Disconnected. Connected.
Expired	This server has been marked as expired after no activity.
Connected to Database	The Historian Server database connection state: Disconnected. Connected.

Primary Server

When green, indicates that this Historian, when used within a group of Historians, is the primary group member. If the primary member fails or shuts down, the standby member with the highest priority becomes the primary group member. When red, indicates that the Historian is a secondary server.

The Historian Server member state:

- The Historian Server is a secondary group member.
- This Historian is the primary group member.

Number of Data Configuration Files

The number of configuration files that are used by the history cache.

Historian / Data Configuration Files

File Name The name of the history cache configuration file.

Substitutions Lists the substitutions specified in the history cache configuration file.

Tomcat Server Summary

Track the performance of one Tomcat Server and get Tomcat hosting and connection details. You can drill down to this display from the Servers table for detailed information and historical trends for a specific server. he trends include Active Sessions, Requests per Sec, and Process Time.

Title Bar:
Indicators and functionality might include the following:

Open the previous and upper display.
CMDB and Table navigate to displays commonly accessed from this display.
19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.
Cls: 3,047 The number of items in the display.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.
Open the **Alert Views - RTView Alerts Table** display.
Open an instance of this display in a new window.
Open the online help page for this display.

Fields and Data
This display includes:

Source	Select the host where the Tomcat Server is running.
Connection	Select a Tomcat Server from the drop-down menu.
Connected	The Tomcat Server connection state: Disconnected. Connected.
Expired	When checked, this server is expired due to inactivity.
Host Name	The name of the host where the application resides.
App Base	The directory in which Tomcat modules are installed.
Auto Deploy	When checked, indicates that the Tomcat option, automatic application deployment, is enabled. NOTE: This Tomcat option is set using the **autoDeploy** property in the **server.xml** file, located in the Tomcat **conf** directory. **autoDeploy=true** enables the option.
Deploy On Startup	When checked, indicates that the option to deploy the application on Tomcat startup is enabled. NOTE: This Tomcat option is set using the **deployOnStartup** property in the **server.xml** file, located in the Tomcat **conf** directory. When enabled (**deployOnStartup=true**), applications from the host are automatically deployed.

Connectors
This table shows Tomcat application connection information.

Protocol	The protocol used by the Tomcat application on the host.
Port	The port number used by the Tomcat application on the host.
RedirectPort	The redirect port number used by the Tomcat application on the host.
Secure	When checked, specifies that the Tomcat application uses a secure connection on the host.

Current Statistics / Totals

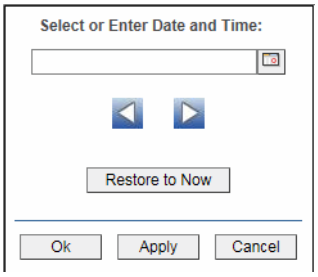
Active Sessions	The number of clients currently in session with the servlet.
Sessions	The total number of client sessions since the server was started.
Page Access / sec	The number of times pages are accessed, per second.
Accesses	The total number of page accesses since the server was started.
Cache Hits / sec	The number of times the cache is accessed, per second.
Requests / sec	The number of requests received, per second.
Requests	The total number of requests since the server was started.
Bytes Rcvd / sec	The number of bytes received, per second.
Bytes Rcvd (Kb)	The number of kilobytes received since the server was started.
Bytes Sent / sec	The number of bytes sent, per second.
Bytes Sent (Kb)	The total number of kilobytes sent since the server was started.
Process Time	The amount of time, in milliseconds, for the servlet to process client requests.

Session / Request / Process Trends
Shows metrics for the selected server.

Log Scale Select to enable a logarithmic scale. Use Log Scale to see usage correlations for data with a wide range of values. For example, if a minority of your data is on a scale of tens, and a majority of your data is on a scale of thousands, the minority of your data is typically not visible in non-log scale graphs. Log Scale makes data on both scales visible by applying logarithmic values rather than actual values to the data.

Base at Zero Use zero as the Y axis minimum for all graph traces.

Time Range Select a time range from the drop down menu varying from **2 Minutes** to **Last 7 Days**, or display **All Data**. To specify a time range, click Calendar ...



By default, the time range end point is the current time. To change the time range end point, click Calendar ... and select a date and time from the calendar or enter the date and time in the text field using the following format: **MMM dd, YYYY HH:MM**. For example, **Aug 21, 2011 12:24 PM**.

Use the navigation arrows to move forward or backward one time period. NOTE: The time period is determined by your selection from the **Time Range** drop-down menu.

Click **Restore to Now** to reset the time range end point to the current time.

Active Sessions Traces the number of currently active client sessions.

Requests /sec Traces the number of requests received, per second.

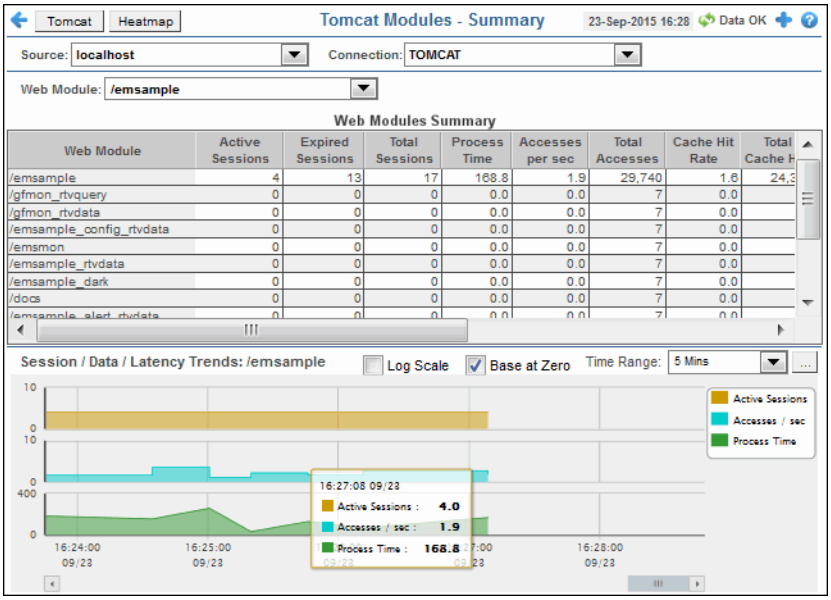
Process Time Traces the average amount of time, in milliseconds, to process requests.

Tomcat Modules Summary

Track the performance of all web application modules in a server and view utilization details. The table summarizes the sessions, accesses, cache hit and so forth, for all installed web modules. Each row in the table is a different web application module. The row color for inactive modules is dark red. Select a web application module to view metrics in the trend graph.

