RTView® Monitor for Solace® User's Guide

Version 3.5

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

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 Release Notes document, which is available on the SL Technical Support site at http://www.sl.com/support/, supplements the information in this user guide.

Documentation and Support Knowledge Base

For a complete list and the most current version of SL documentation, visit the SL Support Web site 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.

You can also install the monitor as a Solution Package (rather than a standalone product).

Solution Package Version

The RTView Monitor for Solace 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 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.

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

Get Started

Go to "Quick Start" on page 5 for details on how to get up and running with RTView Monitor for Solace.

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

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.
- 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

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. Include **JAVA_HOME/bin** for 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 7 application server, you must obtain another application server. This change implies additional configuration steps.

Proceed to "Obtain SEMP Version," next.

Obtain SEMP Version

In order to properly request monitored data, the Solution Package for Solace requires the exact SEMP version on your message routers. These instructions describe how to use SolAdmin to determine the SEMP version for each of your Solace Message Routers or VMRs. You will need this information when you "Connect Your Message Routers" and edit connection properties.

Note: These instructions are for SolAdmin on Windows. For Linux, only the path to the log file changes.

1. Navigate to the SolAdmin installation folder. For example, **C:\Program Files (x86)\SolAdmin\**.

2. Change directory (**cd**) to the **bin** directory and open the **log4j.properties** file in a text editor.

3. Change the logging level to **DEBUG** and provide the full path to the logging file (for example, **C:\Logs**) while retaining all other setting. The edited properties are as follows:

```
# full path to the location where you want the log file to be stored. In this example C:\Logs
log4j.appender.A1.File=C:\Logs\soladmin.log
# Set the logging category to DEBUG
log4j.category.com.solacesystems=DEBUG, A1
```

4. Save the **log4j.properties** file.

5. Start SolAdmin and add your message routers or VMRs as a managed instance.

6. Open the **soladmin.log** file and locate the semp-version tag in SEMP requests. The SEMP version that will be used by the Solultion Package for Solace should replace underscores (_) with dots (**.**). For example, if the SEMP request in the SolAdmin log file is **7_2VMR**, you should use **7.2VMR** for the **$solSempVersion** substitution of the Solultion Package for Solace connection property.

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 from your project directory (**rtvapm_projects/emsample/solmon**).

2. Edit the following lines for each Solace message router or VMR 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>** $solSempVersion:**<SEMP_Version>**

where

- **<UNIQUE_APPLIANCE_NAME>** is a unique string to identify the connection of each monitored message router.
- **<IP or hostname>** 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.
- **<SEMP_Version>** is the value you obtained for each Message Router or VMR from previous step.

Example:
(where **xxx.xxx.xxx.xxx** = IP address)

collector.sl.rtview.http.conn=__name=example url=http://xxx.xxx.xxx.xxx:8080/SEMP username=rtviewadmin password=rtview
collector.sl.rtview.cache.config=sol_cache_source.rtv $solConn:example
$solSempVersion:7.2VMR

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 "Configure Sender/Receiver," next.

Configure Sender/Receiver

If you have decided to deploy the Solution Package for Solace as a Sender/Receiver configuration, continue with instructions in this section. Otherwise, skip these steps and go to "Start the Monitor".

Depending on the network architecture and accessibility of the hosts that will execute the sender and the receiver, there are two options for connecting to a receiver Data Server. These instructions describe how to configure both options, which are:

- **Option 1**: Connect to the receiver Data Server through IP address and port. This option requires higher degree of accessibility between sender and receiver.
- **Option 2**: Connect to the receiver Data Server through the RTView agent servlet. This option requires an application server running in the receiver host with the **solmon_rtvagent** deployed.

These instructions describe how to configure both.

To configure a sender/receiver Data Server for the Solace Message Router or Solace VMR:

1. Open the **sample.properties** file from the **solmon** projects directory on your sender host.

2. Do one of the following options, replacing **bold** strings as appropriate for your system:

- **Option 1**: Connect to the receiver through IP address and port

```
# Sender properties
sender.sl.rtview.sub=$rtvAgentName:MyVMRInstance
sender.sl.rtview.sub=$rtvAgentTarget:'YourReceiverIpAddress:4172'
```

- **Option 2**: Connect to the receiver through the agent servlet

```
# Sender properties
sender.sl.rtview.sub=$rtvAgentName:MyVMRInstance
sender.sl.rtview.sub=$rtvAgentTarget:'http://publicIPAddress/solmon_rtvagent'
```

where **MyVMRInstance** is a string that uniquely identifies the data coming from the sender.

3. On the sender host, change directory (**cd**) to your project directory and start the sender as follows:

start_rtv solmon dataserver –properties:sample –propfilter:sender

or

rundata.sh/.bat –properties:sample –propfilter:sender

4. On the receiver host, change directory (**cd**) to your project directory and start the receiver as follows:

start_rtv solmon dataserver -propfilter:receiver

or

rundata.sh/.bat -propfilter:receiver

5. Verify that you are receiving data from the sender by opening a browser window to reach your deployed Solution Package for Solace.

Note: Syslog data is not sent from sender hosts. You must configure Syslog data from your VMRs and message routers to be collected on the receiver host.

Proceed to "Start the Monitor," next.

Start the Monitor

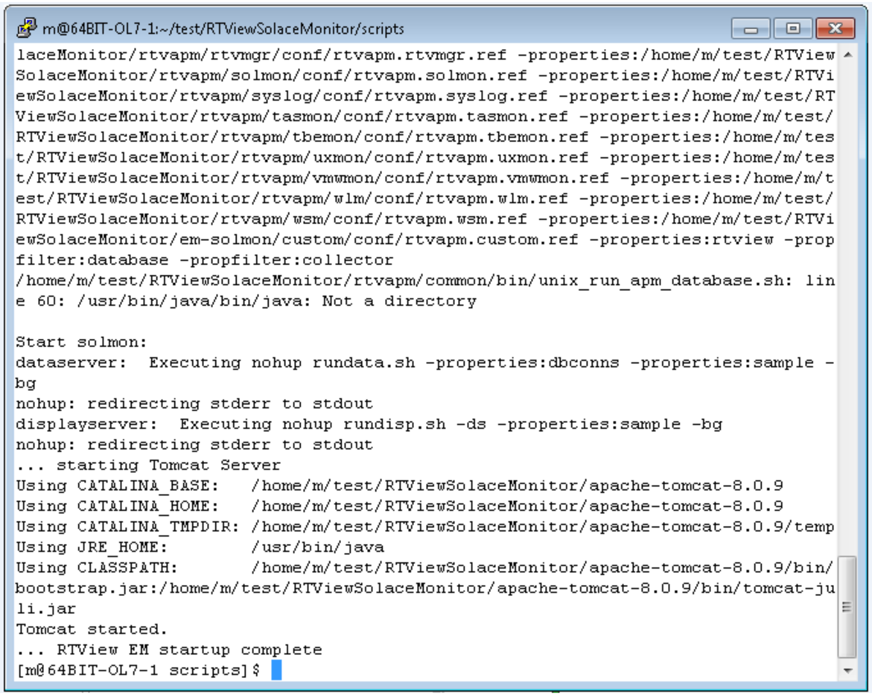
To start the Monitor and Tomcat:

1. Linux/UNIX ONLY (this step is not required on Windows): Open a command line window.

2. Change directory (**cd**) to the **RTViewSolaceMonitor/bin** directory.

3. Execute **sh start_servers.sh** (or **start_servers.bat** for Windows) to start all Monitor components and Tomcat.

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



```
laceMonitor/rtvapm/rtvmgr/conf/rtvapm.rtvmgr.ref -properties:/home/m/test/RTView
SolaceMonitor/rtvapm/solmon/conf/rtvapm.solmon.ref -properties:/home/m/test/RTVi
ewSolaceMonitor/rtvapm/syslog/conf/rtvapm.syslog.ref -properties:/home/m/test/RT
ViewSolaceMonitor/rtvapm/tasmon/conf/rtvapm.tasmon.ref -properties:/home/m/test/
RTViewSolaceMonitor/rtvapm/tbemon/conf/rtvapm.tbemon.ref -properties:/home/m/tes
t/RTViewSolaceMonitor/rtvapm/uxmon/conf/rtvapm.uxmon.ref -properties:/home/m/tes
t/RTViewSolaceMonitor/rtvapm/vmwmon/conf/rtvapm.vmwmon.ref -properties:/home/m/t
est/RTViewSolaceMonitor/rtvapm/wlm/conf/rtvapm.wlm.ref -properties:/home/m/test/
RTViewSolaceMonitor/rtvapm/wsm/conf/rtvapm.wsm.ref -properties:/home/m/test/RTVi
ewSolaceMonitor/em-solmon/custom/conf/rtvapm.custom.ref -properties:rtview -prop
filter:database -propfilter:collector
/home/m/test/RTViewSolaceMonitor/rtvapm/common/bin/unix_run_apm_database.sh: lin
e 60: /usr/bin/java/bin/java: Not a directory

Start solmon:
dataserver:  Executing nohup rundata.sh -properties:dbconns -properties:sample -
bg
nohup: redirecting stderr to stdout
displayserver:  Executing nohup rundisp.sh -ds -properties:sample -bg
nohup: redirecting stderr to stdout
... starting Tomcat Server
Using CATALINA_BASE:   /home/m/test/RTViewSolaceMonitor/apache-tomcat-8.0.9
Using CATALINA_HOME:   /home/m/test/RTViewSolaceMonitor/apache-tomcat-8.0.9
Using CATALINA_TMPDIR: /home/m/test/RTViewSolaceMonitor/apache-tomcat-8.0.9/temp
Using JRE_HOME:        /usr/bin/java
Using CLASSPATH:       /home/m/test/RTViewSolaceMonitor/apache-tomcat-8.0.9/bin/
bootstrap.jar:/home/m/test/RTViewSolaceMonitor/apache-tomcat-8.0.9/bin/tomcat-ju
li.jar
Tomcat started.
... RTView EM startup complete
[m@64BIT-OL7-1 scripts]$
```

4. 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.

5. In the Monitor, go to **Administration>**"RTView Cache Tables" on page 119 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 10.

You have completed the Quick Start.

Stop the Monitor

To stop the Monitor and Tomcat:

1. Linux/UNIX ONLY (this step is not required on Windows): Open a command line window.
2. Change directory (**cd**) to the **RTViewSolaceMonitor/bin** directory.
3. Execute **../stop_servers.sh** (or **stop_servers.bat** for Windows) to stop all Monitor components and Tomcat.
4. 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 11
- “Permissions” on page 11
- “Network/DNS” on page 11
- “Verify Data Received from Data Server” on page 11
- “Verify Port Assignments” on page 11

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 119 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 119 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 119 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 Production Configuration

This section describes how to configure the RTView® Monitor for Solace® 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 16
- "Configure HA" on page 19
- "Setup Data Persistence" on page 20

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 18
- "Notification Persistence" on page 19

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 10.

6. Start the Monitor as described in “Start the Monitor” on page 9.

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 4 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”
- “Solace Monitor Views/Displays”

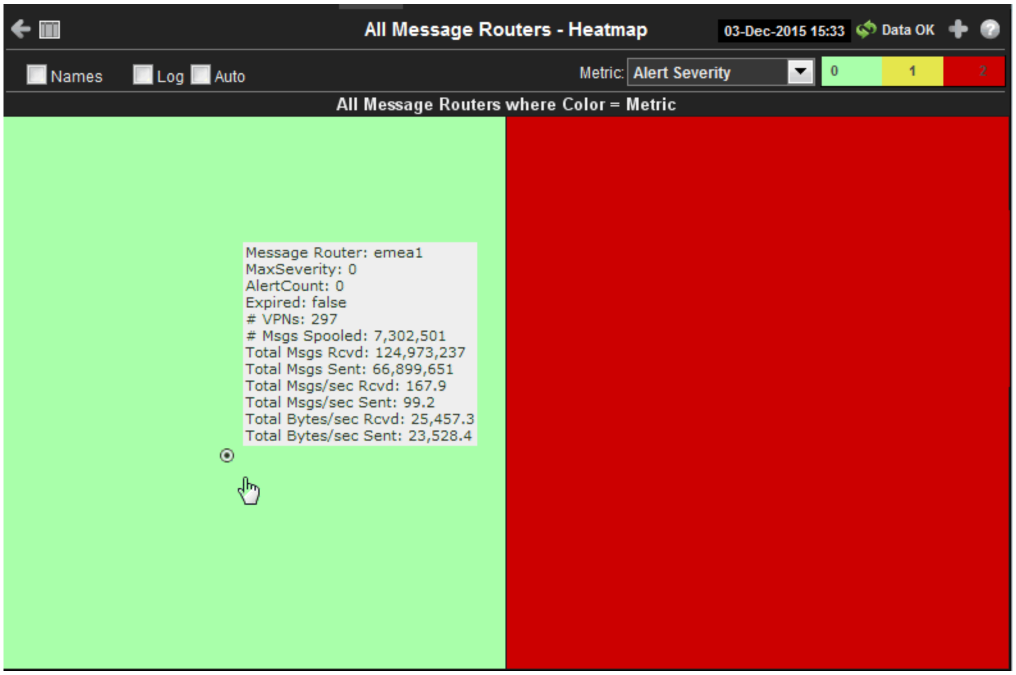
Overview

This section describes the general operation of the Solace Monitor and the user interface. This section includes:

- “Heatmaps” on page 22: Describes how to read heatmaps.
- “Tables” on page 24: Describes how to read tables.
- “Trend Graphs” on page 25: Describes how to read trend graphs.
- “Title Bar Functionality” on page 25: Describes the top layer of the title bar shared by EMS Monitor displays.
- “Export Report” on page 26: Allows you to quickly export reports for displays, or for tables and grid objects in a display, to a PDF file.

Heatmaps

Heatmaps organize your Solace resources (instances, databases, and collections) into rectangles and use color to highlight the most critical value in each. Heatmaps enable you to view various alert 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 Solace resources in the rectangle; a larger size is a larger value. Heatmaps include drop-down menus by which to filter data. The filtering options vary among heatmaps (the **All Message Routers Heatmap** is shown below).


All Message Routers - Heatmap
03-Dec-2015 15:33
Data OK
□ Names
□ Log
□ Auto
Metric:
Alert Severity
0
1
2
All Message Routers where Color = Metric

Message Router: emea1
MaxSeverity: 0
AlertCount: 0
Expired: false
VPNs: 297
Msgs Spooled: 7,302,501
Total Msgs Rcvd: 124,973,237
Total Msgs Sent: 66,899,651
Total Msgs/sec Rcvd: 167.9
Total Msgs/sec Sent: 99.2
Total Bytes/sec Rcvd: 25,457.3
Total Bytes/sec Sent: 23,528.4

For example, the **All Instances Heatmap** (shown above) contains a **Metric** drop-down menu with options to show **Alert Severity**, **Alert Count**, **Physical Memory**, **Open Cursors, Connections**, and **Databases**. Menu options vary according to the data populating the heatmap. **Alert Severity** is selected and its corresponding color gradient 🟩0 🟨1 🟥2 bar is shown. Each rectangle represents a connection. A red rectangle in the heatmap indicates that one or more resources associated with that connection currently has an alert in an alarm state. The yellow rectangles in the heatmap indicate that one or more resources associated with that host currently have an alert in a warning state. A green rectangle would indicate that no alert is in a warning or alarm state.

In most heatmaps, you can also drill-down to more detail by clicking a rectangle in the heatmap. Or, open a new window by using the ✚ button and then drill-down. The drill-down opens a display that contains relevant and more detailed data.

Note: Typically, it takes about 30 seconds after a server is started to appear in an Solace Monitor display. By default, data is collected every 15 seconds, and the display is refreshed 15 seconds afterward.

As previously mentioned, each Metric drop-down menu option has a color gradient bar that maps relative values to colors. The following summarizes the heatmap color code translation for typical heatmaps:

Alert Impact

The product of the maximum **Alert Severity** multiplied by the maximum **Criticality** of alerts in a given heatmap rectangle. Values range from **0 - 10**, as indicated in the color gradient bar, where **10** is the highest **Alert Impact**.

Alert Severity

The maximum alert level in the item (index) associated with the rectangle. Values range from **0 - 2**, as indicated in the color gradient bar, where **2** is the highest Alert **Severity.**

🔴 Metrics that have exceeded their specified **ALARM LEVEL** threshold have an **Alert Severity** value of **2**. For a given rectangle, this indicates that one or more metrics have reached their alert thresholds.

🟡 Metrics that have exceeded their specified **WARNING LEVEL** threshold have an **Alert Severity** value of **1**. For a given rectangle, this indicates that one or more metrics have reached their warning thresholds.

🟢 Metrics that have not exceeded either specified threshold have an **Alert Severity** value of **0**. For a given rectangle, this indicates that no metrics have reached their warning or alert thresholds.

Alert Count

The total number of critical and warning alerts in a given item (index) associated with the rectangle. The color gradient bar numerical values range from **0** to the maximum count of alerts currently in the heatmap. The middle value in the gradient bar indicates the average alert count.

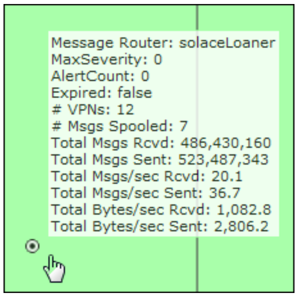
Criticality

The maximum level of **Criticality** (rank of importance) in a given item (index) associated with the rectangle. Values range from **0** to **5**, as indicated in the color gradient bar, where **5** is the highest Criticality.

Criticality is specified in the Service Data Model by your administrator. **Criticality** values range from **A** to **E**, where **A** is the highest Criticality (level **5** maps to a Criticality of **A** and level **1** maps to a **Criticality** of **E** with equally spaced intermediate values).

Mouse-over

The mouse-over functionality provides additional detailed data in a tool-tip when you mouse-over a heatmap. The following figure illustrates mouse-over functionality in a heatmap object. In this example, when you mouse-over a host, details are shown such as alert count, number of connections, and pending messages.



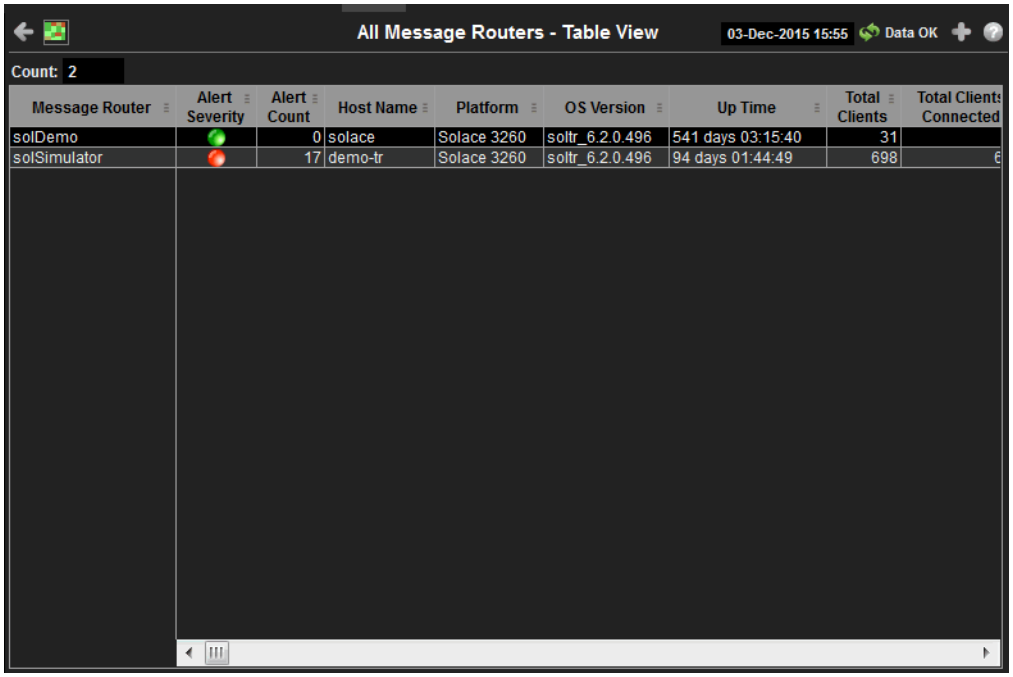
Message Router: solaceLoaner
MaxSeverity: 0
AlertCount: 0
Expired: false
VPNs: 12
Msgs Spooled: 7
Total Msgs Rcvd: 486,430,160
Total Msgs Sent: 523,487,343
Total Msgs/sec Rcvd: 20.1
Total Msgs/sec Sent: 36.7
Total Bytes/sec Rcvd: 1,082.8
Total Bytes/sec Sent: 2,806.2

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

Solace 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 above).



All Message Routers - Table View

03-Dec-2015 15:55 Data OK

Count: 2

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

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:

🔴 One or more alerts exceeded their critical threshold for one or more associated resources.