Use this data to verify response times of your Web application modules.

Use the available drop-down menus or right-click to filter data shown in the display.



Title Bar:
Indicators and functionality might include the following:

Open the previous and upper display.

CMDB and Table navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Cls: 3,047 The number of items in the display.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

Fields and Data
This display includes:

Source	Select the host where the Tomcat Server is running.
Connection	Select a Tomcat Server from the drop-down menu. This menu is populated by the selected Source.
Web Module	Select a Web module from the drop-down menu. This menu is populated by the selected Connection. The Web Module you select populates the trend graphs.

Web Module Summary

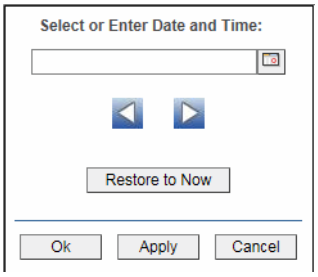
Web Module	The name of the Web module.
Sessions Active	The number of currently active client sessions.
Sessions Total	The total number of client sessions since the application was started.
Sessions Expired	The total number of client sessions that expired since the application was started.
Accesses per sec	The number of times pages are accessed, per second.
Accesses Total	The total number of times pages have been accessed since the application was started.
Bytes Rcvd per sec	The number of bytes received per second.
Bytes Rcvd Total	The total number of bytes received since the application was started.
Bytes Sent per sec	The number of bytes sent per second.
Bytes Sent Total	The total number of bytes sent since the application was started.
Cache Hit Rate	The number of times the cache is accessed, per second.
Requests per sec	The number of requests received, per second.
Requests Total	The total number of requests received since the application was started.
Process Time	The average amount of time, in milliseconds, to process requests.
Error Count	The number of errors occurred since the application was started.
appBase	The directory in which Tomcat is installed.
Expired	When checked, this connection is expired due to inactivity.
time_stamp	The date and time this row of data was last updated. Format: **MM/DD/YY HH:MM:SS** **<month>/ <day>/<year> <hours>:<minutes>:<seconds>**

Session/Data/Latency Trends
Shows metrics for the selected Web module. The Web module can be selected from the **Web Module** drop-down menu or the **Web Modules Summary** table.

Log Scale Select to enable a logarithmic scale. Use Log Scale to see usage correlations for data with a wide range of values. For example, if a minority of your data is on a scale of tens, and a majority of your data is on a scale of thousands, the minority of your data is typically not visible in non-log scale graphs. Log Scale makes data on both scales visible by applying logarithmic values rather than actual values to the data.

Base at Zero Use zero as the Y axis minimum for all graph traces.

Time Range Select a time range from the drop down menu varying from **2 Minutes** to **Last 7 Days**, or display **All Data**. To specify a time range, click Calendar ...



By default, the time range end point is the current time. To change the time range end point, click Calendar ... and select a date and time from the calendar or enter the date and time in the text field using the following format: **MMM dd, YYYY HH:MM**. For example, **Aug 21, 2011 12:24 PM**.

Use the navigation arrows to move forward or backward one time period. NOTE: The time period is determined by your selection from the **Time Range** drop-down menu.

Click **Restore to Now** to reset the time range end point to the current time.

Active Sessions Traces the number of currently active client sessions.

Accesses / sec Traces the number of times pages are accessed, per second.

Process Time Traces the average amount of time, in milliseconds, to process requests.

JVM CPU / Mem Summary

Track JVM memory and CPU usage, get JVM system information, application performance metrics, and input arguments for a single connection. Verify whether the memory usage has reached a plateau. Or, if usage is getting close to the limit, determine whether to allocate more memory.

Use the available drop-down menus or right-click to filter data shown in the display.

Title Bar:
Indicators and functionality might include the following:

Open the previous and upper display.

CMDB and Table navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Cls: 3,047 The number of items in the display.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

Fields and Data
This display includes:

Source Select the type of connection to the RTView Server.

Connection Select an RTView Server from the drop-down menu. Names can be modified in the RTView Server configuration properties file.

Operating System
Displays data pertaining to the operating system running on the host on which the JVM resides.

Connected	The data connection state: Disconnected. Connected.
Expired	When checked, this server is expired due to inactivity.
Operating System	The name of the operating system running on the host on which the JVM resides.
OS Version	The operating system version.
Architecture	The ISA used by the processor.
Available Processors	The total number of processors available to the JVM.

Runtime

Process Name	Name of the process.
Start Time	The date and time that the application started running.
Up Time	The amount of time the application has been running, in the following format: **0d 00:00** **<days>d <hours>:<minutes>:<seconds>** For example: **10d 08:41:38**
JVM CPU %	The amount of CPU usage by the JVM, in percent.
Live Threads	The total number of live threads.
Daemon Threads	The total number of live daemon threads.
Peak Threads	The total number of peak live threads since the JVM started or the peak was reset.
Max Heap Mb	The maximum amount of memory used for memory management by the application in the time range specified. This value may change or be undefined. NOTE: A memory allocation can fail if the JVM attempts to set the **Used** memory allocation to a value greater than the **Committed** memory allocation, even if the amount for **Used** memory is less than or equal to the *Maximum* memory allocation (for example, when the system is low on virtual memory).
Committed Mb	The amount of memory, in megabytes, guaranteed to be available for use by the JVM. The amount of committed memory can be a fixed or variable size. If set to be a variable size, the amount of committed memory can change over time, as the JVM may release memory to the system. This means that the amount allocated for **Committed** memory could be less than the amount initially allocated. **Committed** memory will always be greater than or equal to the amount allocated for **Used** memory.
Used Mb	The amount of memory currently used by the application. Memory used includes the memory occupied by all objects including both reachable and unreachable objects.

Class Name	Class name used for JVM.
Arguments	The arguments used to start the application.

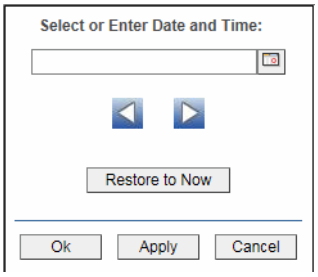
More Arguments Additional arguments used to start the application.

JVM CPU, Memory, Thread Trends
Shows JVM metrics for the selected server.

Log Scale Enable to use a logarithmic scale for the Y axis. Use Log Scale to see usage correlations for data with a wide range of values. For example, if a minority of your data is on a scale of tens, and a majority of your data is on a scale of thousands, the minority of your data is typically not visible in non-log scale graphs. Log Scale makes data on both scales visible by applying logarithmic values rather than actual values to the data.

Base at Zero Use zero as the Y axis minimum for all graph traces.