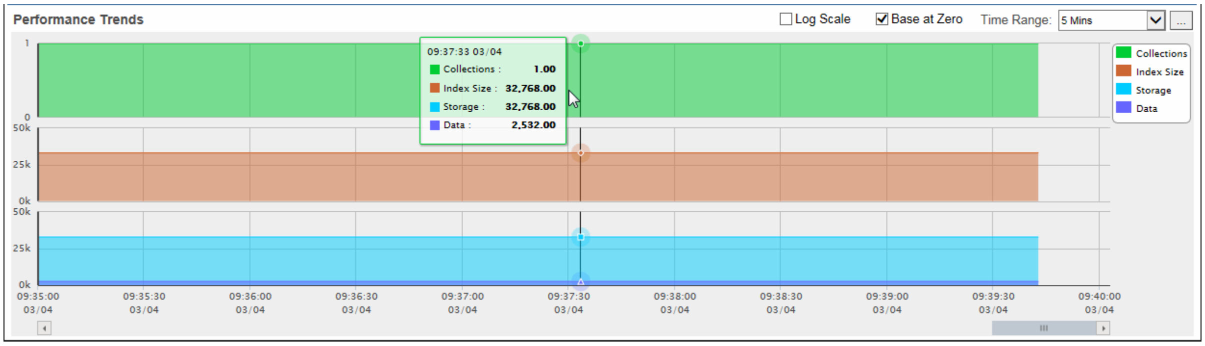
🟡 One or more alerts exceeded their warning threshold for one or more associated resources.

Sorting

Solace Monitor allows you to sort the rows of a table using the ▲ button. To do so, you click on the column title. A symbol appears when sorting in ascending order, and the inverted symbol when sorting in descending order.

Trend Graphs

Solace Monitor trend graphs enable you to view and compare various important metrics over time, such as server memory and virtual memory utilization.



Performance Trends

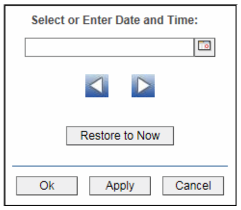
□ Log Scale ☑ Base at Zero Time Range: 5 Mins ...

09:37:33 03/04

🟩 Collections :	1.00
🟧 Index Size :	32,768.00
🟦 Storage :	32,768.00
🟪 Data :	2,532.00

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 enter a specific time range, click the associated ellipsis button ... .



To change the time range click the Open Calendar button ▭, 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) and 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 above figure illustrates mouse-over functionality. In the example above, when you mouse-over a single dot, or data point, in the Index Size trend graph, a pop-up window shows data for that data point. In this case, the X-axis value is 9:37:30 hours on March 4th, and the Y-axis value is 32768.00 bytes.

Title Bar Functionality

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

←	Opens the previous display.
↑	Opens the display that is up one level.

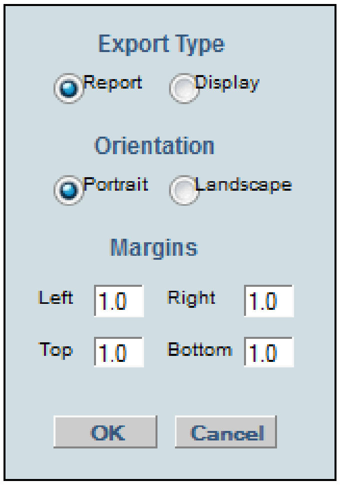
Table	Navigates to a display that is most commonly accessed from the current display. The target display differs among displays.
⚠	Opens the Alerts Table display in a new window.
19-Feb-2014 16:50	The current date and time. If the time is incorrect, this might indicate that RTView stopped running. When 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.

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.



Export Type

● Report ○ Display

Orientation

● Portrait ○ Landscape

Margins

Left 1.0 Right 1.0

Top 1.0 Bottom 1.0

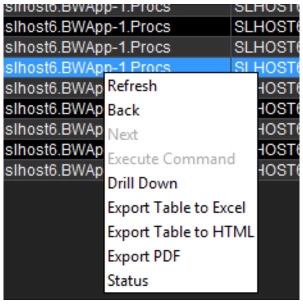
Set the margins and choose the **Export Type**:

- **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**.



Solace Monitor Views/Displays

This section contains the following:

- "Message Routers" on page 28: 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 54: The displays in this View present views of the VPN-level metrics.
- "Clients" on page 67: 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 77: 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 85: 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 94: The displays in this View present current metrics, alert count and severity at the message router level.
- "Syslog" on page 105: View all Syslog events for your Solace message routers.
- "Alert Views" on page 107: Track and manage all alerts that have occurred in the system, add comments, acknowledge or assign Owners to alerts.
- "Administration" on page 111: Set alert thresholds, observe how alerts are managed, and view internal data gathered and stored by RTView.
- "RTView Servers" on page 122: View and monitor all RTView Servers, get information about your software versions and available data sources.

Message Routers

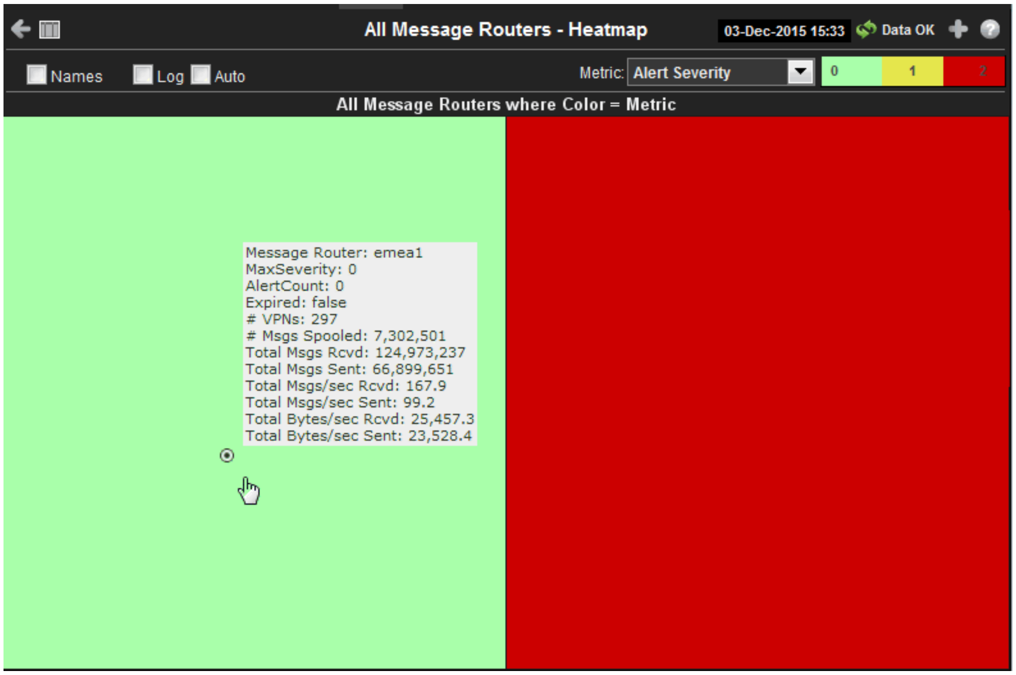
These displays provide detailed data and statuses for message routers and their connected message routers. Displays in this View are:

- "All Message Routers Heatmap" on page 28: A color-coded heatmap view of the current status of each of your message routers.
- "All Message Routers Table" on page 31: A tabular view of all available message router performance data.
- "Message Router Summary" on page 38: Current and historical metrics for a single message router.
- "Environmental Sensors" on page 42: 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 43: Provides message router host, chassis, redundancy, memory, and fabric data for a particular message router.
- "Interface Summary" on page 46: 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 48: Provides status and usage data for message spools associated with one or all message router(s).
- "Message Router VPN Activity" on page 50: 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 52: 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.


All Message Routers - Heatmap
03-Dec-2015 15:33
Data OK
□ Names
□ Log
□ Auto
Metric: Alert Severity
0
1
2
All Message Routers where Color = Metric

Message Router: emea1
MaxSeverity: 0
AlertCount: 0
Expired: false
VPNs: 297
Msgs Spooled: 7,302,501
Total Msgs Rcvd: 124,973,237
Total Msgs Sent: 66,899,651
Total Msgs/sec Rcvd: 167.9
Total Msgs/sec Sent: 99.2
Total Bytes/sec Rcvd: 25,457.3
Total Bytes/sec Sent: 23,528.4

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 0 1 2 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 0 13 26 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 0 5 10 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 0 2.5 5 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 0 2.5 5 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 0 5 10 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 0 5 10 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 0 5 10 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.

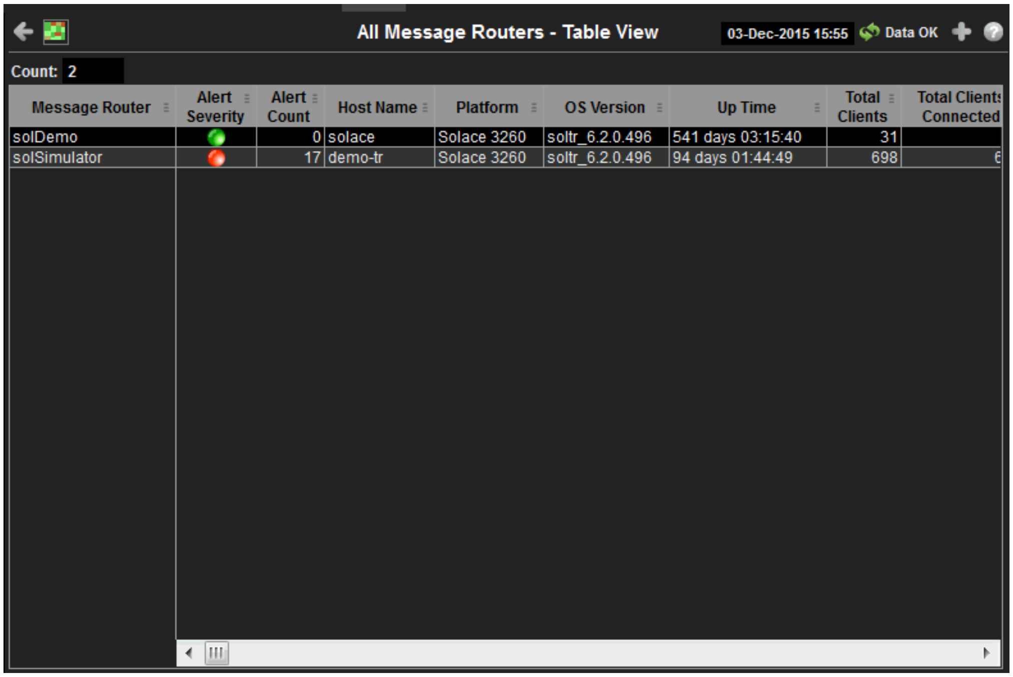
Total Bytes/ sec Sent
The total number of bytes sent per second in the message router. The color gradient 0 5 10 bar, populated by the current heatmap, shows the value/color mapping. The numerical values in the gradient bar range from 0 to the defined alert threshold of **SolMsgRouterOutboundByteRateHigh**. 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



Count: 2

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 0 1 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.

ChassisProduct 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.

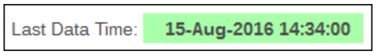
Time Stamp The date and time the row data was last updated.

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.



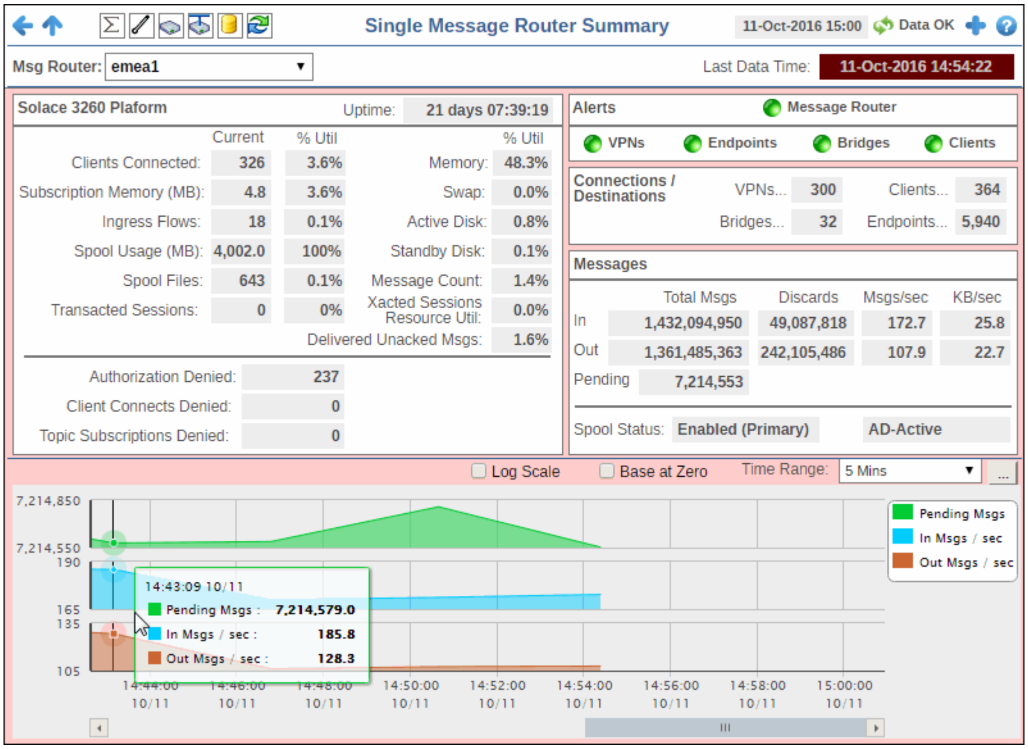
Last Data Time: 15-Aug-2016 14:34:00

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, outgoing, and pending message data.



Single Message Router Summary 11-Oct-2016 15:00 Data OK

Msg Router: emea1 ▼ Last Data Time: 11-Oct-2016 14:54:22

Solace 3260 Plaform Uptime: 21 days 07:39:19

	Current	% Util		% Util
Clients Connected:	326	3.6%	Memory:	48.3%
Subscription Memory (MB):	4.8	3.6%	Swap:	0.0%
Ingress Flows:	18	0.1%	Active Disk:	0.8%
Spool Usage (MB):	4,002.0	100%	Standby Disk:	0.1%
Spool Files:	643	0.1%	Message Count:	1.4%
Transacted Sessions:	0	0%	Xacted Sessions Resource Util:	0.0%
			Delivered Unacked Msgs:	1.6%

Authorization Denied:	237
Client Connects Denied:	0
Topic Subscriptions Denied:	0

Alerts ● Message Router

● VPNs ● Endpoints ● Bridges ● Clients

Connections / Destinations

VPNs...	300	Clients...	364
Bridges...	32	Endpoints...	5,940

Messages

	Total Msgs	Discards	Msgs/sec	KB/sec
In	1,432,094,950	49,087,818	172.7	25.8
Out	1,361,485,363	242,105,486	107.9	22.7
Pending	7,214,553			

Spool Status: Enabled (Primary) AD-Active

□ Log Scale □ Base at Zero Time Range: 5 Mins ▼ ...

14:43:09 10/11
🟩 Pending Msgs : 7,214,579.0
🟦 In Msgs / sec : 185.8
🟧 Out Msgs / sec : 128.3

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:

Platform Name The Solace platform name.

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.

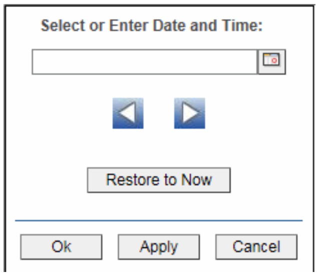
In Msgs/ sec Traces the number of incoming messages per second.

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 … .



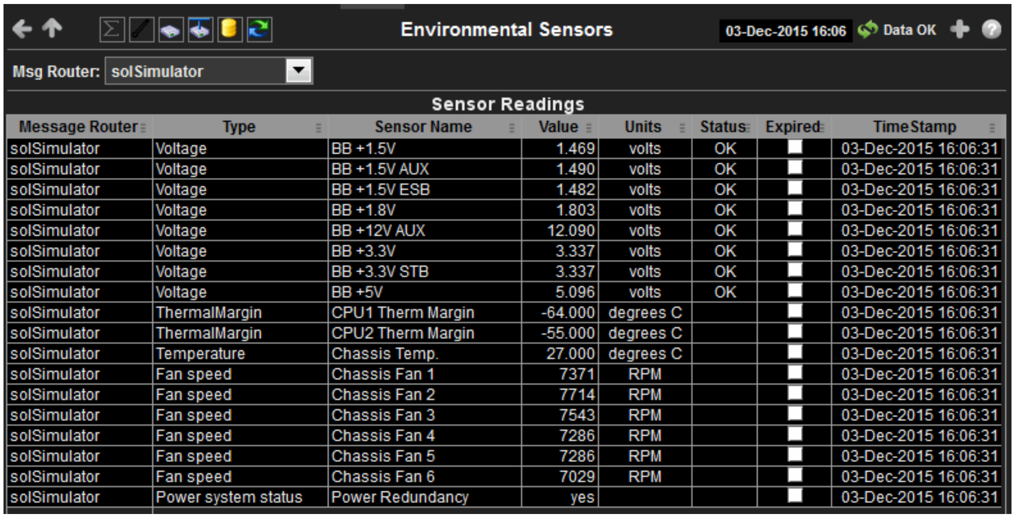
By default, the time range end point is the current time. To change the time range end point, click Calendar … and select a date and time from the calendar or enter the date and time in the text field using the following format: **MMM dd, YYYY HH:MM**. For example, **Aug 21, 2011 12:24 PM**.

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.



Msg Router: solSimulator

Sensor Readings

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:

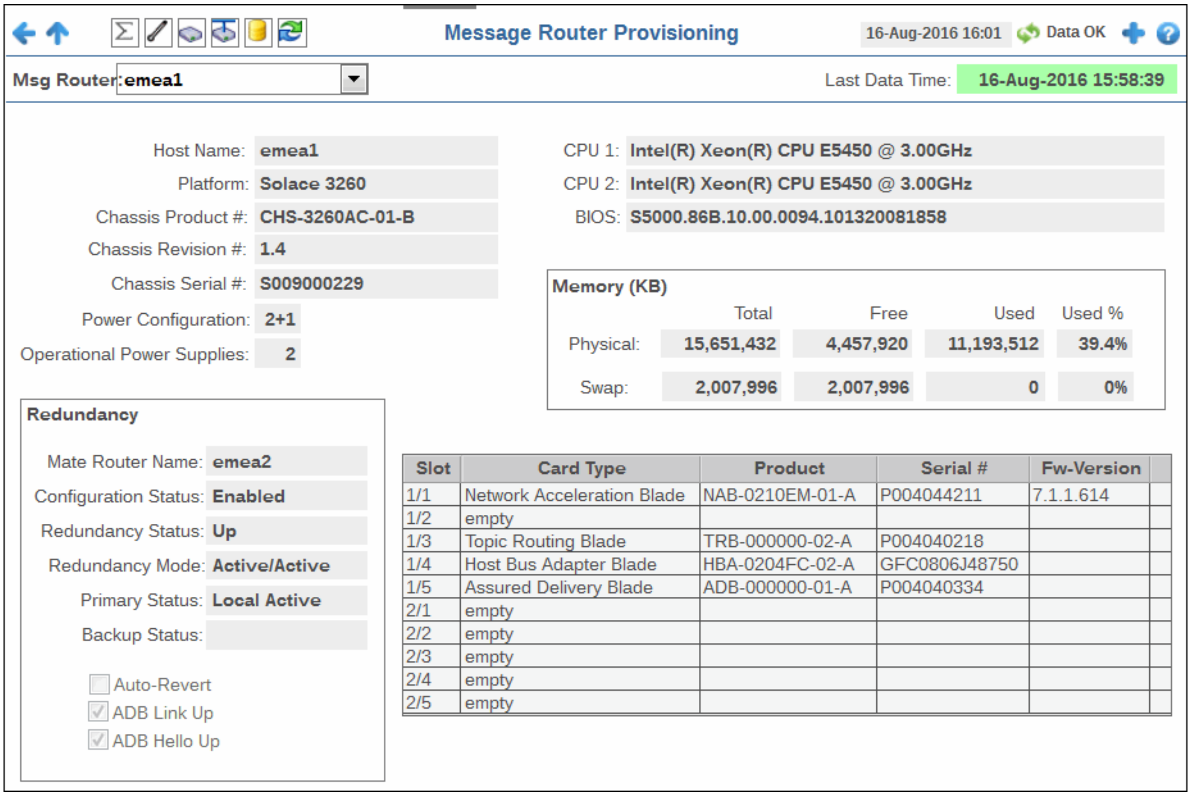
- When the display background color is ● (Red) the data is stale.
- The Last Data Time shows the date and time the selected message router was last updated.

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.



Message Router Provisioning 16-Aug-2016 16:01 Data OK

Msg Router: emea1

Last Data Time: 16-Aug-2016 15:58:39

Host Name:	emea1
Platform:	Solace 3260
Chassis Product #:	CHS-3260AC-01-B
Chassis Revision #:	1.4
Chassis Serial #:	S009000229
Power Configuration:	2+1
Operational Power Supplies:	2

CPU 1:	Intel(R) Xeon(R) CPU E5450 @ 3.00GHz
CPU 2:	Intel(R) Xeon(R) CPU E5450 @ 3.00GHz
BIOS:	S5000.86B.10.00.0094.101320081858

Memory (KB)

	Total	Free	Used	Used %
Physical:	15,651,432	4,457,920	11,193,512	39.4%
Swap:	2,007,996	2,007,996	0	0%

Redundancy

Mate Router Name:	emea2
Configuration Status:	Enabled
Redundancy Status:	Up
Redundancy Mode:	Active/Active
Primary Status:	Local Active
Backup Status:	

□ Auto-Revert
☑ ADB Link Up
☑ ADB Hello Up

Slot	Card Type	Product	Serial #	Fw-Version
1/1	Network Acceleration Blade	NAB-0210EM-01-A	P004044211	7.1.1.614
1/2	empty			
1/3	Topic Routing Blade	TRB-000000-02-A	P004040218	
1/4	Host Bus Adapter Blade	HBA-0204FC-02-A	GFC0806J48750	
1/5	Assured Delivery Blade	ADB-000000-01-A	P004040334	
2/1	empty			
2/2	empty			
2/3	empty			
2/4	empty			
2/5	empty			

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.

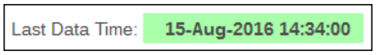
Interface Summary

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.

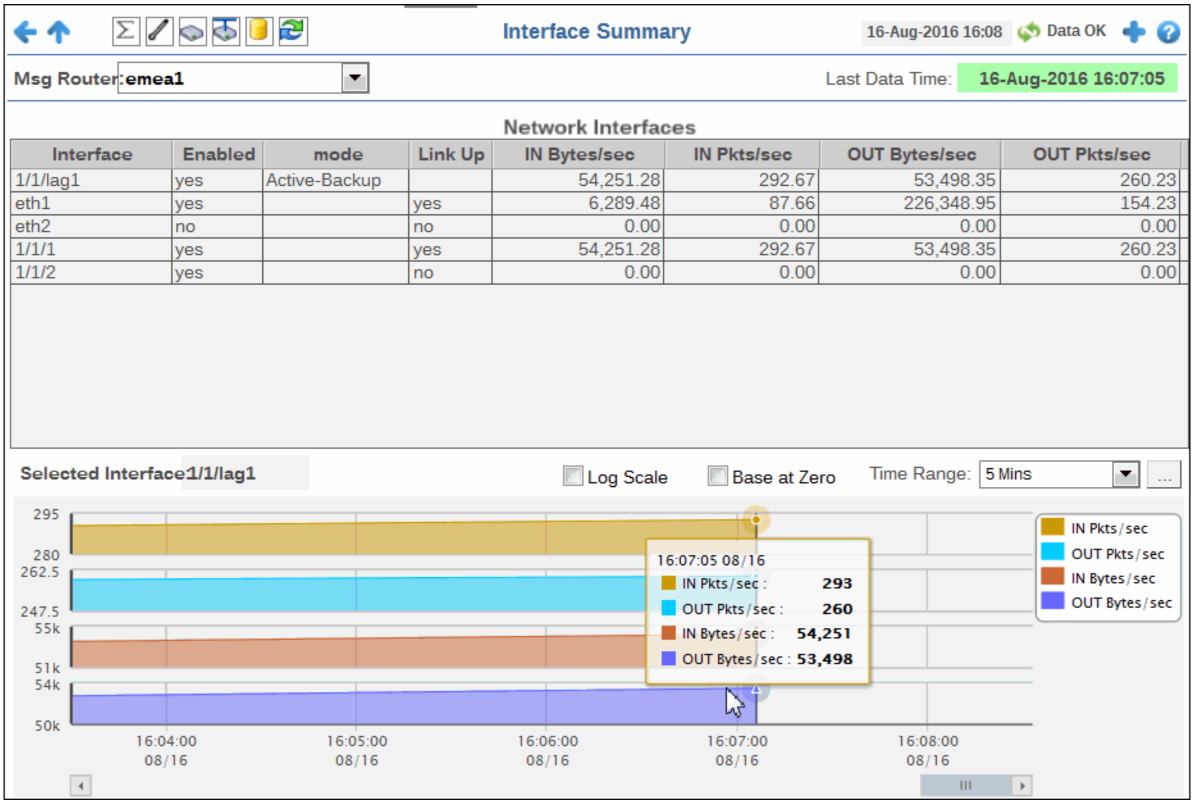


Last Data Time: 15-Aug-2016 14:34:00

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



Interface Summary

16-Aug-2016 16:08 Data OK

Msg Router: emea1

Last Data Time: 16-Aug-2016 16:07:05

Network Interfaces

Interface	Enabled	mode	Link Up	IN Bytes/sec	IN Pkts/sec	OUT Bytes/sec	OUT Pkts/sec
1/1/lag1	yes	Active-Backup		54,251.28	292.67	53,498.35	260.23
eth1	yes		yes	6,289.48	87.66	226,348.95	154.23
eth2	no		no	0.00	0.00	0.00	0.00
1/1/1	yes		yes	54,251.28	292.67	53,498.35	260.23
1/1/2	yes		no	0.00	0.00	0.00	0.00

Selected Interface: 1/1/lag1

□ Log Scale □ Base at Zero Time Range: 5 Mins

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 (Σ) 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.

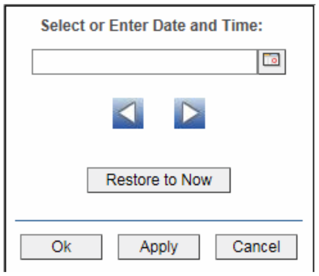
IN Bytes/sec Traces the number of bytes per second contained in the incoming messages.

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 ... .



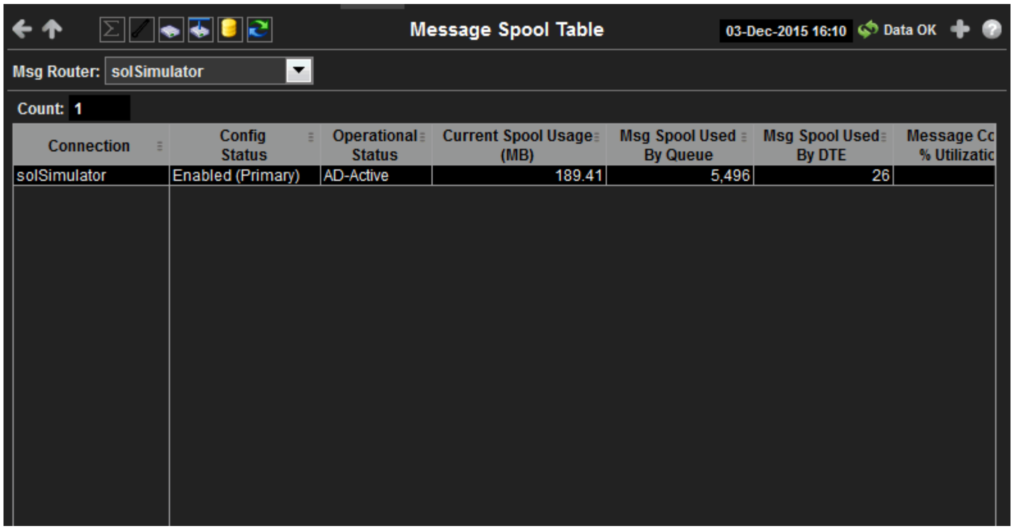
By default, the time range end point is the current time. To change the time range end point, click Calendar ... and select a date and time from the calendar or enter the date and time in the text field using the following format: **MMM dd, YYYY HH:MM**. For example, **Aug 21, 2011 12:24 PM**.

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.



Message Spool Table 03-Dec-2015 16:10 Data OK

Msg Router: solSimulator

Count: 1

Connection	Config Status	Operational Status	Current Spool Usage (MB)	Msg Spool Used By Queue	Msg Spool Used By DTE	Message Cc % Utilizatic
solSimulator	Enabled (Primary)	AD-Active	189.41	5,496	26	

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 (Σ) 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.

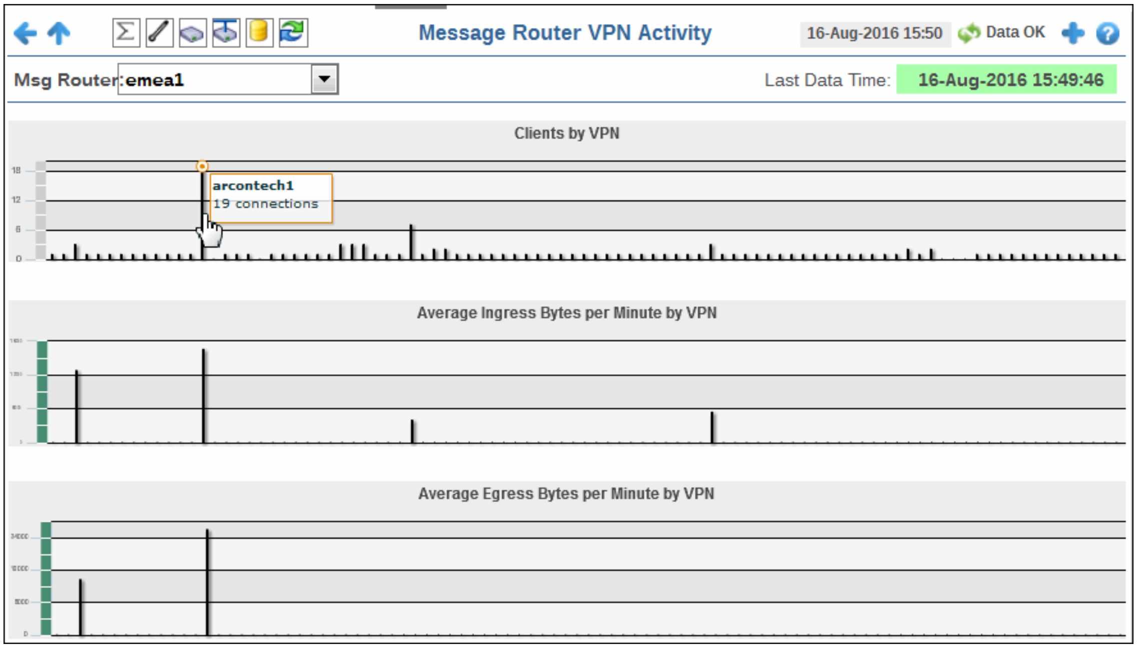
Last Data Time: 15-Aug-2016 14:34:00

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.

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.



Message Router VPN Activity 16-Aug-2016 15:50 Data OK

Msg Router: emea1

Last Data Time: 16-Aug-2016 15:49:46

Clients by VPN
18
12
6
0
arcontech1
19 connections
Average Ingress Bytes per Minute by VPN
1800
1200
600
0
Average Egress Bytes per Minute by VPN
24000
16000
8000
0

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.

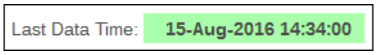
? Open the online help page for this display.

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:

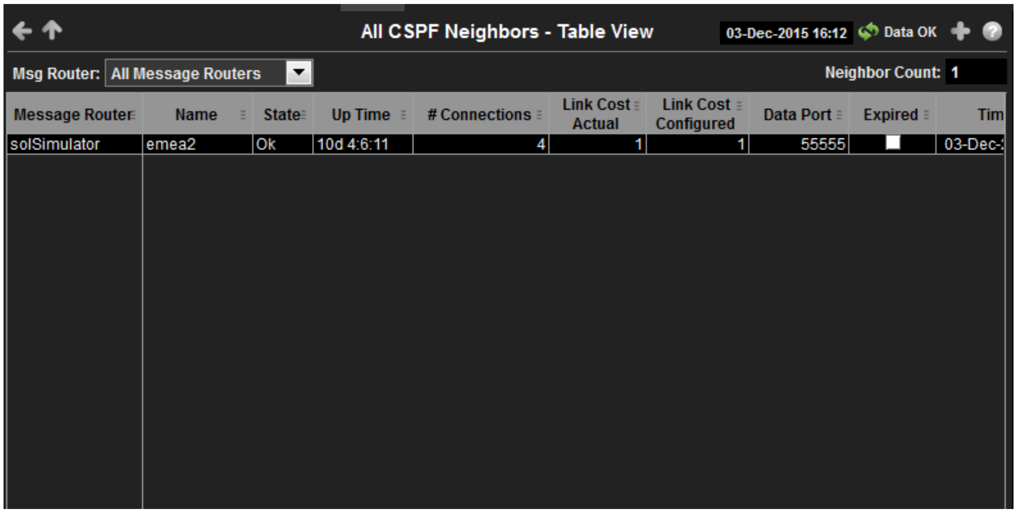
Clients Lists the clients and the number of connections for each client for the selected message router. Hovering over each client in the graph displays the exact number of connections for the clients.

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.



All CSPF Neighbors - Table View

03-Dec-2015 16:12 Data OK

Msg Router: All Message Routers

Neighbor Count: 1

Message Router	Name	State	Up Time	# Connections	Link Cost Actual	Link Cost Configured	Data Port	Expired	Tim
solSimulator	emea2	Ok	10d 4:6:11	4	1	1	55555	□	03-Dec-

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

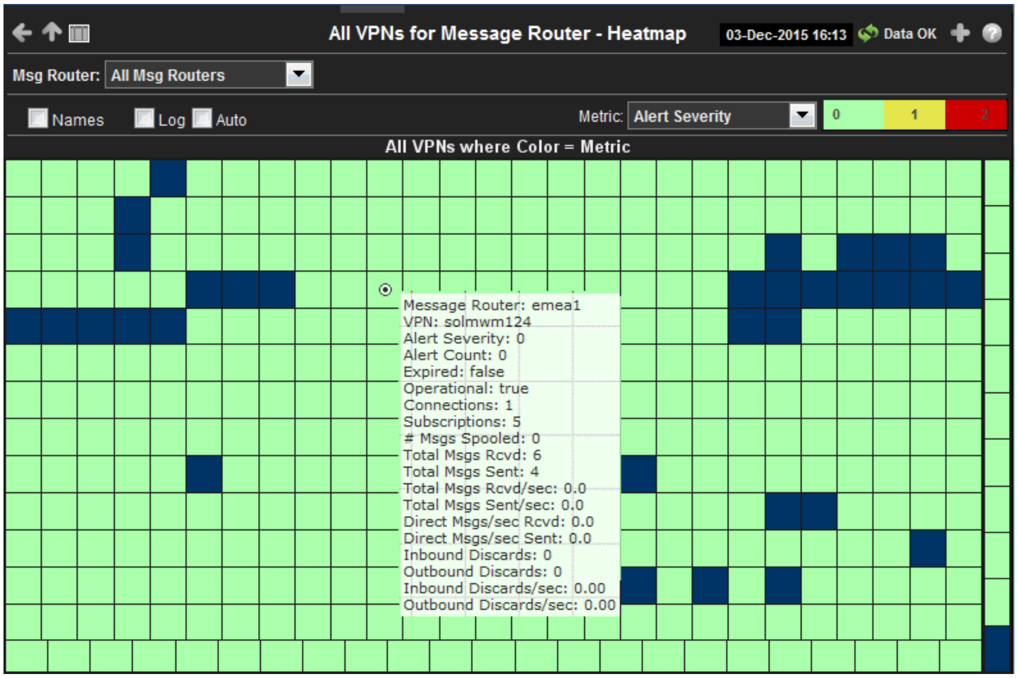
You can view data for all VPNs configured on a specific message router in heatmap, table, or grid formats, or you can view data for a single VPN. Displays in this View are:

- "All VPNs Heatmap" on page 54: A color-coded heatmap view of the current status of all VPNs configured on a specific message router.
- "All VPNs Table" on page 58: A tabular view of all available data for all VPNs configured on a specific router.
- "Top VPNs Grid" on page 61: Lists VPNs configured on a specific message router, in ascending or descending order, based on a selected metric.
- "Single VPN Summary" on page 63: 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.


All VPNs for Message Router - Heatmap
03-Dec-2015 16:13
Data OK
Names
Log
Auto
0
1
2
All VPNs where Color = Metric

Msg Router: All Msg Routers

Metric: Alert Severity

```
Message Router: emea1
VPN: solmwm124
Alert Severity: 0
Alert Count: 0
Expired: false
Operational: true
Connections: 1
Subscriptions: 5
# Msgs Spooled: 0
Total Msgs Rcvd: 6
Total Msgs Sent: 4
Total Msgs Rcvd/sec: 0.0
Total Msgs Sent/sec: 0.0
Direct Msgs/sec Rcvd: 0.0
Direct Msgs/sec Sent: 0.0
Inbound Discards: 0
Outbound Discards: 0
Inbound Discards/sec: 0.00
Outbound Discards/sec: 0.00
```

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 0 1 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 0 13 26 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 0 5 10 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 0 5 10 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 0 2.5 5 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 0 2.5 5 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 0 2.5 5 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 0 2.5 5 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 0 5 10 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 0 5 10 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.

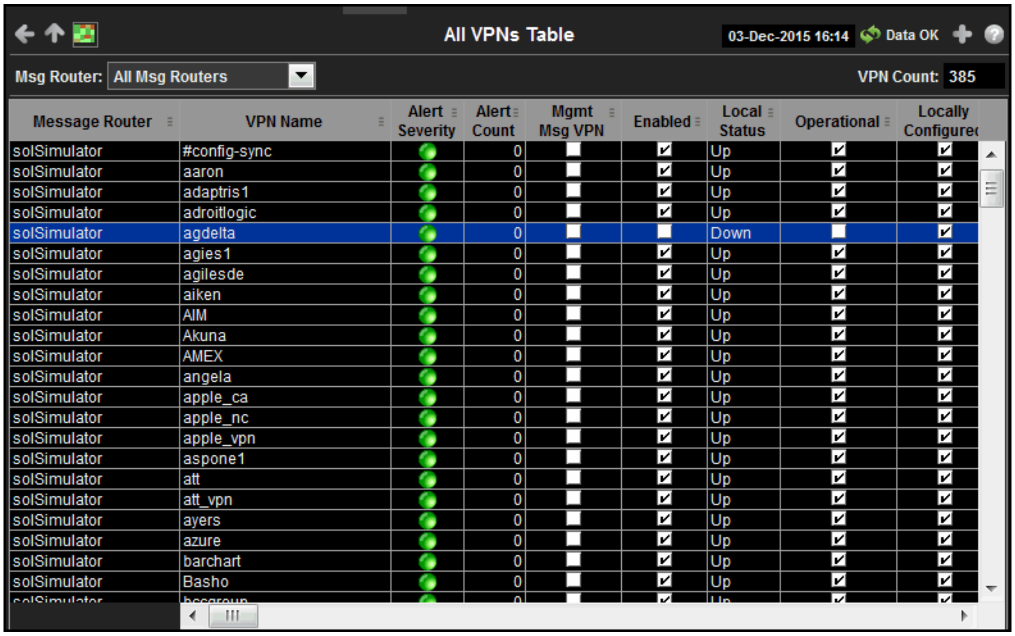
When **Auto** is checked, the numeric values in the color gradient bar show the range of the data being displayed rather than the default values. The middle value changes accordingly to indicate the color of the middle value of the range.

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.