Time Range Select a time range from the drop down menu varying from **2 Minutes** to **Last 7 Days**, or display **All Data**. To specify a time range, click Calendar ...



By default, the time range end point is the current time. To change the time range end point, click Calendar ... and select a date and time from the calendar or enter the date and time in the text field using the following format: **MMM dd, YYYY HH:MM**. For example, **Aug 21, 2011 12:24 PM**.

Use the navigation arrows to move forward or backward one time period. NOTE: The time period is determined by your selection from the **Time Range** drop-down menu.

Click **Restore to Now** to reset the time range end point to the current time.

JVM CPU % Traces the amount of memory, in percent, used by the JVM in the time range specified.

Max Heap Mb Traces the maximum amount of memory used for memory management by the application in the time range specified. This value may change or be undefined.

NOTE: A memory allocation can fail if the JVM attempts to set the **Used** memory allocation to a value greater than the **Committed** memory allocation, even if the amount for **Used** memory is less than or equal to the **Maximum** memory allocation (for example, when the system is low on virtual memory).

Cur Heap Mb Traces the current amount of memory, in megabytes, used for memory management by the application in the time range specified.

Used Heap Mb Traces the memory currently used by the application.

Live Threads Traces the total number of currently active threads in the time range specified.

JVM Mem Pool Trends

Track JVM heap and non-heap memory usage for a single connection. Use the available drop-down menus or right-click to filter data shown in the display.

Title Bar:
Indicators and functionality might include the following:

Open the previous and upper display.

CMDB and Table navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Cls: 3,047 The number of items in the display.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

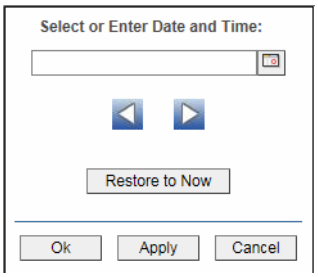
Open an instance of this display in a new window.

Open the online help page for this display.

Fields and Data
This display includes:

Source	Select the type of connection to the RTView Server.
Connection	Select an RTView Server from the drop-down menu. Names can be modified in the RTView Server configuration properties file.
Connected	The data connection state: Disconnected. Connected.
Base at Zero	Use zero as the Y axis minimum for all graph traces.

Time Range Select a time range from the drop down menu varying from **2 Minutes** to **Last 7 Days**, or display **All Data**. To specify a time range, click Calendar ...



By default, the time range end point is the current time. To change the time range end point, click Calendar ... and select a date and time from the calendar or enter the date and time in the text field using the following format: **MMM dd, YYYY HH:MM**. For example, **Aug 21, 2011 12:24 PM**.

Use the navigation arrows to move forward or backward one time period. NOTE: The time period is determined by your selection from the **Time Range** drop-down menu.

Click **Restore to Now** to reset the time range end point to the current time.

Heap Memory

Maximum The maximum amount of memory used, in megabytes, for memory management by the application in the time range specified. This value may change or be undefined.

NOTE: A memory allocation can fail if the JVM attempts to set the **Used** memory allocation to a value greater than the **Committed** memory allocation, even if the amount for **Used** memory is less than or equal to the **Maximum** memory allocation (for example, when the system is low on virtual memory).

Committed The amount of memory, in megabytes, guaranteed to be available for use by the JVM. The amount of committed memory can be a fixed or variable size. If set to be a variable size, the amount of committed memory can change over time, as the JVM may release memory to the system. This means that the amount allocated for **Committed** memory could be less than the amount initially allocated. **Committed** memory will always be greater than or equal to the amount allocated for **Used** memory.

Used The amount of memory, in megabytes, currently used by the application. Memory used includes the memory occupied by all objects including both reachable and unreachable objects.

Peak Tenured Used The amount of memory, in megabytes, used by tenured JVM objects in the time range specified. Tenured refers to JVM objects contained in a pool that holds objects that have avoided garbage collection and reside in the survivor space. Peak tenured refers to the maximum value of the tenured memory over a specified period of time.

Eden Space Traces the amount of memory used by the JVM eden pool in the time range specified. Eden refers to the JVM eden pool, which is used to initially allocate memory for most objects.

Survivor Space Traces the amount of memory used by the JVM survivor pool in the time range specified. The JVM survivor pool holds objects that survive the eden space garbage collection.

Tenured Gen Traces the amount of memory used by tenured JVM objects in the time range specified. Tenured refers to JVM objects contained in a pool that holds objects that have avoided garbage collection and reside in the survivor space. Peak tenured refers to the maximum value of the tenured memory over a specified period of time.

Non-Heap Memory

Maximum	The maximum amount of memory, in megabytes, used for JVM non-heap memory management by the application in the time range specified.
Committed	The amount of memory, in megabytes, guaranteed to be available for use by JVM non-heap memory management. The amount of committed memory can be a fixed or variable size. If set to be a variable size, it can change over time, as the JVM may release memory to the system. This means that the amount allocated for **Committed** memory could **be** less than the amount initially allocated. Committed memory will always be greater than or equal to the amount allocated for **Used** memory.
Used	The amount of memory, in megabytes, currently used by the application. Memory used includes the memory occupied by all objects including both reachable and unreachable objects.
Objects Pending Finalization	The value of the **MemoryMXBean ObjectPendingFinalizationCount** attribute.
Verbose	The value of the **MemoryMXBean Verbose** attribute.
Code Cache	Traces the amount of non-heap memory used in the JVM for compilation and storage of native code.
Perm Gen	Traces the amount of memory used by the pool containing reflective data of the virtual machine, such as class and method objects. With JVMs that use class data sharing, this generation is divided into read-only and read-write areas.

Operations

Run Garbage Collector	Performs garbage collection on the selected server.
Reset Peak Usage	Clears peak usage on the selected server.

JVM Mem GC Trends

Track JVM garbage collection memory usage for a single connection. Use the available drop-down menus or right-click to filter data shown in the display.

Title Bar:
Indicators and functionality might include the following:

Open the previous and upper display.

CMDB and Table navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Cls: 3,047 The number of items in the display.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

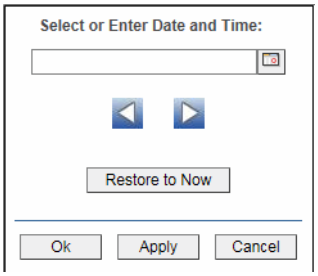
Fields and Data
This display includes:

Source	Select the type of connection to the RTView Server.
Connection	Select an RTView Server from the drop-down menu. Names can be modified in the RTView Server configuration properties file.
Garbage Collector	Select a garbage collection method: **Copy** or **MarkSweepCompact**.
Max	Shows the maximum amount of memory used for JVM garbage collection in the time range specified.

Committed Shows the amount of memory guaranteed to be available for use by JVM non-heap memory management. The amount of committed memory can be a fixed or variable size. If set to be a variable size, it can change over time, as the JVM may release memory to the system. This means that the amount allocated for **Committed** memory could be less than the amount initially allocated. **Committed** memory will always be greater than or equal to the amount allocated for **Used** memory.

Base at Zero Use zero as the Y axis minimum for all graph traces.

Time Range Select a time range from the drop down menu varying from **2 Minutes** to **Last 7 Days**, or display **All Data**. To specify a time range, click Calendar .



By default, the time range end point is the current time. To change the time range end point, click Calendar and select a date and time from the calendar or enter the date and time in the text field using the following format: **MMM dd, YYYY HH:MM**. For example, **Aug 21, 2011 12:24 PM**.

Use the navigation arrows to move forward or backward one time period. NOTE: The time period is determined by your selection from the **Time Range** drop-down menu.

Click **Restore to Now** to reset the time range end point to the current time.

Memory Usage (in MB) Before and After Garbage Collection

Maximum Traces the maximum amount of memory used by garbage collection in the time range specified. This value may change or be undefined.

NOTE: A memory allocation can fail if the JVM attempts to set the **Used** memory allocation to a value greater than the **Committed** memory allocation, even if the amount for **Used** memory is less than or equal to the **Maximum** memory allocation (for example, when the system is low on virtual memory).

Committed Traces the amount of memory guaranteed to be available for use by the JVM. The amount of committed memory can be a fixed or variable size. If set to be a variable size, the amount of committed memory can change over time, as the JVM may release memory to the system. This means that the amount allocated for **Committed** memory could be less than the amount initially allocated. **Committed** memory will always be greater than or equal to the amount allocated for **Used** memory.

Used - Before Traces the amount of memory used before the last garbage collection.

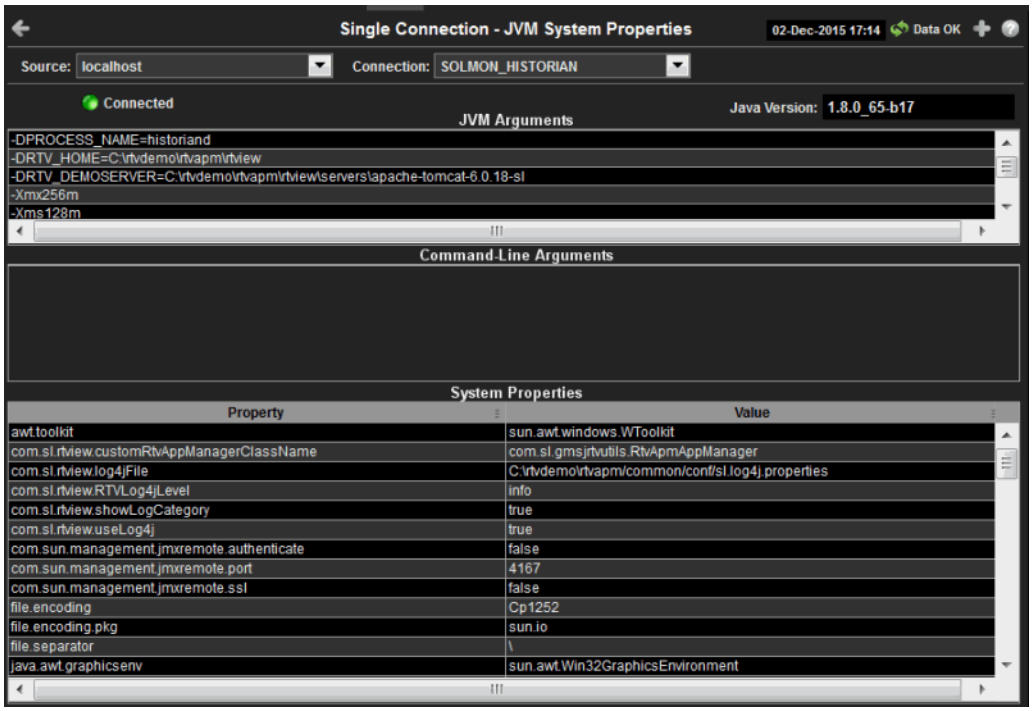
Used - After Traces the amount of memory used after the last garbage collection.

Duration The duration, in seconds, of garbage collection.

Duty Cycle The percentage of time that the application spends in garbage collection.

JVM System Properties

Track JVM input arguments and system properties for a single connection. Use the available drop-down menus or right-click to filter data shown in the display.



Title Bar:
Indicators and functionality might include the following:

Open the previous and upper display.

CMDB and Table navigate to displays commonly accessed from this display.

19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.

Cls: 3,047 The number of items in the display.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.

Open the **Alert Views - RTView Alerts Table** display.

Open an instance of this display in a new window.

Open the online help page for this display.

Fields and Data
This display includes:

Source	Select the type of connection to the RTView Server.
Connection	Select an RTView Server from the drop-down menu. Names can be modified in the RTView Server configuration properties file.
Connected	The data connection state: Disconnected. Connected.
Java Version	The Java version running on the selected server.

JVM Arguments The JVM arguments in the **RuntimeMXBean InputArguments** attribute.

Command Line Arguments Arguments used to start the application.

System Properties
This table lists and describes system property settings.

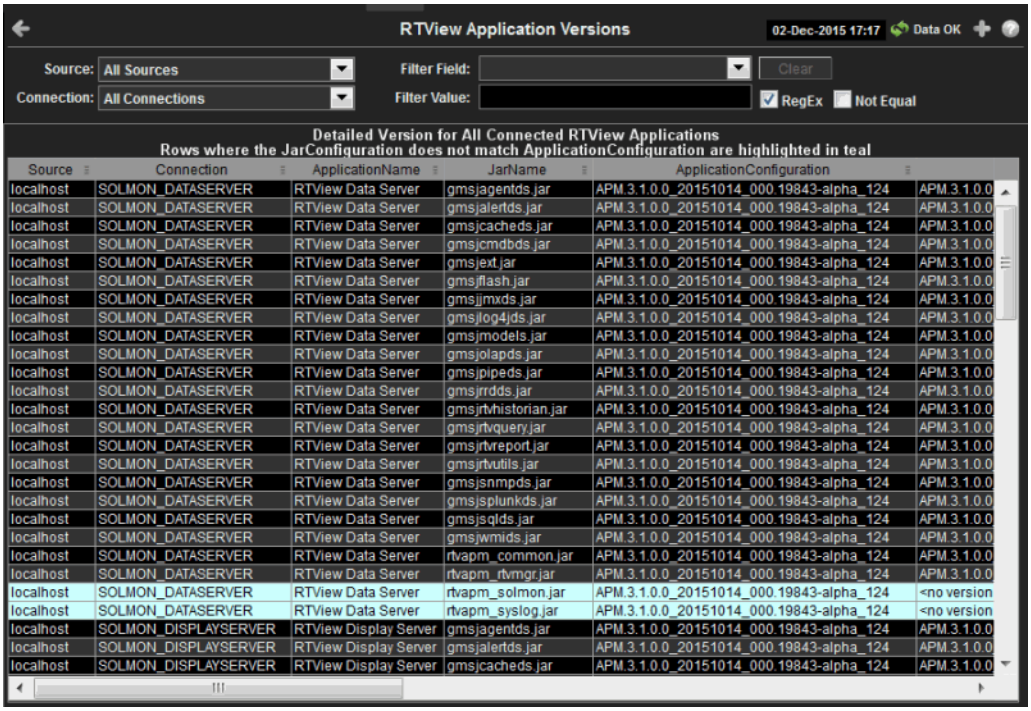
Property Name of the property.