All VPNs Table

03-Dec-2015 16:14 Data OK

Msg Router: All Msg Routers

VPN Count: 385

Message Router	VPN Name	Alert Severity	Alert Count	Mgmt Msg VPN	Enabled	Local Status	Operational	Locally Configurec
solSimulator	#config-sync	●	0	□	☑	Up	☑	☑
solSimulator	aaron	●	0	□	☑	Up	☑	☑
solSimulator	adaptris1	●	0	□	☑	Up	☑	☑
solSimulator	adroitlogic	●	0	□	☑	Up	☑	☑
solSimulator	agdelta	●	0	□	□	Down	□	☑
solSimulator	agies1	●	0	□	☑	Up	☑	☑
solSimulator	agilesde	●	0	□	☑	Up	☑	☑
solSimulator	aiken	●	0	□	☑	Up	☑	☑
solSimulator	AIM	●	0	□	☑	Up	☑	☑
solSimulator	Akuna	●	0	□	☑	Up	☑	☑
solSimulator	AMEX	●	0	□	☑	Up	☑	☑
solSimulator	angela	●	0	□	☑	Up	☑	☑
solSimulator	apple_ca	●	0	□	☑	Up	☑	☑
solSimulator	apple_nc	●	0	□	☑	Up	☑	☑
solSimulator	apple_vpn	●	0	□	☑	Up	☑	☑
solSimulator	aspone1	●	0	□	☑	Up	☑	☑
solSimulator	att	●	0	□	☑	Up	☑	☑
solSimulator	att_vpn	●	0	□	☑	Up	☑	☑
solSimulator	ayers	●	0	□	☑	Up	☑	☑
solSimulator	azure	●	0	□	☑	Up	☑	☑
solSimulator	barchart	●	0	□	☑	Up	☑	☑
solSimulator	Basho	●	0	□	☑	Up	☑	☑
solSimulator	bccgroup	●	0	□	☑	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: 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
```

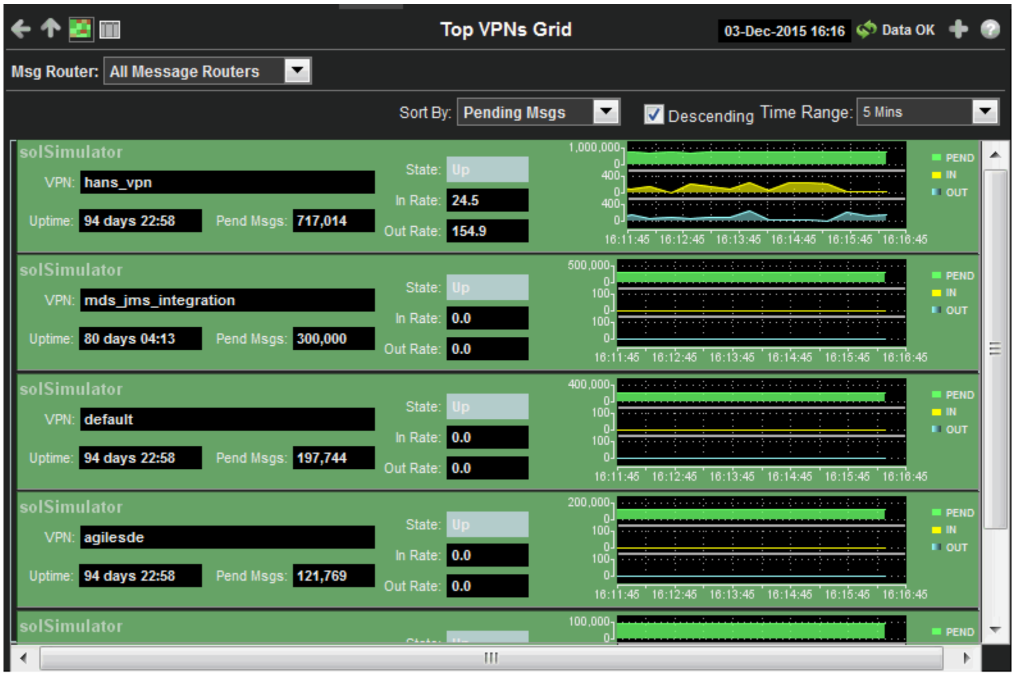
In the example above, the **Expired** check box would be checked after 45 seconds, and the row would be removed from the table after 3600 seconds.

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.



Top VPNs Grid 03-Dec-2015 16:16 Data OK

Msg Router: All Message Routers

Sort By: Pending Msgs ☑ Descending Time Range: 5 Mins

solSimulator
VPN: hans_vpn
Uptime: 94 days 22:58 Pend Msgs: 717,014
State: Up
In Rate: 24.5
Out Rate: 154.9

solSimulator
VPN: mds_jms_integration
Uptime: 80 days 04:13 Pend Msgs: 300,000
State: Up
In Rate: 0.0
Out Rate: 0.0

solSimulator
VPN: default
Uptime: 94 days 22:58 Pend Msgs: 197,744
State: Up
In Rate: 0.0
Out Rate: 0.0

solSimulator
VPN: agilesde
Uptime: 94 days 22:58 Pend Msgs: 121,769
State: Up
In Rate: 0.0
Out Rate: 0.0

solSimulator

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.

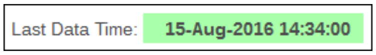
Trend Graph Displays, in graph form, the Pending Messages, In Message Rate/sec, and Out Message Rate/sec based on the selected **Time Range**. For example, if **20 Mins** was selected in the **Time Range** drop down, the graph displays the total pending messages (**Pend**), the incoming message rates (**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.

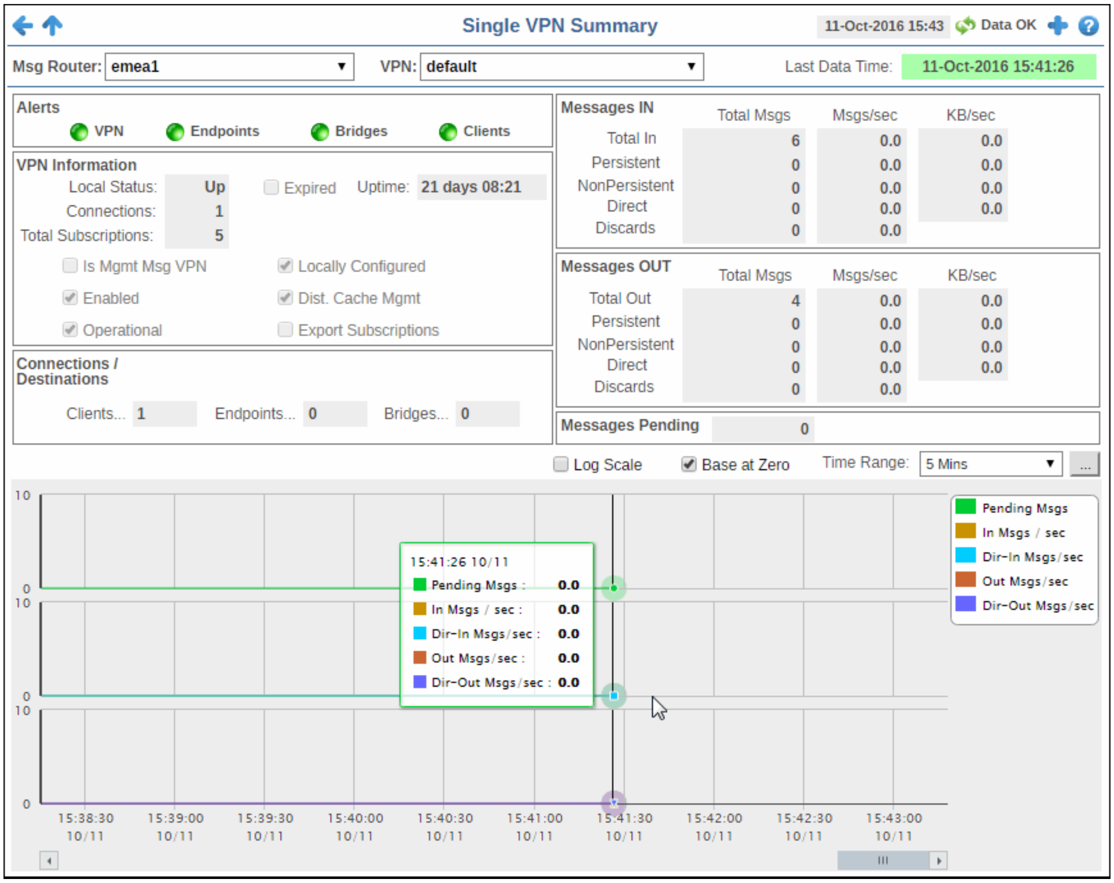


Last Data Time: 15-Aug-2016 14:34:00

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.



Single VPN Summary 11-Oct-2016 15:43 Data OK

Msg Router: emea1 VPN: default Last Data Time: 11-Oct-2016 15:41:26

Alerts

● VPN ● Endpoints ● Bridges ● Clients

VPN Information

Local Status: Up □ Expired Uptime: 21 days 08:21

Connections: 1

Total Subscriptions: 5

□ Is Mgmt Msg VPN ☑ Locally Configured

☑ Enabled ☑ Dist. Cache Mgmt

☑ Operational □ Export Subscriptions

Connections / Destinations

Clients... 1 Endpoints... 0 Bridges... 0

Messages IN	Total Msgs	Msgs/sec	KB/sec
Total In	6	0.0	0.0
Persistent	0	0.0	0.0
NonPersistent	0	0.0	0.0
Direct	0	0.0	0.0
Discards	0	0.0	

Messages OUT	Total Msgs	Msgs/sec	KB/sec
Total Out	4	0.0	0.0
Persistent	0	0.0	0.0
NonPersistent	0	0.0	0.0
Direct	0	0.0	0.0
Discards	0	0.0	

Messages Pending 0

□ Log Scale ☑ Base at Zero Time Range: 5 Mins

15:41:26 10/11

🟩 Pending Msgs : 0.0

🟧 In Msgs / sec : 0.0

🟦 Dir-In Msgs/sec : 0.0

🟫 Out Msgs/sec : 0.0

🟪 Dir-Out Msgs/sec : 0.0

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:36
00
```

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.

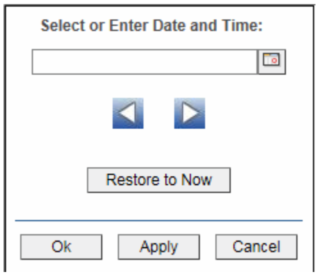
Trend Graphs
Traces the sum of process metrics for the VPN associated with the selected message router.

- **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.

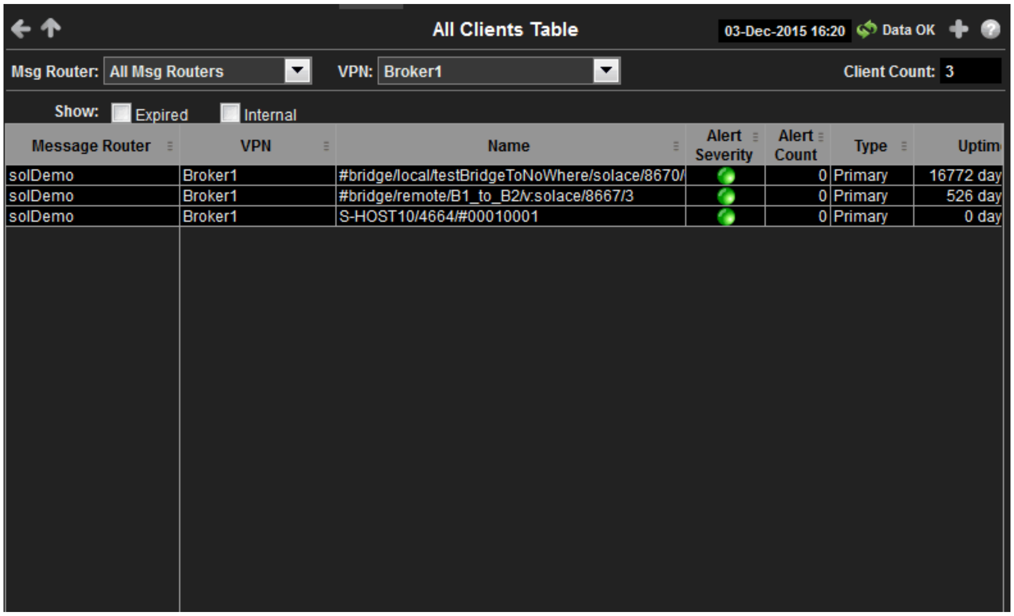
Clients

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 68: A color-coded heatmap view of data for all clients configured on a VPN.
- "Single Client Summary" on page 73: 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.



← ↑ All Clients Table 03-Dec-2015 16:20 Data OK ✚ ?

Msg Router: All Msg Routers VPN: Broker1 Client Count: 3

Show: □ Expired □ Internal

Message Router	VPN	Name	Alert Severity	Alert Count	Type	Uptim
solDemo	Broker1	#bridge/local/testBridgeToNoWhere/solace/8670/	🟢	0	Primary	16772 day
solDemo	Broker1	#bridge/remote/B1_to_B2/v:solace/8667/3	🟢	0	Primary	526 day
solDemo	Broker1	S-HOST10/4664/#00010001	🟢	0	Primary	0 day

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.

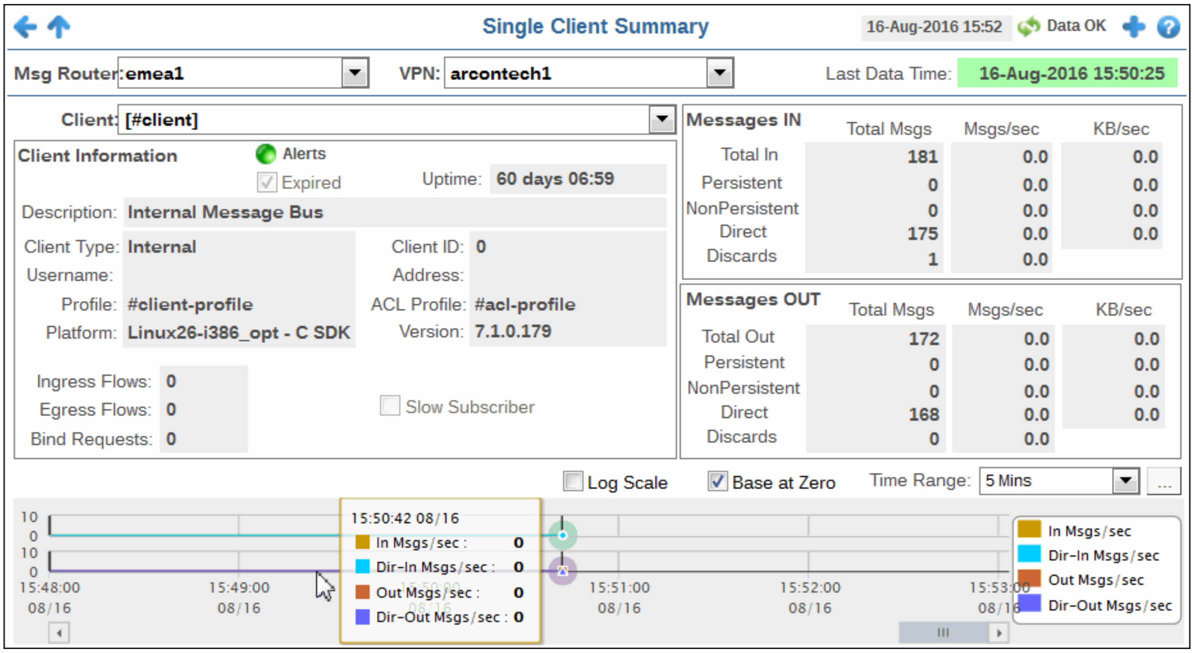
Last Data Time: 15-Aug-2016 14:34:00

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.



Single Client Summary 16-Aug-2016 15:52 Data OK

Msg Router: emea1 VPN: arcontech1 Last Data Time: 16-Aug-2016 15:50:25

Client: [#client]

Client Information Alerts

☑ Expired Uptime: 60 days 06:59

Description: Internal Message Bus

Client Type: Internal Client ID: 0

Username: Address:

Profile: #client-profile ACL Profile: #acl-profile

Platform: Linux26-i386_opt - C SDK Version: 7.1.0.179

Ingress Flows: 0

Egress Flows: 0

Bind Requests: 0

□ Slow Subscriber

Messages IN	Total Msgs	Msgs/sec	KB/sec
Total In	181	0.0	0.0
Persistent	0	0.0	0.0
NonPersistent	0	0.0	0.0
Direct	175	0.0	0.0
Discards	1	0.0	

Messages OUT	Total Msgs	Msgs/sec	KB/sec
Total Out	172	0.0	0.0
Persistent	0	0.0	0.0
NonPersistent	0	0.0	0.0
Direct	168	0.0	0.0
Discards	0	0.0	

□ Log Scale ☑ Base at Zero Time Range: 5 Mins

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:36
00
```

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

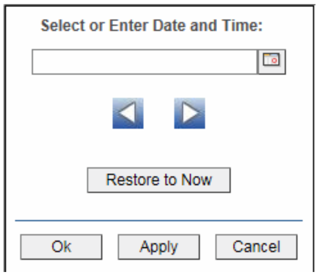
Traces the sum of process metrics for the client associated with the selected message router and VPN.

- **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.

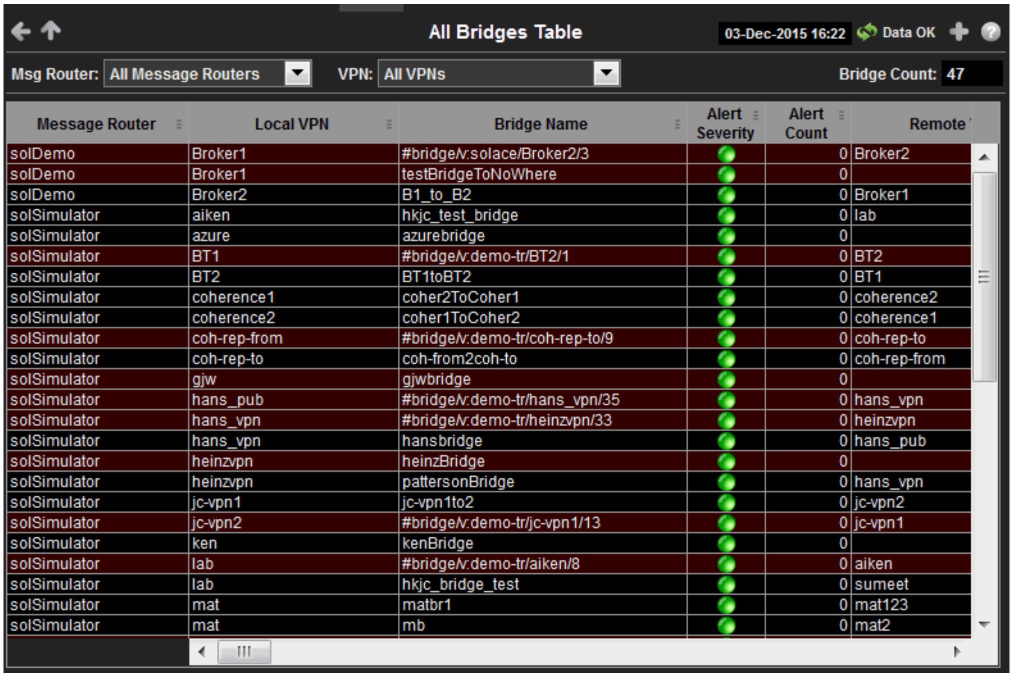
Bridges

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

- "All Bridges" on page 78: A tabular view of all available process performance data for all bridges configured on a VPN.
- "Single Bridge Summary" on page 81: 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.



All Bridges Table

03-Dec-2015 16:22 Data OK

Msg Router: All Message Routers VPN: All VPNs Bridge Count: 47

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.

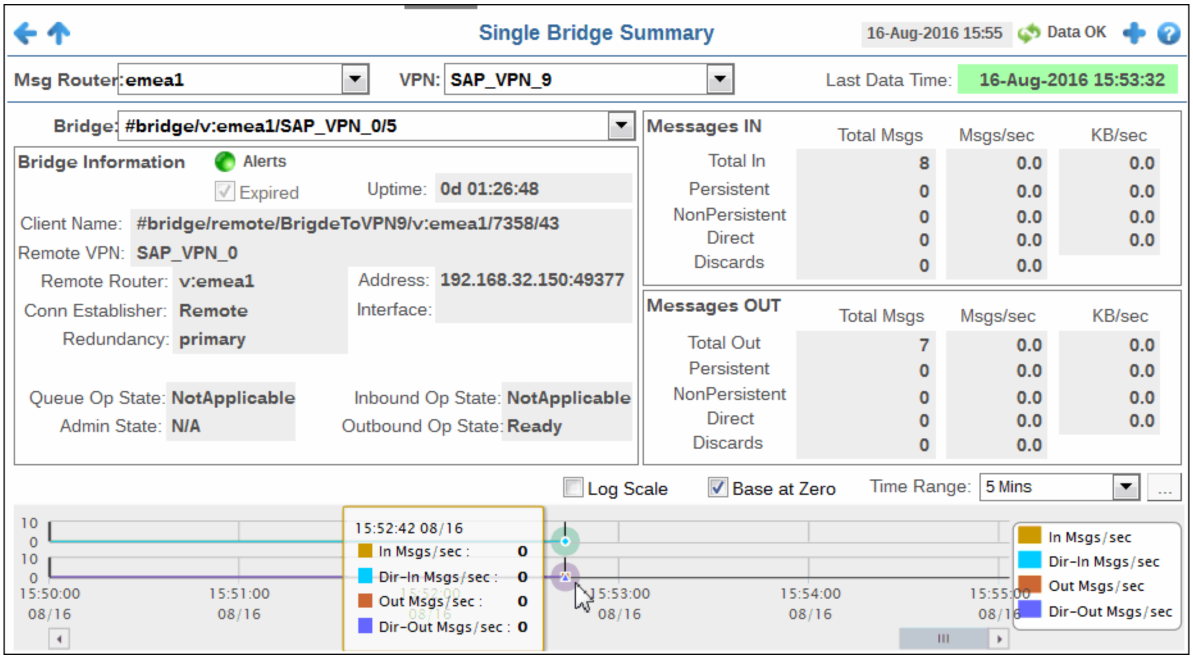
Last Data Time: 15-Aug-2016 14:34:00

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.



Single Bridge Summary 16-Aug-2016 15:55 Data OK

Msg Router: emea1 VPN: SAP_VPN_9 Last Data Time: 16-Aug-2016 15:53:32

Bridge: #bridge/v:emea1/SAP_VPN_0/5

Bridge Information ● Alerts ☑ Expired Uptime: 0d 01:26:48

Client Name: #bridge/remote/BrigdeToVPN9/v:emea1/7358/43

Remote VPN: SAP_VPN_0

Remote Router: v:emea1 Address: 192.168.32.150:49377

Conn Establisher: Remote Interface:

Redundancy: primary

Queue Op State: NotApplicable Inbound Op State: NotApplicable

Admin State: N/A Outbound Op State: Ready

Messages IN	Total Msgs	Msgs/sec	KB/sec
Total In	8	0.0	0.0
Persistent	0	0.0	0.0
NonPersistent	0	0.0	0.0
Direct	0	0.0	0.0
Discards	0	0.0	

Messages OUT	Total Msgs	Msgs/sec	KB/sec
Total Out	7	0.0	0.0
Persistent	0	0.0	0.0
NonPersistent	0	0.0	0.0
Direct	0	0.0	0.0
Discards	0	0.0	

□ Log Scale ☑ Base at Zero Time Range: 5 Mins

15:52:42 08/16
In Msgs/sec : 0
Dir-In Msgs/sec : 0
Out Msgs/sec : 0
Dir-Out Msgs/sec : 0

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:36
00
```

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

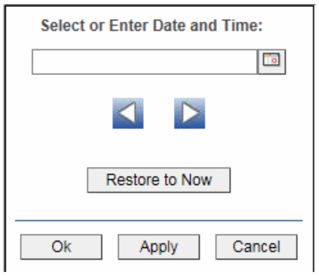
Traces the sum of process metrics for the client associated with the selected message router and VPN.

- **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.

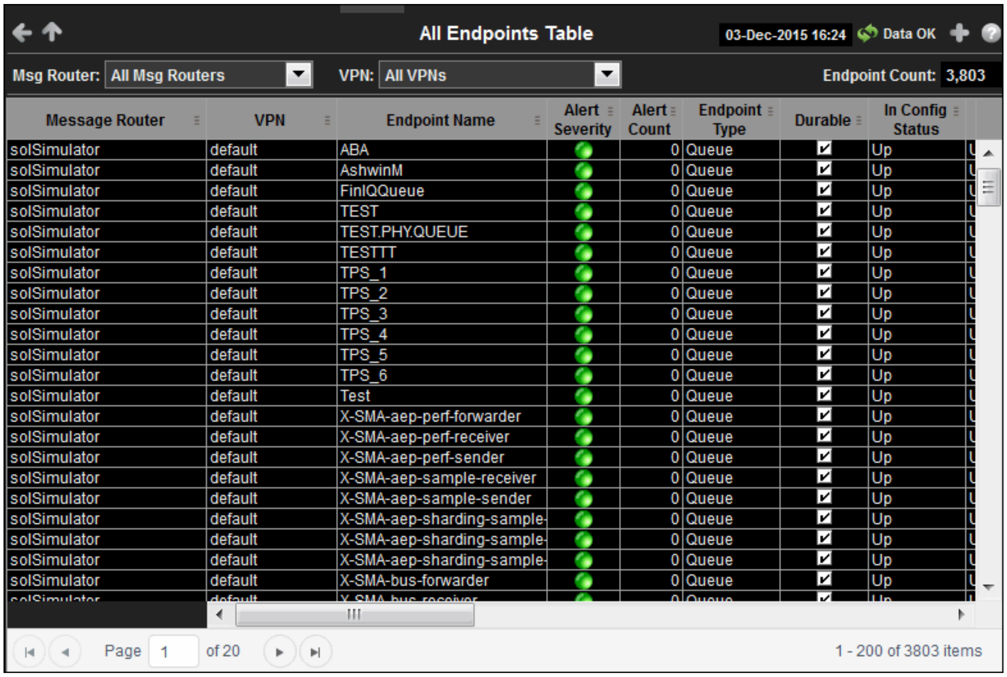
Endpoints

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

- "All Endpoints" on page 86
- "Single Endpoint Summary" on page 88
- "Single Endpoint Summary Rates" on page 91

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.



All Endpoints Table 03-Dec-2015 16:24 Data OK

Msg Router: All Msg Routers VPN: All VPNs Endpoint Count: 3,803

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

Page 1 of 20 1 - 200 of 3803 items

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.

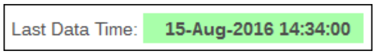
Time Stamp The date and time the data was last updated.

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.



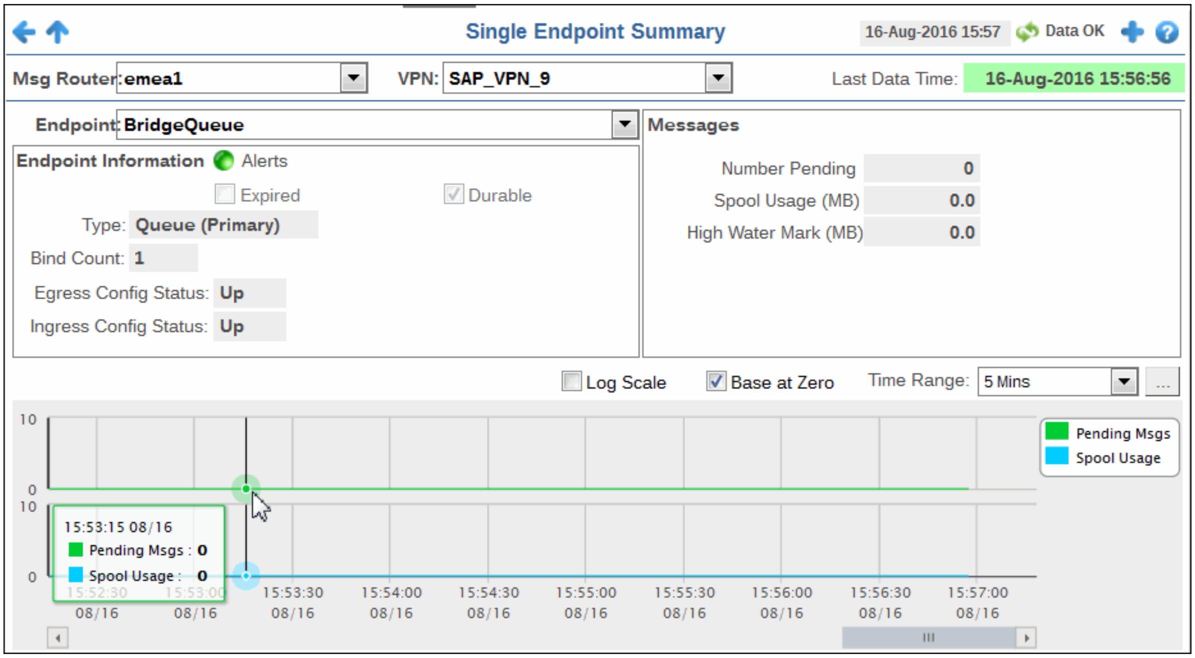
Last Data Time: 15-Aug-2016 14:34:00

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 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.



Single Endpoint Summary 16-Aug-2016 15:57 Data OK

Msg Router: emea1 VPN: SAP_VPN_9 Last Data Time: 16-Aug-2016 15:56:56

Endpoint: BridgeQueue

Endpoint Information ● Alerts

□ Expired ☑ Durable

Type: Queue (Primary)

Bind Count: 1

Egress Config Status: Up

Ingress Config Status: Up

Messages

Number Pending 0

Spool Usage (MB) 0.0

High Water Mark (MB) 0.0

□ Log Scale ☑ Base at Zero Time Range: 5 Mins

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

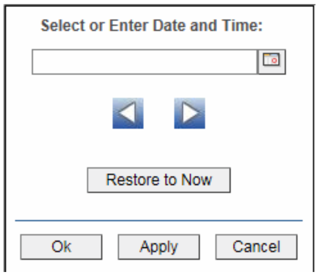
Traces the sum of process metrics for the endpoint associated with the selected message router and VPN.

- **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.

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.

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 **-->**):

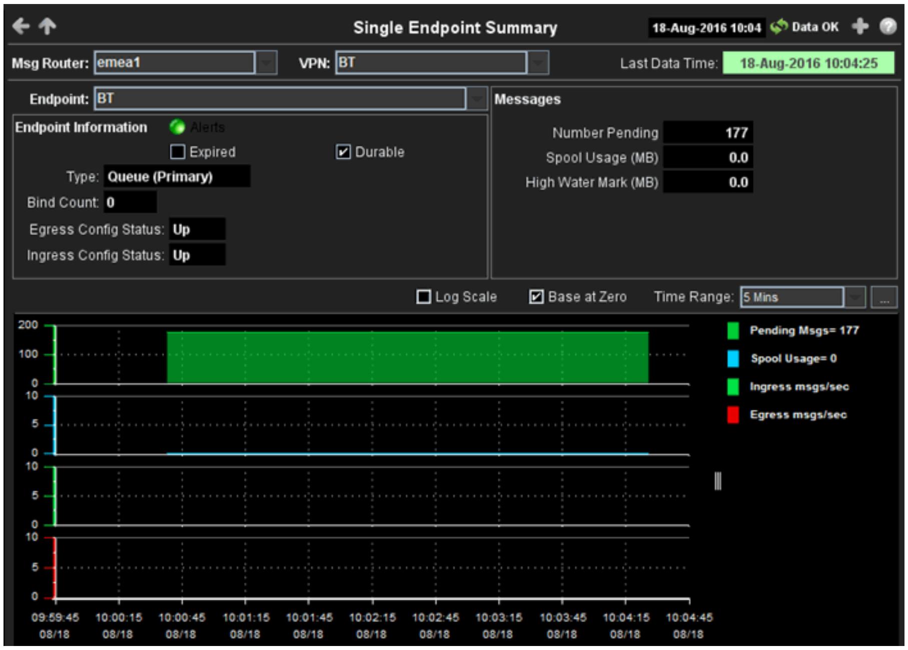
   ```
   <node label="Single Endpoint Summary" display="sol_endpoint_summary"></node>
   ```

   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.



Single Endpoint Summary 18-Aug-2016 10:04 Data OK

Msg Router: emea1 VPN: BT Last Data Time: 18-Aug-2016 10:04:25

Endpoint: BT

Endpoint Information ● Alerts

□ Expired ☑ Durable

Type: Queue (Primary)

Bind Count: 0

Egress Config Status: Up

Ingress Config Status: Up

Messages

Number Pending	177
Spool Usage (MB)	0.0
High Water Mark (MB)	0.0

□ Log Scale ☑ Base at Zero Time Range: 5 Mins

🟩 Pending Msgs= 177

🟦 Spool Usage= 0

🟩 Ingress msgs/sec

🟥 Egress msgs/sec

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).

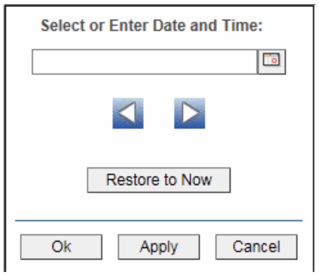
Trend Graphs
Traces the sum of process metrics for the endpoint associated with the selected message router and VPN.

- **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.

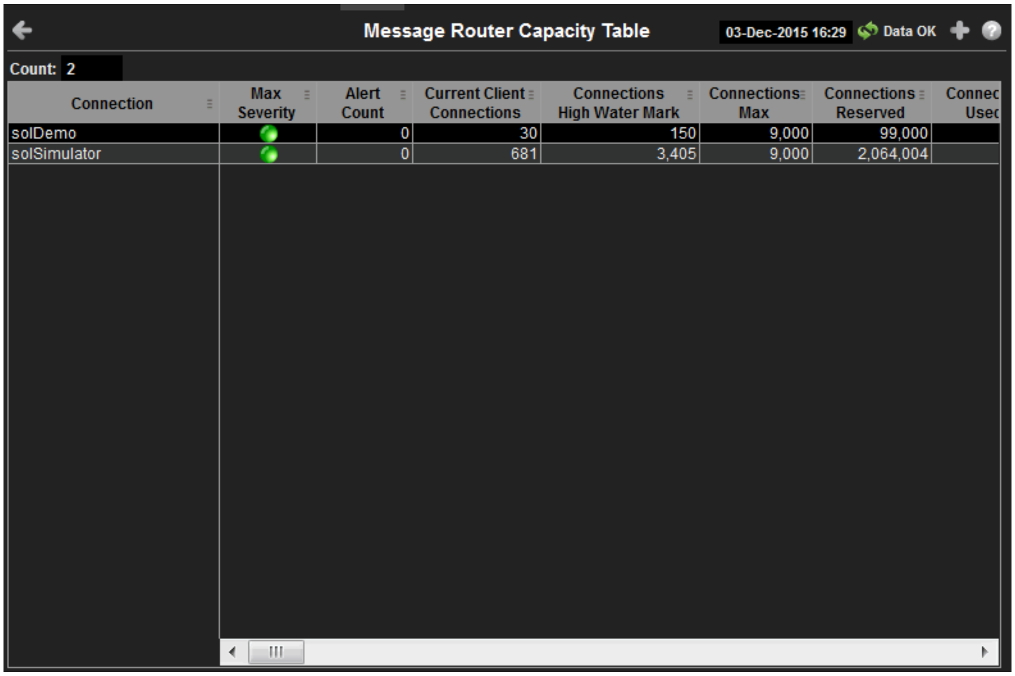
Capacity Analysis

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 95: View client, spool usage, incoming messages, outgoing messages, incoming bytes, and outgoing bytes data for all message routers.
- "Message Router Capacity" on page 98: 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 102: 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.



Message Router Capacity Table

03-Dec-2015 16:29 Data OK

Count: 2

Connection	Max Severity	Alert Count	Current Client Connections	Connections High Water Mark	Connections Max	Connections Reserved	Connec Usec
solDemo	●	0	30	150	9,000	99,000	
solSimulator	●	0	681	3,405	9,000	2,064,004	

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:

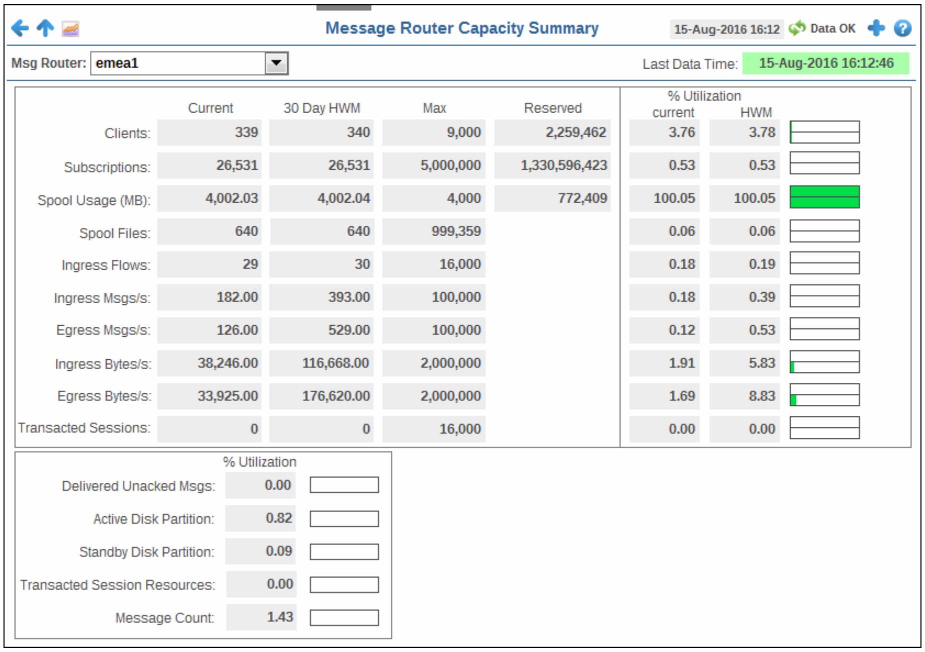
- When the display background color is ● (Red) the data is stale.
- The Last Data Time shows the date and time the selected message router was last updated.

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.



Message Router Capacity Summary

15-Aug-2016 16:12 Data OK

Msg Router: emea1

Last Data Time: 15-Aug-2016 16:12:46

	Current	30 Day HWM	Max	Reserved	% Utilization current	% Utilization HWM
Clients:	339	340	9,000	2,259,462	3.76	3.78
Subscriptions:	26,531	26,531	5,000,000	1,330,596,423	0.53	0.53
Spool Usage (MB):	4,002.03	4,002.04	4,000	772,409	100.05	100.05
Spool Files:	640	640	999,359		0.06	0.06
Ingress Flows:	29	30	16,000		0.18	0.19
Ingress Msgs/s:	182.00	393.00	100,000		0.18	0.39
Egress Msgs/s:	126.00	529.00	100,000		0.12	0.53
Ingress Bytes/s:	38,246.00	116,668.00	2,000,000		1.91	5.83
Egress Bytes/s:	33,925.00	176,620.00	2,000,000		1.69	8.83
Transacted Sessions:	0	0	16,000		0.00	0.00

	% Utilization
Delivered Unacked Msgs:	0.00
Active Disk Partition:	0.82
Standby Disk Partition:	0.09
Transacted Session Resources:	0.00
Message Count:	1.43

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:

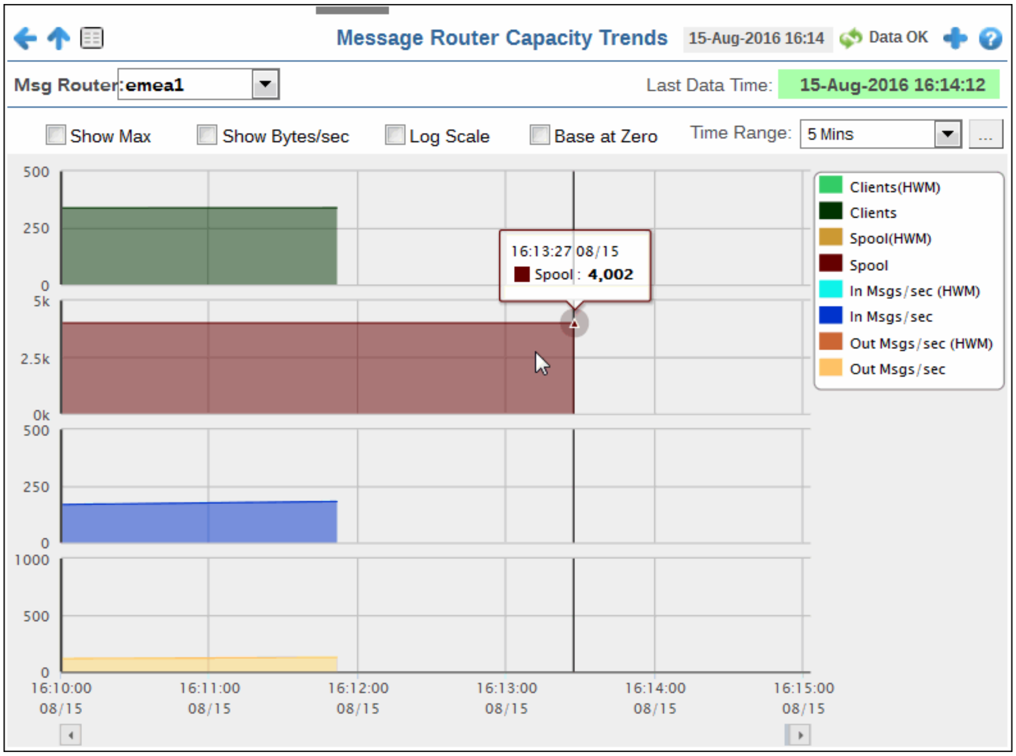
- When the display background color is 🔴 (Red) the data is stale.
- The Last Data Time shows the date and time the selected message router was last updated.

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.



Message Router Capacity Trends 15-Aug-2016 16:14 Data OK

Msg Router: emea1

Last Data Time: 15-Aug-2016 16:14:12

☐ Show Max ☐ Show Bytes/sec ☐ Log Scale ☐ Base at Zero Time Range: 5 Mins

16:13:27 08/15
Spool : 4,002

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.

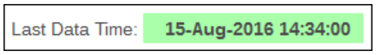
✚ Open an instance of this display in a new window.

? 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.

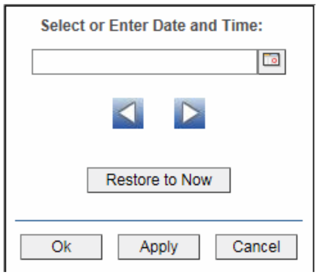
Show Max Selecting this toggle changes metrics using **HWM** (high water mark) to **Max** (maximum value). For example, **Clients (HWM)** becomes **Clients (Max)** and the values in the graph are updated accordingly.