Value Current value of the property.

Version Info

This display provides detailed version information for all of the connected RTView applications. You can view specific applications by filtering data using the **Source**, **Connection**, **Filter Field**, and **Filter Value** fields at the top of the display. This display provides valuable information about the version of each jar that is used in each connected RTView application that can be used to help Technical Support when issues arise. Rows in the table where the **JarConfiguration** does not match the **ApplicationConfiguration** are highlighted in teal.

Note: RTView applications running versions previous to this enhancement have one row in the table and display "version info not supported in this version" in the **ApplicationConfiguration** column.



Source	Connection	ApplicationName	JarName	ApplicationConfiguration	
localhost	SOLMON_DATASERVER	RTView Data Server	gmsjagentds.jar	APM.3.1.0.0_20151014_000.19843-alpha_124	APM.3.1.0.0
localhost	SOLMON_DATASERVER	RTView Data Server	gmsjalertds.jar	APM.3.1.0.0_20151014_000.19843-alpha_124	APM.3.1.0.0
localhost	SOLMON_DATASERVER	RTView Data Server	gmsjcacheds.jar	APM.3.1.0.0_20151014_000.19843-alpha_124	APM.3.1.0.0
localhost	SOLMON_DATASERVER	RTView Data Server	gmsjcmdbds.jar	APM.3.1.0.0_20151014_000.19843-alpha_124	APM.3.1.0.0
localhost	SOLMON_DATASERVER	RTView Data Server	gmsjext.jar	APM.3.1.0.0_20151014_000.19843-alpha_124	APM.3.1.0.0
localhost	SOLMON_DATASERVER	RTView Data Server	gmsjflash.jar	APM.3.1.0.0_20151014_000.19843-alpha_124	APM.3.1.0.0
localhost	SOLMON_DATASERVER	RTView Data Server	gmsjjmxds.jar	APM.3.1.0.0_20151014_000.19843-alpha_124	APM.3.1.0.0
localhost	SOLMON_DATASERVER	RTView Data Server	gmsjlog4jds.jar	APM.3.1.0.0_20151014_000.19843-alpha_124	APM.3.1.0.0
localhost	SOLMON_DATASERVER	RTView Data Server	gmsjmodels.jar	APM.3.1.0.0_20151014_000.19843-alpha_124	APM.3.1.0.0
localhost	SOLMON_DATASERVER	RTView Data Server	gmsjolapds.jar	APM.3.1.0.0_20151014_000.19843-alpha_124	APM.3.1.0.0
localhost	SOLMON_DATASERVER	RTView Data Server	gmsjpipeds.jar	APM.3.1.0.0_20151014_000.19843-alpha_124	APM.3.1.0.0
localhost	SOLMON_DATASERVER	RTView Data Server	gmsjrrdds.jar	APM.3.1.0.0_20151014_000.19843-alpha_124	APM.3.1.0.0
localhost	SOLMON_DATASERVER	RTView Data Server	gmsjrtvhistorian.jar	APM.3.1.0.0_20151014_000.19843-alpha_124	APM.3.1.0.0
localhost	SOLMON_DATASERVER	RTView Data Server	gmsjrtvquery.jar	APM.3.1.0.0_20151014_000.19843-alpha_124	APM.3.1.0.0
localhost	SOLMON_DATASERVER	RTView Data Server	gmsjrtvreport.jar	APM.3.1.0.0_20151014_000.19843-alpha_124	APM.3.1.0.0
localhost	SOLMON_DATASERVER	RTView Data Server	gmsjrtvutils.jar	APM.3.1.0.0_20151014_000.19843-alpha_124	APM.3.1.0.0
localhost	SOLMON_DATASERVER	RTView Data Server	gmsjsnmpds.jar	APM.3.1.0.0_20151014_000.19843-alpha_124	APM.3.1.0.0
localhost	SOLMON_DATASERVER	RTView Data Server	gmsjsplunkds.jar	APM.3.1.0.0_20151014_000.19843-alpha_124	APM.3.1.0.0
localhost	SOLMON_DATASERVER	RTView Data Server	gmsjsqlds.jar	APM.3.1.0.0_20151014_000.19843-alpha_124	APM.3.1.0.0
localhost	SOLMON_DATASERVER	RTView Data Server	gmsjwmids.jar	APM.3.1.0.0_20151014_000.19843-alpha_124	APM.3.1.0.0
localhost	SOLMON_DATASERVER	RTView Data Server	rtvapm_common.jar	APM.3.1.0.0_20151014_000.19843-alpha_124	APM.3.1.0.0
localhost	SOLMON_DATASERVER	RTView Data Server	rtvapm_rtvmgr.jar	APM.3.1.0.0_20151014_000.19843-alpha_124	APM.3.1.0.0
localhost	SOLMON_DATASERVER	RTView Data Server	rtvapm_solmon.jar	APM.3.1.0.0_20151014_000.19843-alpha_124	<no version
localhost	SOLMON_DATASERVER	RTView Data Server	rtvapm_syslog.jar	APM.3.1.0.0_20151014_000.19843-alpha_124	<no version
localhost	SOLMON_DISPLAYSERVER	RTView Display Server	gmsjagentds.jar	APM.3.1.0.0_20151014_000.19843-alpha_124	APM.3.1.0.0
localhost	SOLMON_DISPLAYSERVER	RTView Display Server	gmsjalertds.jar	APM.3.1.0.0_20151014_000.19843-alpha_124	APM.3.1.0.0
localhost	SOLMON_DISPLAYSERVER	RTView Display Server	gmsjcacheds.jar	APM.3.1.0.0_20151014_000.19843-alpha_124	APM.3.1.0.0

Title Bar:
Indicators and functionality might include the following:

Open the previous and upper display.
CMDB and Table navigate to displays commonly accessed from this display.
19-Feb-2014 16:50 The current date and time. When the time is incorrect, this might indicate that RTView stopped running. When the time is correct and the **Data OK** indicator is green, this is a strong indication that the platform is receiving current and valid data.
Cls: 3,047 The number of items in the display.

Data OK The data connection state. Red indicates the data source is disconnected (for example, the Data Server is not receiving data, or the Display Server is not receiving data from the Data Server). Green indicates the data source is connected.
Open the **Alert Views - RTView Alerts Table** display.
Open an instance of this display in a new window.
Open the online help page for this display.

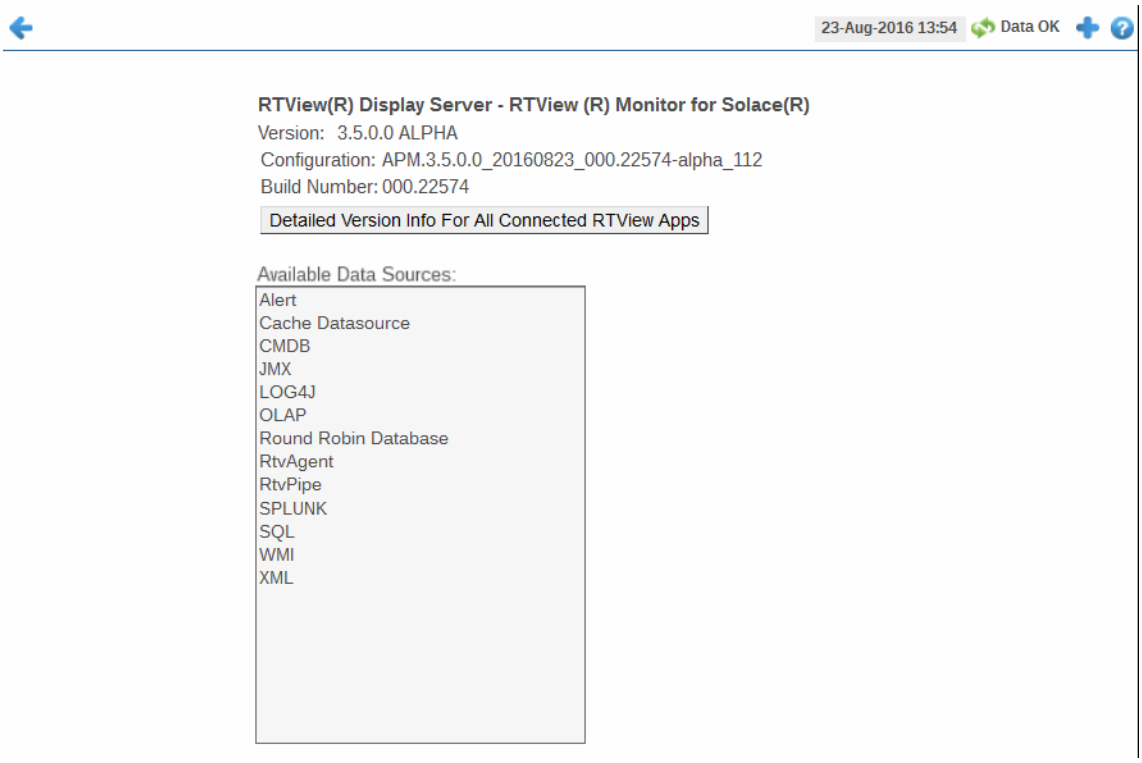
Fields and Data
This display includes:

Source	Select a filter value for the **Source** column.
Connection	Select a filter value for the **Connection** column.
Filter Field	Select a table column from the drop-down menu to perform a search in: **ApplicationName, JarName, ApplicationConfiguration, JarConfiguration, JarVersionNumber,JarVersionDate, JarReleaseDate,** and **JarMicroVersion**. Filters limit display content and drop-down menu selections to only those items that pass through the selected filter's criteria. If no items match the filter, you might have zero search results (an empty table). Double-clicking on a specific field in the table will populate this field with the selected field's content. For example, double-clicking on the **DataServerName** field in one of the rows displays the entire field's content into this field.
Clear	Clears entries in the **Filter Field** display list, **Filter Value** field, and **Not Equal** check box.
Filter Value	Enter the (case-sensitive) string to search for in the selected **Filter Field**.
RegEx	Select this check box to use the **Filter Value** as a regular expression when filtering. When selected, the **Not Equal** check box displays.
Not Equal	Works in conjunction with the **RegEx** field. Selecting this check box searches for values in the specified **Filter Field** that are NOT equal to the value defined in the **Filter Value** field. For example, if the **Filter Field** specified is **JarMicroVersion**, the **Filter Value** is specified as **317,** and this check box is selected, then only those rows containing **JarMicroVersion** fields NOT EQUAL to **317** will display. This field is only enabled when the **RegEx** check box is checked.
Source	The name of the source of the RTVMGR.
Connection	Lists the name of the JMX connection to the RTView application.
Application Name	Lists the name of the application.
JarName	Lists the name of the jar used in the connected application.
Application Configuration	Lists the configuration string of the application. This string contains the main application version that corresponds to the version information printed to the console at startup.
JarConfiguration	Lists the configuration string for the jar.
JarVersionNumber	Lists the version number for the jar.
JarVersionDate	Lists the version date for the jar.
JarReleaseType	Lists the release type for the jar.

JarMicroVersion	Lists the micro version for the jar.
Expired	When checked, this connection is expired due to inactivity.
time_stamp	The time at which the information in the current row was last received.
DataServerName	The name of the RTVMGR data server connection.

About

This display provides detailed version information for RTView Enterprise Monitor and available data sources. Get version information for your connected RTView applications in the "Version Info" display by selecting **Detailed Version Info For All Connected RTView Apps**. Provide this information to Technical Support when issues arise.



APPENDIX A Alert Definitions

This section describes alerts for Solace and their default settings.