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

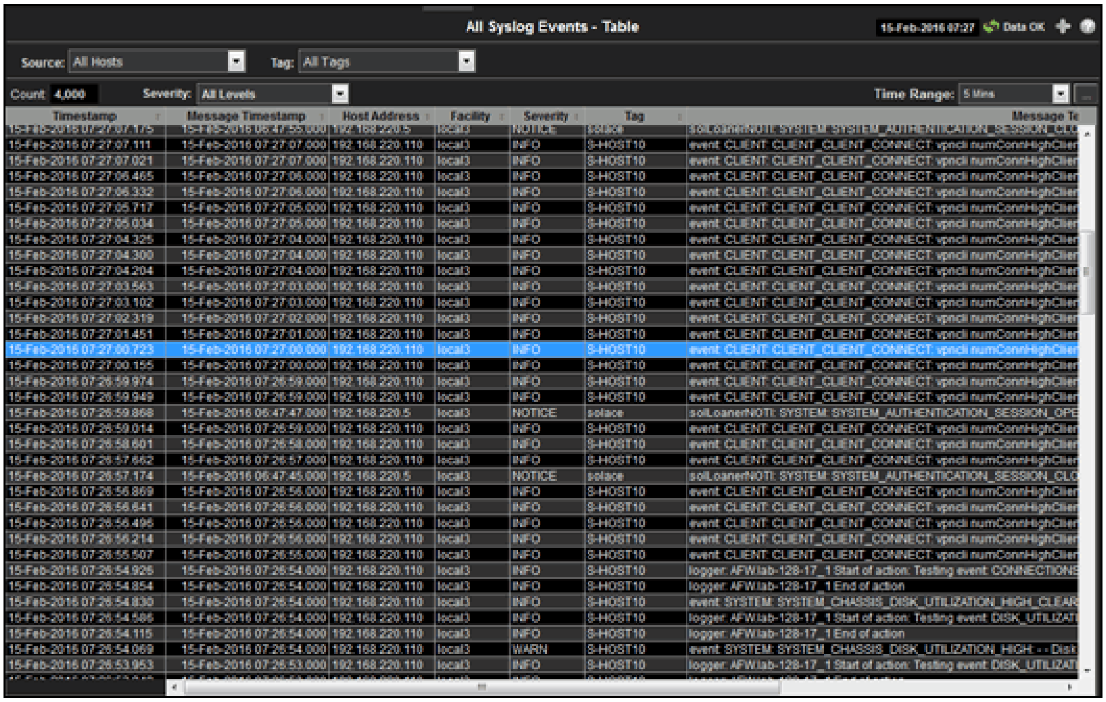
The display in this View provides a tabular list of all Syslog events:

- "All Syslog Events Table" on page 105: 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.



All Syslog Events - Table

15-Feb-2016 07:27 Data OK

Source: All Hosts Tag: All Tags

Count: 4,000 Severity: All Levels Time Range: 5 Mins

Timestamp	Message Timestamp	Host Address	Facility	Severity	Tag	Message Te
15-Feb-2016 07:27:07.175	15-Feb-2016 06:47:55.000	192.168.220.5	local3	NOTICE	solace	solLoanerNOTI: SYSTEM: SYSTEM_AUTHENTICATION_SESSION_CLO
15-Feb-2016 07:27:07.111	15-Feb-2016 07:27:07.000	192.168.220.110	local3	INFO	S-HOST10	event: CLIENT: CLIENT_CLIENT_CONNECT: vpncli numConnHighClien
15-Feb-2016 07:27:07.021	15-Feb-2016 07:27:07.000	192.168.220.110	local3	INFO	S-HOST10	event: CLIENT: CLIENT_CLIENT_CONNECT: vpncli numConnHighClien
15-Feb-2016 07:27:06.465	15-Feb-2016 07:27:06.000	192.168.220.110	local3	INFO	S-HOST10	event: CLIENT: CLIENT_CLIENT_CONNECT: vpncli numConnHighClien
15-Feb-2016 07:27:06.332	15-Feb-2016 07:27:06.000	192.168.220.110	local3	INFO	S-HOST10	event: CLIENT: CLIENT_CLIENT_CONNECT: vpncli numConnHighClien
15-Feb-2016 07:27:05.717	15-Feb-2016 07:27:05.000	192.168.220.110	local3	INFO	S-HOST10	event: CLIENT: CLIENT_CLIENT_CONNECT: vpncli numConnHighClien
15-Feb-2016 07:27:05.034	15-Feb-2016 07:27:05.000	192.168.220.110	local3	INFO	S-HOST10	event: CLIENT: CLIENT_CLIENT_CONNECT: vpncli numConnHighClien
15-Feb-2016 07:27:04.325	15-Feb-2016 07:27:04.000	192.168.220.110	local3	INFO	S-HOST10	event: CLIENT: CLIENT_CLIENT_CONNECT: vpncli numConnHighClien
15-Feb-2016 07:27:04.300	15-Feb-2016 07:27:04.000	192.168.220.110	local3	INFO	S-HOST10	event: CLIENT: CLIENT_CLIENT_CONNECT: vpncli numConnHighClien
15-Feb-2016 07:27:04.204	15-Feb-2016 07:27:04.000	192.168.220.110	local3	INFO	S-HOST10	event: CLIENT: CLIENT_CLIENT_CONNECT: vpncli numConnHighClien
15-Feb-2016 07:27:03.563	15-Feb-2016 07:27:03.000	192.168.220.110	local3	INFO	S-HOST10	event: CLIENT: CLIENT_CLIENT_CONNECT: vpncli numConnHighClien
15-Feb-2016 07:27:03.102	15-Feb-2016 07:27:03.000	192.168.220.110	local3	INFO	S-HOST10	event: CLIENT: CLIENT_CLIENT_CONNECT: vpncli numConnHighClien
15-Feb-2016 07:27:02.319	15-Feb-2016 07:27:02.000	192.168.220.110	local3	INFO	S-HOST10	event: CLIENT: CLIENT_CLIENT_CONNECT: vpncli numConnHighClien
15-Feb-2016 07:27:01.451	15-Feb-2016 07:27:01.000	192.168.220.110	local3	INFO	S-HOST10	event: CLIENT: CLIENT_CLIENT_CONNECT: vpncli numConnHighClien
15-Feb-2016 07:27:00.723	15-Feb-2016 07:27:00.000	192.168.220.110	local3	INFO	S-HOST10	event: CLIENT: CLIENT_CLIENT_CONNECT: vpncli numConnHighClien
15-Feb-2016 07:27:00.155	15-Feb-2016 07:27:00.000	192.168.220.110	local3	INFO	S-HOST10	event: CLIENT: CLIENT_CLIENT_CONNECT: vpncli numConnHighClien
15-Feb-2016 07:26:59.974	15-Feb-2016 07:26:59.000	192.168.220.110	local3	INFO	S-HOST10	event: CLIENT: CLIENT_CLIENT_CONNECT: vpncli numConnHighClien
15-Feb-2016 07:26:59.949	15-Feb-2016 07:26:59.000	192.168.220.110	local3	INFO	S-HOST10	event: CLIENT: CLIENT_CLIENT_CONNECT: vpncli numConnHighClien
15-Feb-2016 07:26:59.868	15-Feb-2016 06:47:47.000	192.168.220.5	local3	NOTICE	solace	solLoanerNOTI: SYSTEM: SYSTEM_AUTHENTICATION_SESSION_OPE
15-Feb-2016 07:26:59.014	15-Feb-2016 07:26:59.000	192.168.220.110	local3	INFO	S-HOST10	event: CLIENT: CLIENT_CLIENT_CONNECT: vpncli numConnHighClien
15-Feb-2016 07:26:58.601	15-Feb-2016 07:26:58.000	192.168.220.110	local3	INFO	S-HOST10	event: CLIENT: CLIENT_CLIENT_CONNECT: vpncli numConnHighClien
15-Feb-2016 07:26:57.662	15-Feb-2016 07:26:57.000	192.168.220.110	local3	INFO	S-HOST10	event: CLIENT: CLIENT_CLIENT_CONNECT: vpncli numConnHighClien
15-Feb-2016 07:26:57.174	15-Feb-2016 06:47:45.000	192.168.220.5	local3	NOTICE	solace	solLoanerNOTI: SYSTEM: SYSTEM_AUTHENTICATION_SESSION_CLO
15-Feb-2016 07:26:56.869	15-Feb-2016 07:26:56.000	192.168.220.110	local3	INFO	S-HOST10	event: CLIENT: CLIENT_CLIENT_CONNECT: vpncli numConnHighClien
15-Feb-2016 07:26:56.641	15-Feb-2016 07:26:56.000	192.168.220.110	local3	INFO	S-HOST10	event: CLIENT: CLIENT_CLIENT_CONNECT: vpncli numConnHighClien
15-Feb-2016 07:26:56.498	15-Feb-2016 07:26:56.000	192.168.220.110	local3	INFO	S-HOST10	event: CLIENT: CLIENT_CLIENT_CONNECT: vpncli numConnHighClien
15-Feb-2016 07:26:56.214	15-Feb-2016 07:26:56.000	192.168.220.110	local3	INFO	S-HOST10	event: CLIENT: CLIENT_CLIENT_CONNECT: vpncli numConnHighClien
15-Feb-2016 07:26:55.507	15-Feb-2016 07:26:55.000	192.168.220.110	local3	INFO	S-HOST10	event: CLIENT: CLIENT_CLIENT_CONNECT: vpncli numConnHighClien
15-Feb-2016 07:26:54.926	15-Feb-2016 07:26:54.000	192.168.220.110	local3	INFO	S-HOST10	logger: AFW.lab-128-17_1 Start of action: Testing event: CONNECTIONS
15-Feb-2016 07:26:54.854	15-Feb-2016 07:26:54.000	192.168.220.110	local3	INFO	S-HOST10	logger: AFW.lab-128-17_1 End of action
15-Feb-2016 07:26:54.830	15-Feb-2016 07:26:54.000	192.168.220.110	local3	INFO	S-HOST10	event: SYSTEM: SYSTEM_CHASSIS_DISK_UTILIZATION_HIGH_CLEAR
15-Feb-2016 07:26:54.586	15-Feb-2016 07:26:54.000	192.168.220.110	local3	INFO	S-HOST10	logger: AFW.lab-128-17_1 Start of action: Testing event: DISK_UTILIZATI
15-Feb-2016 07:26:54.115	15-Feb-2016 07:26:54.000	192.168.220.110	local3	INFO	S-HOST10	logger: AFW.lab-128-17_1 End of action
15-Feb-2016 07:26:54.069	15-Feb-2016 07:26:54.000	192.168.220.110	local3	WARN	S-HOST10	event: SYSTEM: SYSTEM_CHASSIS_DISK_UTILIZATION_HIGH: - - Disk
15-Feb-2016 07:26:53.953	15-Feb-2016 07:26:53.000	192.168.220.110	local3	INFO	S-HOST10	logger: AFW.lab-128-17_1 Start of action: Testing event: DISK_UTILIZATI

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.

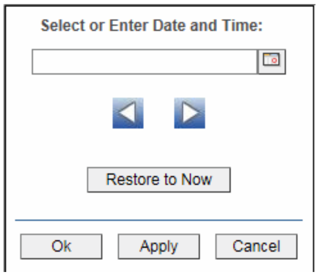
? Open the online help page for this display.

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

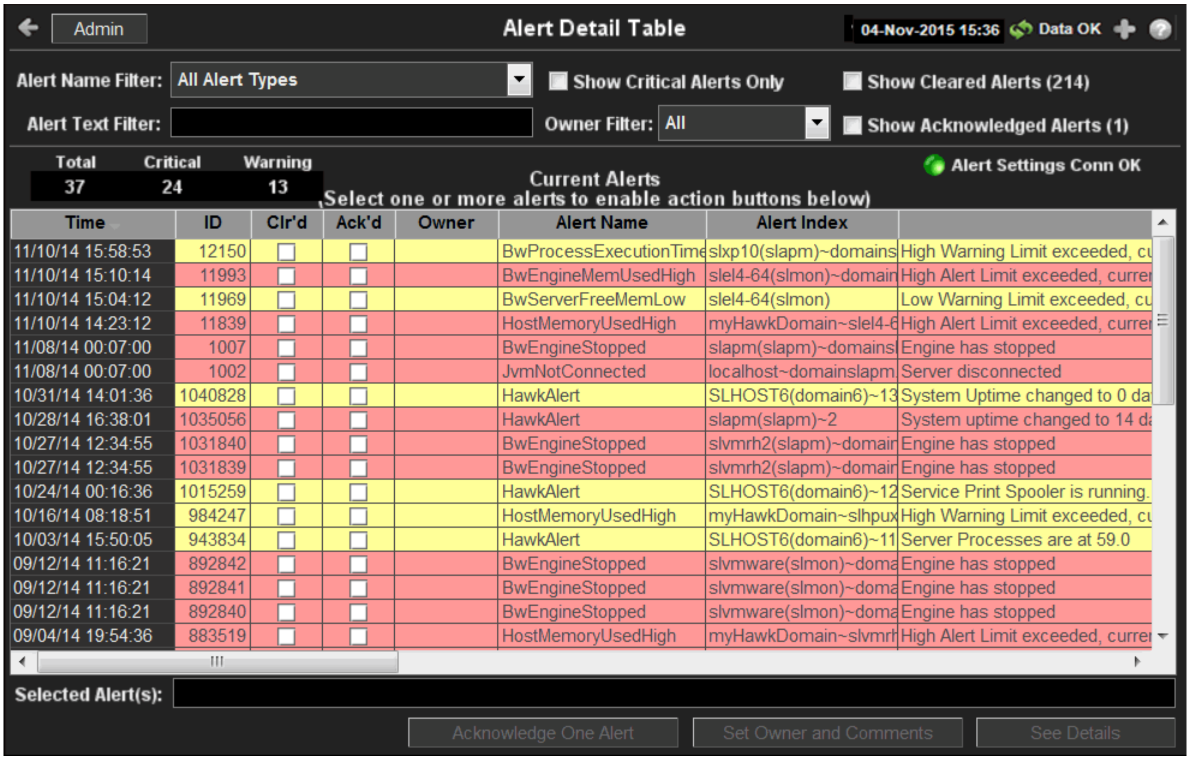
This display presents detailed information about all alerts that have occurred in your system. Displays in this View are:

- "Alert Detail Table" on page 108: Time ordered list of all alerts that have occurred in the system.

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 Sort ▲ to order column data.



Alert Name Filter: All Alert Types

□ Show Critical Alerts Only

□ Show Cleared Alerts (214)

Alert Text Filter:

Owner Filter: All

□ Show Acknowledged Alerts (1)

Total	Critical	Warning
37	24	13

● Alert Settings Conn OK

Current Alerts
(Select one or more alerts to enable action buttons below)

Time	ID	Clr'd	Ack'd	Owner	Alert Name	Alert Index	
11/10/14 15:58:53	12150	□	□		BwProcessExecutionTime	slxp10(slapm)~domains	High Warning Limit exceeded, cu
11/10/14 15:10:14	11993	□	□		BwEngineMemUsedHigh	slel4-64(slmon)~domain	High Alert Limit exceeded, currer
11/10/14 15:04:12	11969	□	□		BwServerFreeMemLow	slel4-64(slmon)	Low Warning Limit exceeded, cu
11/10/14 14:23:12	11839	□	□		HostMemoryUsedHigh	myHawkDomain~slel4-6	High Alert Limit exceeded, currer
11/08/14 00:07:00	1007	□	□		BwEngineStopped	slapm(slapm)~domains	Engine has stopped
11/08/14 00:07:00	1002	□	□		JvmNotConnected	localhost~domainslapm	Server disconnected
10/31/14 14:01:36	1040828	□	□		HawkAlert	SLHOST6(domain6)~13	System Uptime changed to 0 da
10/28/14 16:38:01	1035056	□	□		HawkAlert	slapm(slapm)~2	System uptime changed to 14 da
10/27/14 12:34:55	1031840	□	□		BwEngineStopped	slvmrh2(slapm)~domair	Engine has stopped
10/27/14 12:34:55	1031839	□	□		BwEngineStopped	slvmrh2(slapm)~domair	Engine has stopped
10/24/14 00:16:36	1015259	□	□		HawkAlert	SLHOST6(domain6)~12	Service Print Spooler is running.
10/16/14 08:18:51	984247	□	□		HostMemoryUsedHigh	myHawkDomain~slhpux	High Warning Limit exceeded, cu
10/03/14 15:50:05	943834	□	□		HawkAlert	SLHOST6(domain6)~11	Server Processes are at 59.0
09/12/14 11:16:21	892842	□	□		BwEngineStopped	slvmware(slmon)~doma	Engine has stopped
09/12/14 11:16:21	892841	□	□		BwEngineStopped	slvmware(slmon)~doma	Engine has stopped
09/12/14 11:16:21	892840	□	□		BwEngineStopped	slvmware(slmon)~doma	Engine has stopped
09/04/14 19:54:36	883519	□	□		HostMemoryUsedHigh	myHawkDomain~slvmrh	High Alert Limit exceeded, currer

Selected Alert(s):

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.

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.

Fields and Data
This display includes:

Alert Name Filter Select from a list of alert types or select All Alert Types. Filters limit display content and drop down menu selections to only those items that pass through the selected filter's criteria. Therefore if no items match the filter, you may see nothing in a given display and may not have any options available in the drop-down menu(s).

NOTE: Filter selection is disabled on drill down summary displays.

Show Critical Alerts Only If selected, only currently critical alerts are shown in the table. Otherwise, all active alerts are shown in the table.

Show Cleared Alerts If selected, cleared alerts are shown in the table.

Alert Text Filter Enter all or part of the Alert Text to view specific alerts. For example, High selects and displays all alerts that include High in the Alert Text. **NOTE:** Wild card characters are supported.

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.

Show Acknowledged Alerts If selected, acknowledged alerts are shown in the table.

Total Total number of alerts.

Critical Number of critical alerts.

Warning Total number of alerts that are currently in a warning state.

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

Alerts Table
This table lists all active alerts for the current filters.

Time The time (Java format) that the alert was activated.

ID A unique string identifier assigned to each activated alert.

Clr'd When checked, this typically indicates that the alert has been resolved. An alert is automatically cleared when the value being monitored no longer in the alert threshold.

Ack'd When checked, this typically indicates that the alert is being addressed.

Owner The named owner assigned by the administrator.

Alert Name The name of the alert. For a list of all alerts, see Alert Administration.

Alert Index The IP address and port number for the source (application, server, and so forth) associated with the alert.

Alert Text Descriptive text about the alert.

Severity The severity of the alert:

0 = Normal

1 = Warning / Yellow

2 = Alarm / Red
The color for the alert severity is shown by the row in the alert table.

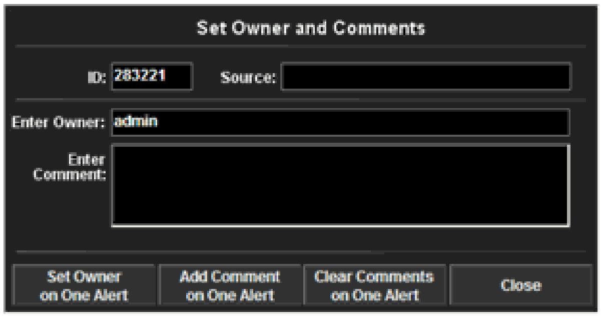
Source Name of RTView Data Server sending this data (or localhost).

Selected Alerts Lists the alerts selected in the table.

Acknowledge One Alert Select one alert from the Current Alerts table and click to acknowledge.

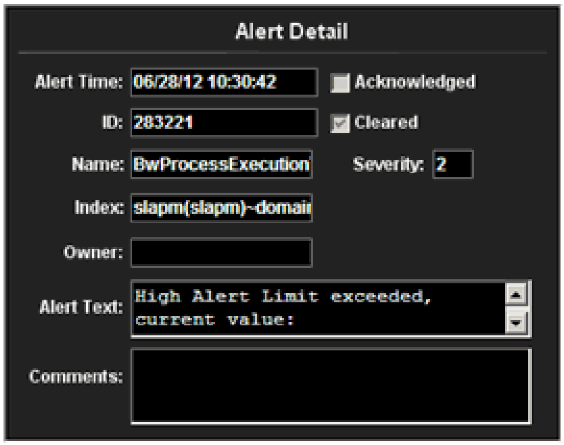
Acknowledge Multiple Alerts Select one or more alerts from the Current Alerts table and click to acknowledge.

Set Owner and Comments Select one or more alerts from the Current Alerts table and click to open the Set Owner and Comments dialog.



ID: 283221
Source:
Enter Owner: admin
Enter Comment:

See Details Select an alert from the Current Alerts table and click to open the Set Owner and Comments dialog.



Alert Time: 06/28/12 10:30:42
☐ Acknowledged
ID: 283221
☑ Cleared
Name: BwProcessExecution
Severity: 2
Index: slapm(slapm)~domair
Owner:
Alert Text: High Alert Limit exceeded, current value:
Comments:

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 111: Displays active alerts and provides interface to modify and manage alerts.
- "Alert Administration Audit" on page 117: 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 119: Display information about RTView Agent data servers.
- "RTView Agent Admin" on page 121: Display information about RTView Agent data servers.

Alert Administration

This section includes:

- "Tabular Alert Administration" on page 114
- "Setting Override Alerts" on page 116

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.

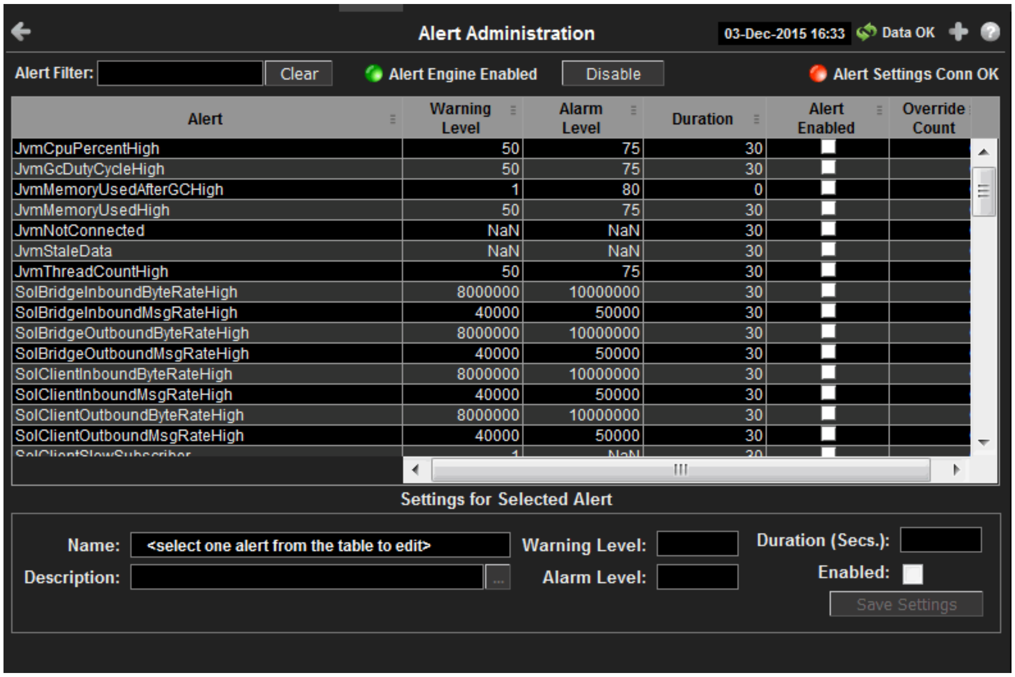
The manner in which global alerts are applied depends on the Solution Package. For example, the EMS Monitor Solution Package has queue alerts, topic alerts and server alerts. When a queue alert is applied globally, it is applied to all queues on all servers. Likewise, a server alert applies to all servers, 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**.



Alert Administration

03-Dec-2015 16:33 Data OK

Alert Filter: Clear ● Alert Engine Enabled Disable ● Alert Settings Conn OK

Alert	Warning Level	Alarm Level	Duration	Alert Enabled	Override Count
JvmCpuPercentHigh	50	75	30	□	
JvmGcDutyCycleHigh	50	75	30	□	
JvmMemoryUsedAfterGCHigh	1	80	0	□	
JvmMemoryUsedHigh	50	75	30	□	
JvmNotConnected	NaN	NaN	30	□	
JvmStaleData	NaN	NaN	30	□	
JvmThreadCountHigh	50	75	30	□	
SolBridgeInboundByteRateHigh	8000000	10000000	30	□	
SolBridgeInboundMsgRateHigh	40000	50000	30	□	
SolBridgeOutboundByteRateHigh	8000000	10000000	30	□	
SolBridgeOutboundMsgRateHigh	40000	50000	30	□	
SolClientInboundByteRateHigh	8000000	10000000	30	□	
SolClientInboundMsgRateHigh	40000	50000	30	□	
SolClientOutboundByteRateHigh	8000000	10000000	30	□	
SolClientOutboundMsgRateHigh	40000	50000	30	□	
SolClientSlowSubscriber	1	NaN	30	□	

Settings for Selected Alert

Name: <select one alert from the table to edit>

Description:

Warning Level:

Alarm Level:

Duration (Secs.):

Enabled: □

Save Settings

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.

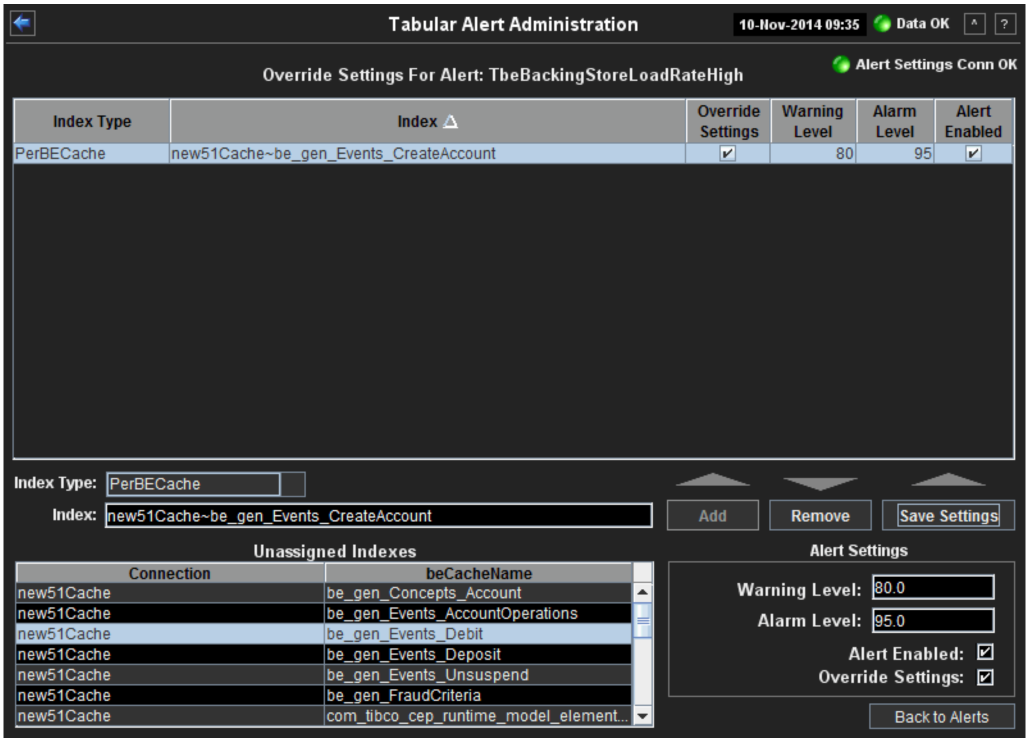
Save Settings Click to apply alert settings.

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**.



Tabular Alert Administration 10-Nov-2014 09:35 Data OK

Override Settings For Alert: TbeBackingStoreLoadRateHigh

Alert Settings Conn OK

Index Type	Index △	Override Settings	Warning Level	Alarm Level	Alert Enabled
PerBECache	new51Cache~be_gen_Events_CreateAccount	☑	80	95	☑

Index Type: PerBECache

Index: new51Cache~be_gen_Events_CreateAccount

Unassigned Indexes

Connection	beCacheName
new51Cache	be_gen_Concepts_Account
new51Cache	be_gen_Events_AccountOperations
new51Cache	be_gen_Events_Debit
new51Cache	be_gen_Events_Deposit
new51Cache	be_gen_Events_Unsuspend
new51Cache	be_gen_FraudCriteria
new51Cache	com_tibco_cep_runtime_model_element...

Alert Settings

Warning Level: 80.0

Alarm Level: 95.0

Alert Enabled: ☑

Override Settings: ☑

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.

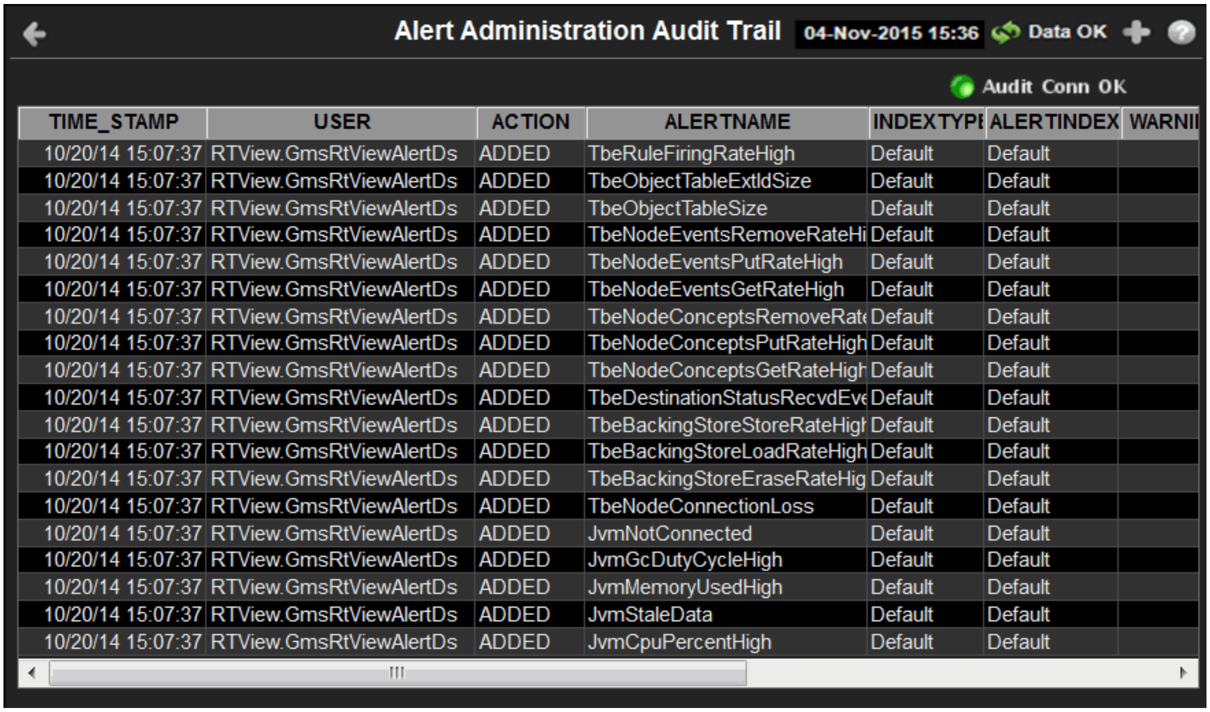
   Levels Enabled Deselect this option.

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, sort the **ALERTNAME** column using the button.



TIME_STAMP	USER	ACTION	ALERTNAME	INDEXTYPI	ALERTINDEX	WARNII
10/20/14 15:07:37	RTView.GmsRtViewAlertDs	ADDED	TbeRuleFiringRateHigh	Default	Default	
10/20/14 15:07:37	RTView.GmsRtViewAlertDs	ADDED	TbeObjectTableExtIdSize	Default	Default	
10/20/14 15:07:37	RTView.GmsRtViewAlertDs	ADDED	TbeObjectTableSize	Default	Default	
10/20/14 15:07:37	RTView.GmsRtViewAlertDs	ADDED	TbeNodeEventsRemoveRateHi	Default	Default	
10/20/14 15:07:37	RTView.GmsRtViewAlertDs	ADDED	TbeNodeEventsPutRateHigh	Default	Default	
10/20/14 15:07:37	RTView.GmsRtViewAlertDs	ADDED	TbeNodeEventsGetRateHigh	Default	Default	
10/20/14 15:07:37	RTView.GmsRtViewAlertDs	ADDED	TbeNodeConceptsRemoveRat	Default	Default	
10/20/14 15:07:37	RTView.GmsRtViewAlertDs	ADDED	TbeNodeConceptsPutRateHigh	Default	Default	
10/20/14 15:07:37	RTView.GmsRtViewAlertDs	ADDED	TbeNodeConceptsGetRateHigh	Default	Default	
10/20/14 15:07:37	RTView.GmsRtViewAlertDs	ADDED	TbeDestinationStatusRecvdEve	Default	Default	
10/20/14 15:07:37	RTView.GmsRtViewAlertDs	ADDED	TbeBackingStoreStoreRateHigh	Default	Default	
10/20/14 15:07:37	RTView.GmsRtViewAlertDs	ADDED	TbeBackingStoreLoadRateHigh	Default	Default	
10/20/14 15:07:37	RTView.GmsRtViewAlertDs	ADDED	TbeBackingStoreEraseRateHig	Default	Default	
10/20/14 15:07:37	RTView.GmsRtViewAlertDs	ADDED	TbeNodeConnectionLoss	Default	Default	
10/20/14 15:07:37	RTView.GmsRtViewAlertDs	ADDED	JvmNotConnected	Default	Default	
10/20/14 15:07:37	RTView.GmsRtViewAlertDs	ADDED	JvmGcDutyCycleHigh	Default	Default	
10/20/14 15:07:37	RTView.GmsRtViewAlertDs	ADDED	JvmMemoryUsedHigh	Default	Default	
10/20/14 15:07:37	RTView.GmsRtViewAlertDs	ADDED	JvmStaleData	Default	Default	
10/20/14 15:07:37	RTView.GmsRtViewAlertDs	ADDED	JvmCpuPercentHigh	Default	Default	

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.

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.

ALERTINDEX The IP address and port number for the source (application, server, and so forth) associated with the alert.

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 exceed the specified Warning Level or Alarm Level threshold before an alert is executed. 0 is for immediate execution.

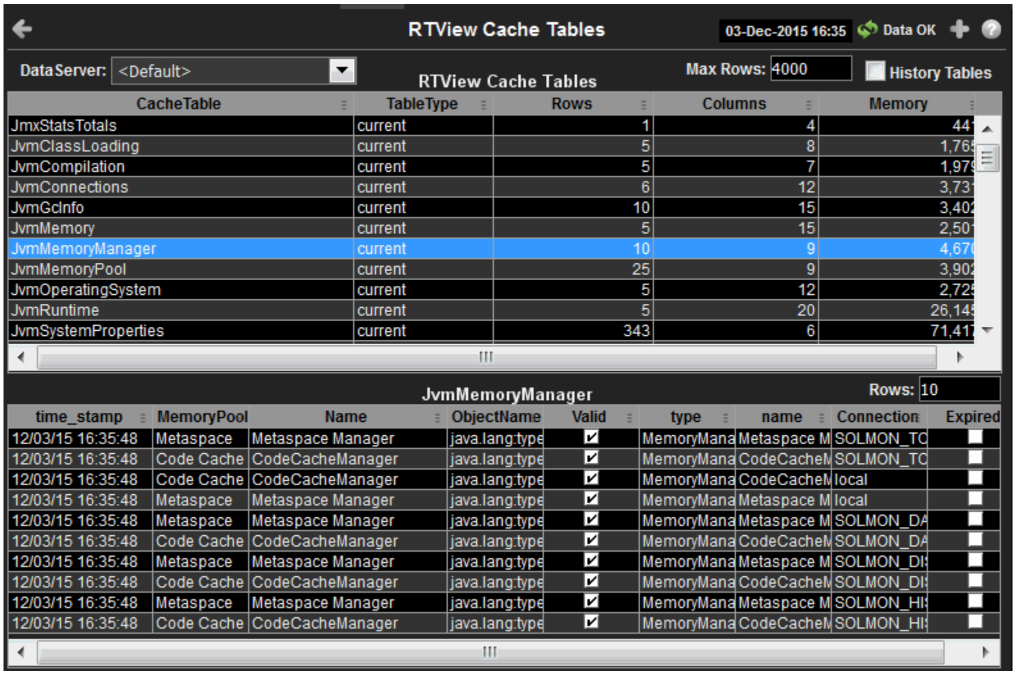
ENABLED When checked, indicates the alert was Enabled at the time this modification was made, as indicated in the **TIME_STAMP** column.

USEINDEX When checked, this action was performed on an override alert (the alert does not use the global settings).

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.



DataServer: <Default>

Max Rows: 4000

□ History Tables

RTView Cache Tables

CacheTable	TableType	Rows	Columns	Memory
JmxStatsTotals	current	1	4	44
JvmClassLoading	current	5	8	1,76
JvmCompilation	current	5	7	1,97
JvmConnections	current	6	12	3,73
JvmGcInfo	current	10	15	3,40
JvmMemory	current	5	15	2,50
JvmMemoryManager	current	10	9	4,67
JvmMemoryPool	current	25	9	3,90
JvmOperatingSystem	current	5	12	2,72
JvmRuntime	current	5	20	26,14
JvmSystemProperties	current	343	6	71,41

JvmMemoryManager

Rows: 10

time_stamp	MemoryPool	Name	ObjectName	Valid	type	name	Connection	Expired
12/03/15 16:35:48	Metaspace	Metaspace Manager	java.lang:type	☑	MemoryMana	Metaspace M	SOLMON_TC	□
12/03/15 16:35:48	Code Cache	CodeCacheManager	java.lang:type	☑	MemoryMana	CodeCacheM	SOLMON_TC	□
12/03/15 16:35:48	Code Cache	CodeCacheManager	java.lang:type	☑	MemoryMana	CodeCacheM	local	□
12/03/15 16:35:48	Metaspace	Metaspace Manager	java.lang:type	☑	MemoryMana	Metaspace M	local	□
12/03/15 16:35:48	Metaspace	Metaspace Manager	java.lang:type	☑	MemoryMana	Metaspace M	SOLMON_DA	□
12/03/15 16:35:48	Code Cache	CodeCacheManager	java.lang:type	☑	MemoryMana	CodeCacheM	SOLMON_DA	□
12/03/15 16:35:48	Metaspace	Metaspace Manager	java.lang:type	☑	MemoryMana	Metaspace M	SOLMON_DI	□
12/03/15 16:35:48	Code Cache	CodeCacheManager	java.lang:type	☑	MemoryMana	CodeCacheM	SOLMON_DI	□
12/03/15 16:35:48	Metaspace	Metaspace Manager	java.lang:type	☑	MemoryMana	Metaspace M	SOLMON_HI	□
12/03/15 16:35:48	Code Cache	CodeCacheManager	java.lang:type	☑	MemoryMana	CodeCacheM	SOLMON_HI	□

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.

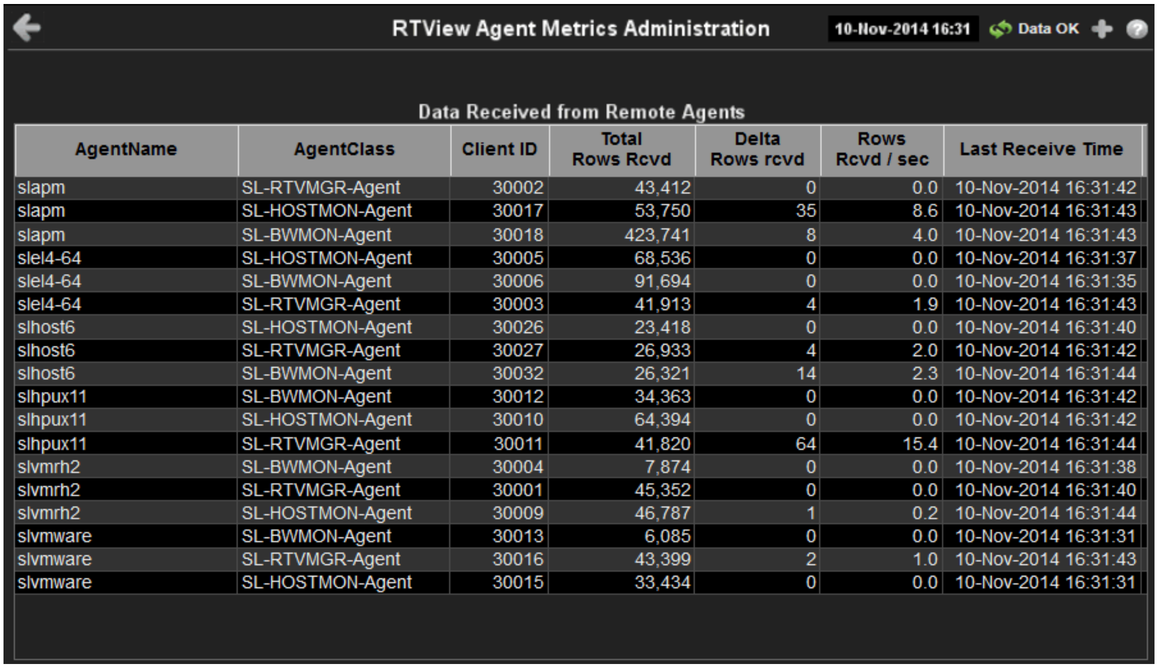
Rows Number of rows currently in the table.