Alert	Warning Level	Alarm Level	Duration	Enabled
SolMsgRouterActiveDiskUtilHigh The utilization of the active disk partition for the message router is excessive. Index Type: PerAppliance	70	85	30	FALSE
SolMsgRouterByteEgressUtilHigh The egress rate (bytes/sec) utilization (current egress rate divided by max allowed) for the message router is excessive. Index Type: PerAppliance	70	85	30	FALSE
SolMsgRouterByteIngressUtilHigh The ingress rate (bytes/sec) utilization (current ingress rate divided by max allowed) for the message router is excessive. Index Type: PerAppliance	70	85	30	FALSE
SolMsgRouterConnectionUtilHigh The connection utilization for the message router (current number of connections divided by max allowed) is excessive. Index Type: PerAppliance	70	85	30	FALSE
SolMsgRouterCpuTemperatureHigh CPU temperature margin is above threshold. Index Type: PerApplianceSensor	-30	-15	30	FALSE
SolMsgRouterDelvrdUnAckMsgUtilHigh The delivered unacked messages as a percentage of all messages delivered for the application is excessive. Index Type: PerAppliance	70	85	30	FALSE
SolMsgRouterFailoverDetected The backup message router in a HA pair has assumed control. Index Type: PerAppliance	1	NaN	30	FALSE
SolMsgRouterFanSensorCheckFailed The speed measured for one or more fans is below threshold. Index Type: PerApplianceSensor	5000	2657	30	FALSE

SolMsgRouterInboundByteRateHigh The number of inbound bytes per second for the message router has reached its max threshold. Index Type: PerAppliance	400000	500000	30	FALSE
SolMsgRouterInboundMsgRateHigh The number of inbound messages per second for the message router has reached its max threshold. Index Type: PerAppliance	400000	500000	30	FALSE
SolMsgRouterIngressFlowUtilHigh The ingress flow utilization (current flows divided by max allowed) for the message router is excessive. Index Type: PerAppliance	70	85	30	FALSE
SolMsgRouterMsgCountUtilHigh The message count utilization for the message router is excessive. Index Type: PerAppliance	70	85	30	FALSE
SolMsgRouterMsgEgressUtilHigh The message egress rate utilization (current message egress rate divided by max allowed) for the message router is excessive. Index Type: PerAppliance	70	85	30	FALSE
SolMsgRouterMsgIngressUtilHigh The message ingress rate utilization (current message ingress rate divided by max allowed) for the message router is excessive. Index Type: PerAppliance	70	85	30	FALSE
SolMsgRouterOutboundByteRateHigh The number of outbound bytes per second for the message router has reached its max threshold. Index Type: PerAppliance	400000	500000	30	FALSE
SolMsgRouterOutboundMsgRateHigh The number of outbound messages per second for the message router has reached its max threshold. Index Type: PerAppliance	400000	500000	30	FALSE
SolMsgRouterPendingMsgsHigh The total number of pending messages for this message router has reached its maximum. Index Type: PerAppliance	400000	500000	30	FALSE
SolMsgRouterPowerSupplyFailed A power supply has failed. Index Type: PerAppliance	0	NaN	30	FALSE
SolMsgRouterSpoolUtilization The amount of spool space used for messages is excessive. Index Type: PerAppliance	70	85	30	FALSE
SolMsgRouterStandbyDiskUtilHigh The utilization of the standby disk partition for the message router is excessive. Index Type: PerAppliance	70	85	30	FALSE

SolMsgRouterSubscriptionUtilHigh The subscription utilization (current number of subscriptions divided by max allowed) for the message router is excessive. Index Type: PerAppliance	70	85	30	FALSE
SolMsgRouterSwapUsedHigh The amount of swap space used by the message router operating system is excessive. Index Type: PerAppliance	70	85	30	FALSE
SolMsgRouterSyslog This alert executes when a Solace Syslog Warning or Critical message is received. To get Syslog event alerts (in RTView Enterprise Monitor or the standalone Monitor), go to the Alert Administration display and enable the **SolMsgRouterSyslog** alert.	-	-	-	-
SolMsgRouterTemperatureSensorCheckFailed A chassis temperature measurement is above threshold. Index Type: PerAppliance	40	45	30	FALSE
SolMsgRouterTranSessionCntUtilHigh The transacted session count utilization for the message router is excessive. Index Type: PerAppliance	70	85	30	FALSE
SolMsgRouterTranSessionResUtilHigh The transacted session resource utilization for the message router is excessive. Index Type: PerAppliance	70	85	30	FALSE
SolMsgRouterVoltageSensorCheckFailed A power supply voltage is high or low. Index Type: PerApplianceSesor	NaN	NaN	30	FALSE
SolBridgeInboundByteRateHigh The number of inbound bytes per second across the bridge has reached its maximum. Index Type: PerBridge	8000000	10000000	30	FALSE
SolBridgeInboundMsgRateHigh The number of inbound messages per second across the bridge as a whole has reached its maximum. Index Type: PerBridge	40000	50000	30	FALSE
SolBridgeOutboundByteRateHigh The number of outbound bytes per second across the bridge has reached its maximum. Index Type: PerBridge	8000000	10000000	30	FALSE
SolBridgeOutboundMsgRateHigh The number of outbound messages per second across the bridge has reached its maximum. Index Type: PerBridge	40000	50000	30	FALSE
SolClientInboundByteRateHigh The number of outbound bytes per second for the client has reached its maximum. Index Type: PerClient	8000000	10000000	30	FALSE

SolClientInboundMsgRateHigh The number of outbound messages per second for the client as a whole has reached its maximum. Index Type: PerClient	40000	50000	30	FALSE
SolClientOutboundByteRateHigh The number of outbound bytes per second for the client has reached its maximum. Index Type: PerClient	8000000	10000000	30	FALSE
SolClientOutboundMsgRateHigh The number of outbound messages per second for the client as a whole has reached its maximum. Index Type: PerClient	40000	50000	30	FALSE
SolClientSlowSubscriber One or more clients are consuming messages too slowly; endpoints may drop messages! Index Type: PerClient	1	NaN	30	FALSE
SolCspfNeighberDown State is not “OK” for one or more CSPF neighbors. Index Type: PerNeighbor	1	NaN	30	FALSE
SolEndpointPendingMsgsHigh The number of pending messages on a queue has reached its maximum. Index Type: PerEndpoint	8000	10000	30	FALSE
SolEndpointSpoolUsageHigh The endpoint is consuming too much message router memory for storing spooled messages. (Threshold units are megabytes.) Index Type: PerEndpoint	40	50	30	FALSE
SolGuaranteedMsgingHbaLinkDown For Guaranteed Messaging only, the Operational State for each HBA Fibre-Channel should be Online (e.g., not Linkdown). Index Type: PerHbaLink	0	NaN	30	FALSE
SolGuaranteedMsgingMatePortDown For Guaranteed Messaging only, the Mate Link Ports for ADB should have status OK. Index Type: PerADB	0	NaN	30	FALSE
SolGuaranteedMsgingNoMsgSpoolAdActive For Guaranteed Messaging only with Redundancy, at least one message router in an HA pair should show “AD-Active.” Index Type: PerPair	0	NaN	30	FALSE
SolInterfaceDown Link-detect = no for one or more enabled network interfaces. Index Type: PerSolInterface	NaN	NaN	30	FALSE
SolNABUsageHigh Network Acceleration Blade memory usage is excessive. Index Type: PerNAB	60	80	30	FALSE

SolVpnConnectionCountHigh The number of connections to the server has reached its maximum. Index Type: PerVPN	60	80	30	FALSE
SolVpnInboundByteRateHigh The number of inbound bytes per second for the vpn has reached its maximum. Index Type: PerVPN	8000000	10000000	30	FALSE
SolVpnInboundDiscardRateHigh The number of discarded inbound messages per second for the server is excessive. Index Type: PerVPN	1	5	30	FALSE
SolVpnInboundMsgRateHigh The number of inbound messages per second for the vpn as a whole has reached its maximum. Index Type: PerVPN	40000	50000	30	FALSE
SolVpnOutboundByteRateHigh The number of outbound bytes per second for the VPN has reached its maximum. Index Type: PerVPN	8000000	10000000	30	FALSE
SolVpnOutboundDiscardRateHigh The number of discarded outbound messages per second for the server is excessive. Index Type: PerVPN	1	5	30	FALSE
SolVpnOutboundMsgRateHigh The number of outbound messages per second for the server as a whole has reached its maximum. Index Type: PerVPN	40000	50000	30	FALSE
SolVpnPendingMsgsHigh The total number of pending messages for this destination has reached its maximum. Index Type: PerVPN	8000000	10000000	30	FALSE
SolVpnSubscriptionCountHigh The number of endpoints in this VPN has reached its maximum. Index Type: PerVPN	8000	10000	30	FALSE

APPENDIX B Limitations

iPad Safari Limitations

- In the iPad settings for Safari, **JavaScript** must be **ON** and **Block Pop-ups** must be **OFF**. As of this writing, the Thin Client has been tested only on iOS 4.3.5 in Safari.
- The iPad does not support Adobe Flash, so the Fx graph objects (obj_fxtrend, obj_fxpie, obj_fxbar) are unavailable. The Thin Client automatically replaces the Fx graph objects with the equivalent non-Fx object (obj_trendgraph02, obj_pie, obj_bargraph). Note that the replacement objects behave the same as the Fx objects in most cases but not in all. In particular, obj_trendgraph02 does not support the sliding cursor object nor the **legendPosition** property. Custom Fx objects are not supported on the iPad.
- The Thin Client implements scrollbars for table objects and graph objects. However, unlike the scrollbars used on desktop browsers, the scrollbars used on the iPad do not have arrow buttons at each end. This can make it difficult to scroll precisely (for example, row by row) on objects with a large scrolling range.
- At full size, users may find it difficult to touch the intended display object without accidentally touching nearby objects and performing an unwanted drill-down, sort, scroll, and so forth. This is particularly true of table objects that support drill-down and also scrolling, and also in panel layouts that contain the tree navigation control. In those cases, the user may want to zoom the iPad screen before interacting with the Thin Client.
- If the iPad sleeps or auto-locks while a Thin Client display is open in Safari, or if the Safari application is minimized by clicking on the iPad's home button, the display is not updated until the iPad is awakened and Safari is reopened. In some cases it may be necessary to refresh the page from Safari's navigation bar.

Because the iPad uses a touch interface there are differences in the Thin Client appearance and behavior in iOS Safari as compared to the conventional desktop browsers that use a cursor (mouse) interface, such as Firefox and Internet Explorer. These are described below.

- Popup browser windows: An RTView object's drill-down target can be configured to open a display in a new window. In a desktop browser, when the RTView object is clicked the drill-down display is opened in a popup browser window. But in iOS Safari 4.3.5, only one page is visible at a time, so when the RTView object is touched a new page containing the drill-down display opens and fills the screen. The Safari navigation bar can be used to toggle between the currently open pages or close them.
- Mouseover text: When mouseover text and drill-down are both enabled on an RTView object (for example, a bar graph), in iOS Safari the first touch on an element in the object (for example, a bar) displays the mouseover text for that element and the second touch on the same element performs the drill-down.
- Resize Mode and Layout: By default, the Display Server runs with **resizeMode** set to **crop**. In **crop** mode, if a display is larger than the panel that contains it only a portion of the display is visible. In a desktop browser, scrollbars become available to allow the user to scroll to view the entire display. In iOS Safari, scrollbars do not appear but the display can be scrolled by dragging two fingers inside the display. (Dragging one finger scrolls the entire page, not the display).

  If the Display Server is run with **resizeMode** set to **scale** or **layout**, the display is resized to fit into the panel that contains it. If a desktop browser is resized after a display is opened, the display is resized accordingly. On the iPad, the Safari browser can only be resized by reorienting the iPad itself, between portrait mode and landscape mode.

  The panel layout feature is supported in the Thin Client. However, unlike a desktop browser which resizes to match the layout size, the size of Safari is fixed. So if the Display Server is run with **resizeMode** set to **crop** or **scale** mode, there may be unused space at the edges of the display(s) or, in **crop** mode, the panels and displays may be cropped.

  This means that **layout** mode should be used for best results on the iPad. For layout mode to be most effective, displays should use the **anchor** and **dock** object properties. Please see RTView documentation for more information.
- Scrolling: The Thin Client implements scrollbars for table objects and graph objects. The scrollbars are activated by dragging with one finger.

  If an RTView display is viewed in **crop** mode and is too large to be displayed entirely in Safari, scrollbars do not appear (as they would in a desktop browser) but the display can be scrolled by dragging with two fingers inside the display.

  Scrollbars do not ever appear in a text area control. If the text area contains more text than is visible, use the two finger drag in the text area to scroll the text.

Regardless of the size of a listbox control, it can only display a single item (typically, the selected item). When the listbox is touched, the list of items appear in a popup list. In other words, on iOS Safari the listbox control and the combobox control behave identically.

- Context menu: The Thin Client context menu is opened by a right mouse button click in a desktop browser. It is opened in iOS Safari by touching any location on a display and holding that touch for 2 seconds. The menu appears in the top left corner of the display, regardless of where the display is touched. The items **Export Table to Excel**, **Drill Down**, and **Execute Command** are not included on the context menu in Safari. All other items are available. The **Export Table to HTML** item is enabled if a table object is touched (unless the table object's drillDownTarget is configured to open another display). After an **Export to PDF/HTML** is performed, the exported content opens on another page in Safari. From there, the content can either be opened by another application (for example, the iBooks application opens PDF) and emailed, or it can be copied ands pasted into an email.
-