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.



RTView Agent Metrics Administration 10-Nov-2014 16:31 Data OK

Data Received from Remote Agents

AgentName	AgentClass	Client ID	Total Rows Rcvd	Delta Rows rcvd	Rows Rcvd / sec	Last Receive Time
slapm	SL-RTVMGR-Agent	30002	43,412	0	0.0	10-Nov-2014 16:31:42
slapm	SL-HOSTMON-Agent	30017	53,750	35	8.6	10-Nov-2014 16:31:43
slapm	SL-BWMON-Agent	30018	423,741	8	4.0	10-Nov-2014 16:31:43
slel4-64	SL-HOSTMON-Agent	30005	68,536	0	0.0	10-Nov-2014 16:31:37
slel4-64	SL-BWMON-Agent	30006	91,694	0	0.0	10-Nov-2014 16:31:35
slel4-64	SL-RTVMGR-Agent	30003	41,913	4	1.9	10-Nov-2014 16:31:43
slhost6	SL-HOSTMON-Agent	30026	23,418	0	0.0	10-Nov-2014 16:31:40
slhost6	SL-RTVMGR-Agent	30027	26,933	4	2.0	10-Nov-2014 16:31:42
slhost6	SL-BWMON-Agent	30032	26,321	14	2.3	10-Nov-2014 16:31:44
slhpux11	SL-BWMON-Agent	30012	34,363	0	0.0	10-Nov-2014 16:31:42
slhpux11	SL-HOSTMON-Agent	30010	64,394	0	0.0	10-Nov-2014 16:31:42
slhpux11	SL-RTVMGR-Agent	30011	41,820	64	15.4	10-Nov-2014 16:31:44
slvmrh2	SL-BWMON-Agent	30004	7,874	0	0.0	10-Nov-2014 16:31:38
slvmrh2	SL-RTVMGR-Agent	30001	45,352	0	0.0	10-Nov-2014 16:31:40
slvmrh2	SL-HOSTMON-Agent	30009	46,787	1	0.2	10-Nov-2014 16:31:44
slvmware	SL-BWMON-Agent	30013	6,085	0	0.0	10-Nov-2014 16:31:31
slvmware	SL-RTVMGR-Agent	30016	43,399	2	1.0	10-Nov-2014 16:31:43
slvmware	SL-HOSTMON-Agent	30015	33,434	0	0.0	10-Nov-2014 16:31:31

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.

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

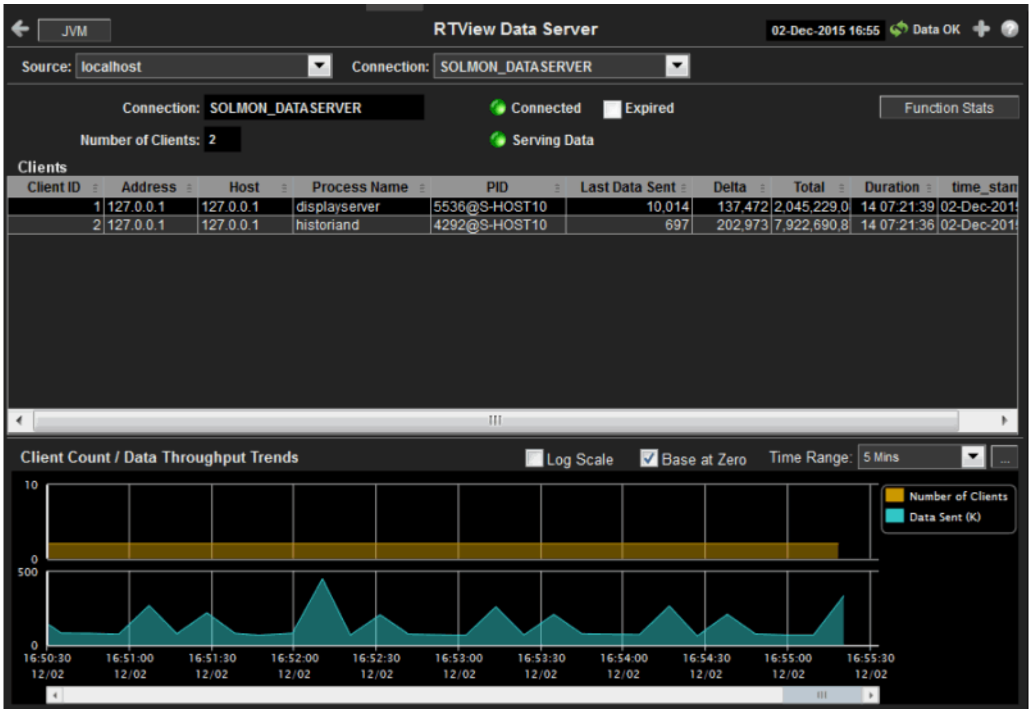
These displays enable you to monitor performance of all RTView Servers.

- “Data Server Metrics” on page 122: Shows metrics for RTView Data Servers.
- “Display Server Metrics” on page 125: Shows metrics for RTView Display Servers.
- “Historian Servers” on page 126: Shows metrics for RTView Historian Servers.
- “Tomcat Server Summary” on page 128: Shows metrics for Tomcat application sessions, including Tomcat hosting and connection details.
- “Tomcat Modules Summary” on page 131: Shows metrics for Tomcat application modules and utilization details.
- “JVM CPU/Mem Summary” on page 134: 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 138: Shows Java Virtual Machine heap and non-heap memory usage for a single connection.
- “JVM Mem GC Trends” on page 141: Shows Java Virtual Machine garbage collection memory usage for a single connection.
- “JVM System Properties” on page 143: Shows Java Virtual Machine input arguments and system properties for a single connection.
- “Version Info” on page 144: Shows the version information of each jar used in each connected RTView application.
- “About” on page 146: 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.



Source: localhost

Connection: SOLMON_DATASERVER

Connection: SOLMON_DATASERVER

● Connected ☐ Expired

Number of Clients: 2

● Serving Data

Clients

Client ID	Address	Host	Process Name	PID	Last Data Sent	Delta	Total	Duration	time_stan
1	127.0.0.1	127.0.0.1	displayserver	5536@S-HOST10	10,014	137,472	2,045,229,0	14 07:21:39	02-Dec-201
2	127.0.0.1	127.0.0.1	historiand	4292@S-HOST10	697	202,973	7,922,690,8	14 07:21:36	02-Dec-201

Client Count / Data Throughput Trends

☐ Log Scale ☑ Base at Zero Time Range: 5 Mins

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.

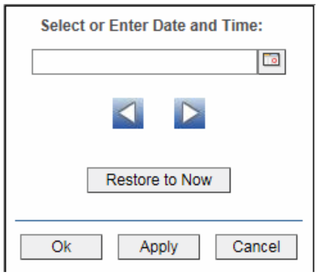
TIME_STAMP The date and time this row of data was last updated.

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.

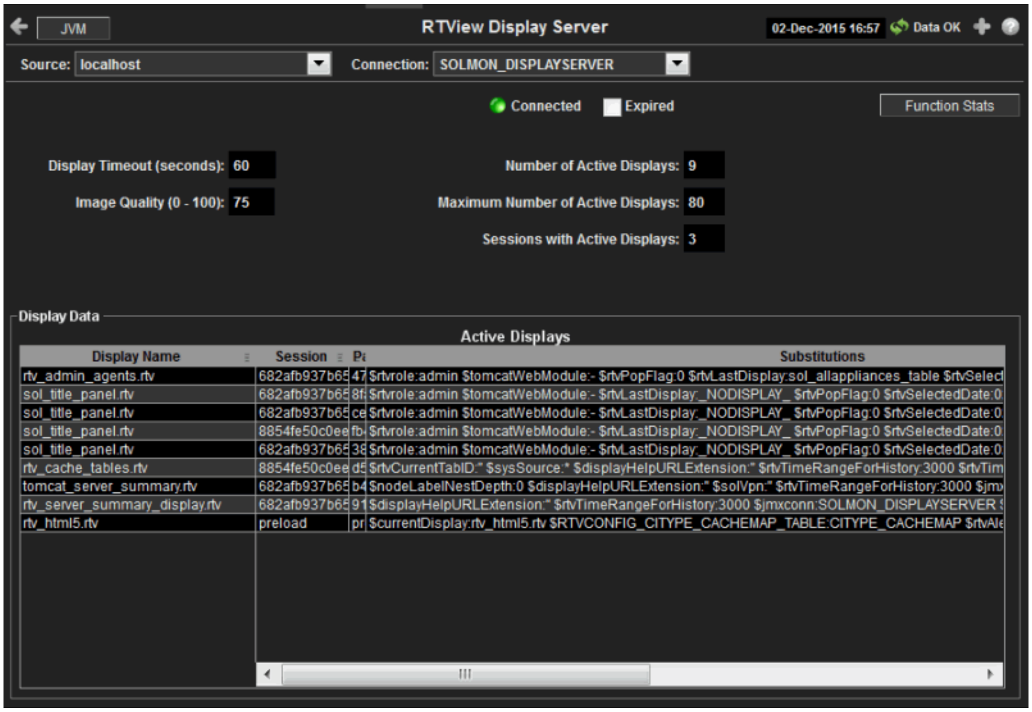
Number of Clients Traces the number of clients being served by the Data Server.

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.



JVM RTView Display Server 02-Dec-2015 16:57 Data OK

Source: localhost Connection: SOLMON_DISPLAYSERVER

● Connected □ Expired Function Stats

Display Timeout (seconds): 60

Image Quality (0 - 100): 75

Number of Active Displays: 9

Maximum Number of Active Displays: 80

Sessions with Active Displays: 3

Display Data

Active Displays

Display Name	Session	Pa	Substitutions
rtv_admin_agents.rtv	682afb937b65	47	$rtvrole:admin $tomcatWebModule:- $rtvPopFlag:0 $rtvLastDisplay:sol_allappliances_table $rtvSelect
sol_title_panel.rtv	682afb937b65	8f	$rtvrole:admin $tomcatWebModule:- $rtvLastDisplay:_NODISPLAY_ $rtvPopFlag:0 $rtvSelectedDate:0
sol_title_panel.rtv	682afb937b65	ce	$rtvrole:admin $tomcatWebModule:- $rtvLastDisplay:_NODISPLAY_ $rtvPopFlag:0 $rtvSelectedDate:0
sol_title_panel.rtv	8854fe50c0ee	fb	$rtvrole:admin $tomcatWebModule:- $rtvLastDisplay:_NODISPLAY_ $rtvPopFlag:0 $rtvSelectedDate:0
sol_title_panel.rtv	682afb937b65	38	$rtvrole:admin $tomcatWebModule:- $rtvLastDisplay:_NODISPLAY_ $rtvPopFlag:0 $rtvSelectedDate:0
rtv_cache_tables.rtv	8854fe50c0ee	d5	$rtvCurrentTabID:" $sysSource:* $displayHelpURLExtension:" $rtvTimeRangeForHistory:3000 $rtvTim
tomcat_server_summary.rtv	682afb937b65	b4	$nodeLabelNestDepth:0 $displayHelpURLExtension:" $solVpn:" $rtvTimeRangeForHistory:3000 $jmx
rtv_server_summary_display.rtv	682afb937b65	91	$displayHelpURLExtension:" $rtvTimeRangeForHistory:3000 $jmxconn:SOLMON_DISPLAYSERVER $
rtv_html5.rtv	preload	pr	$currentDisplay:rtv_html5.rtv $RTVCONFIG_CITYPE_CACHEMAP_TABLE:CITYPE_CACHEMAP $rtvAle

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.

CIs: 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.

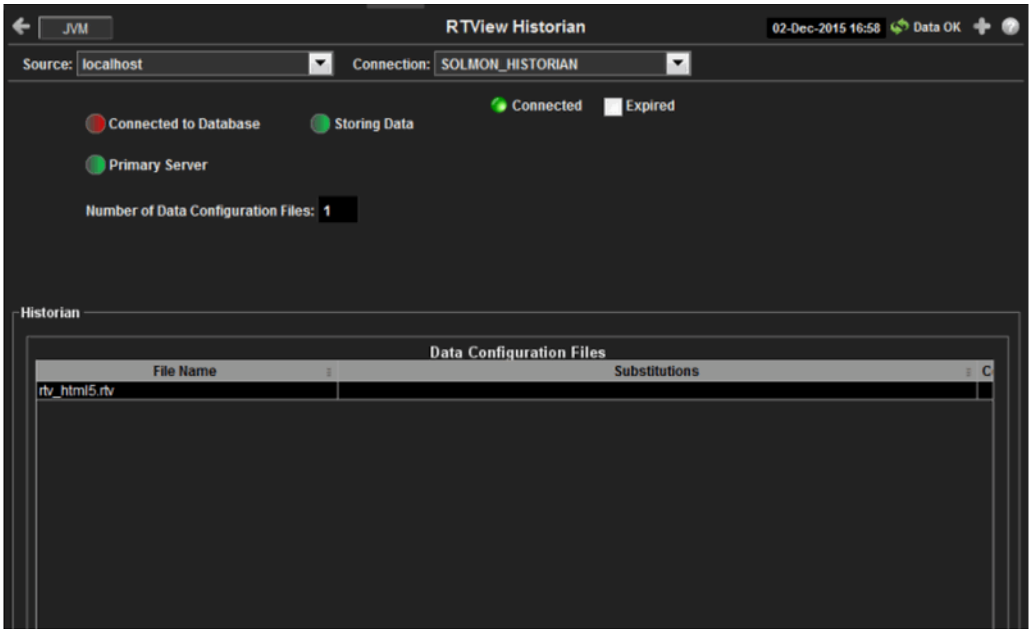
ID The client ID.

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.



← JVM RTView Historian 02-Dec-2015 16:58 Data OK ✚ ?

Source: localhost ▾ Connection: SOLMON_HISTORIAN ▾

🔴 Connected to Database 🟢 Storing Data 🟢 Connected □ Expired

🟢 Primary Server

Number of Data Configuration Files: 1

Historian

Data Configuration Files

File Name	Substitutions	C
rtv_html5.rtv		

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.

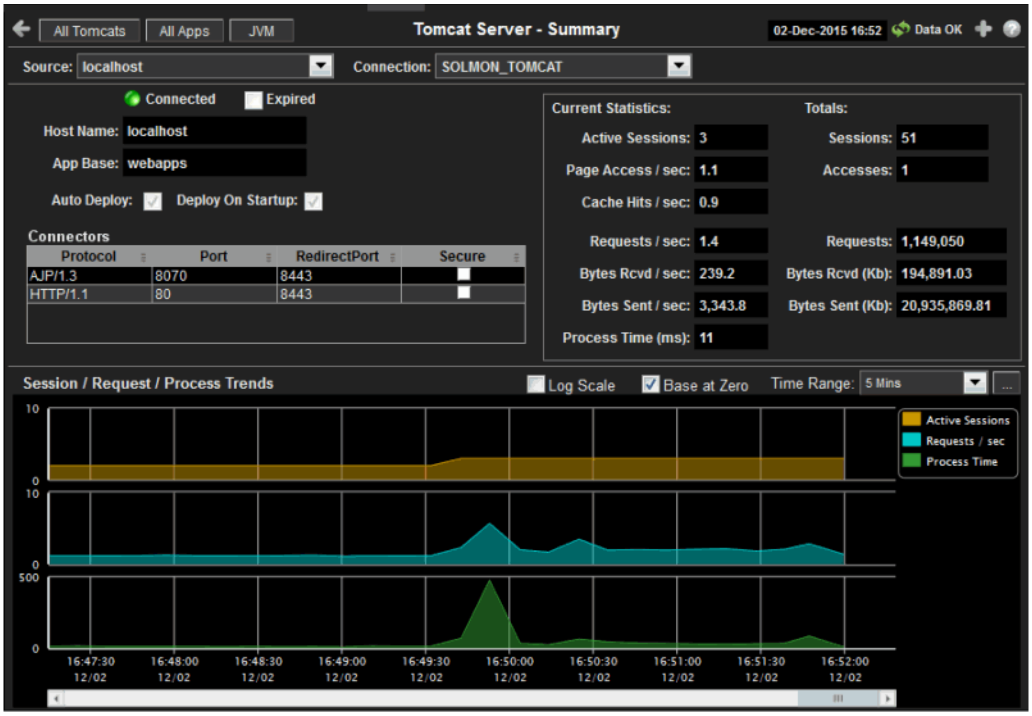
Historian / Data Configuration Files

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.



Source: localhost

Connection: SOLMON_TOMCAT

● Connected □ Expired

Host Name: localhost

App Base: webapps

Auto Deploy: ☑ Deploy On Startup: ☑

Connectors

Protocol	Port	RedirectPort	Secure
AJP/1.3	8070	8443	□
HTTP/1.1	80	8443	□

Current Statistics:

Active Sessions: 3

Page Access / sec: 1.1

Cache Hits / sec: 0.9

Requests / sec: 1.4

Bytes Rcvd / sec: 239.2

Bytes Sent / sec: 3,343.8

Process Time (ms): 11

Totals:

Sessions: 51

Accesses: 1

Requests: 1,149,050

Bytes Rcvd (Kb): 194,891.03

Bytes Sent (Kb): 20,935,869.81

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.

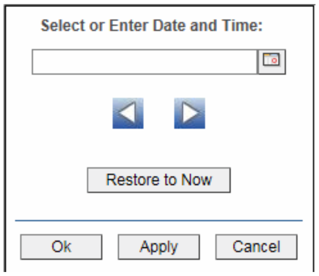
Process Time The amount of time, in milliseconds, for the servlet to process client requests.

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.

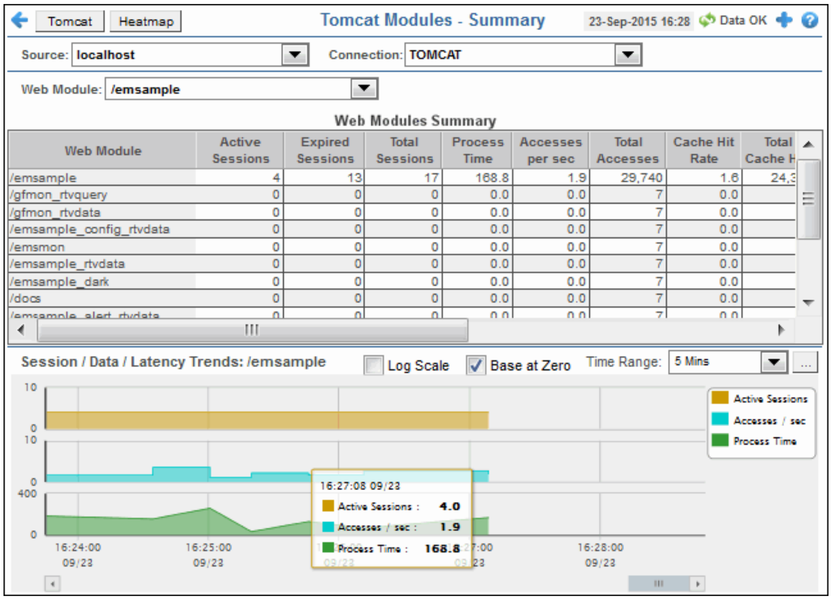
Process Time Traces the average amount of time, in milliseconds, to process requests.

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.



Tomcat | Heatmap | **Tomcat Modules - Summary** | 23-Sep-2015 16:28 | Data OK

Source: localhost   Connection: TOMCAT

Web Module: /emsample

Web Modules Summary

Web Module	Active Sessions	Expired Sessions	Total Sessions	Process Time	Accesses per sec	Total Accesses	Cache Hit Rate	Total Cache H
/emsample	4	13	17	168.8	1.9	29,740	1.6	24,3
/gfmon_rtvquery	0	0	0	0.0	0.0	7	0.0	
/gfmon_rtvdata	0	0	0	0.0	0.0	7	0.0	
/emsample_config_rtvdata	0	0	0	0.0	0.0	7	0.0	
/emsmon	0	0	0	0.0	0.0	7	0.0	
/emsample_rtvdata	0	0	0	0.0	0.0	7	0.0	
/emsample_dark	0	0	0	0.0	0.0	7	0.0	
/docs	0	0	0	0.0	0.0	7	0.0	
/emsample_alert_rtvdata	0	0	0	0.0	0.0	7	0.0	

Session / Data / Latency Trends: /emsample   ☐ Log Scale   ☑ Base at Zero   Time Range: 5 Mins

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

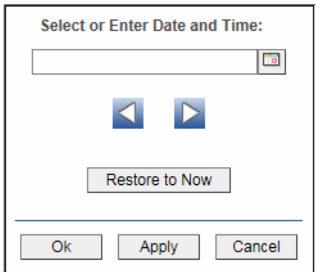
<month>/ <day>/<year> <hours>:<minutes>:<seconds>

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.

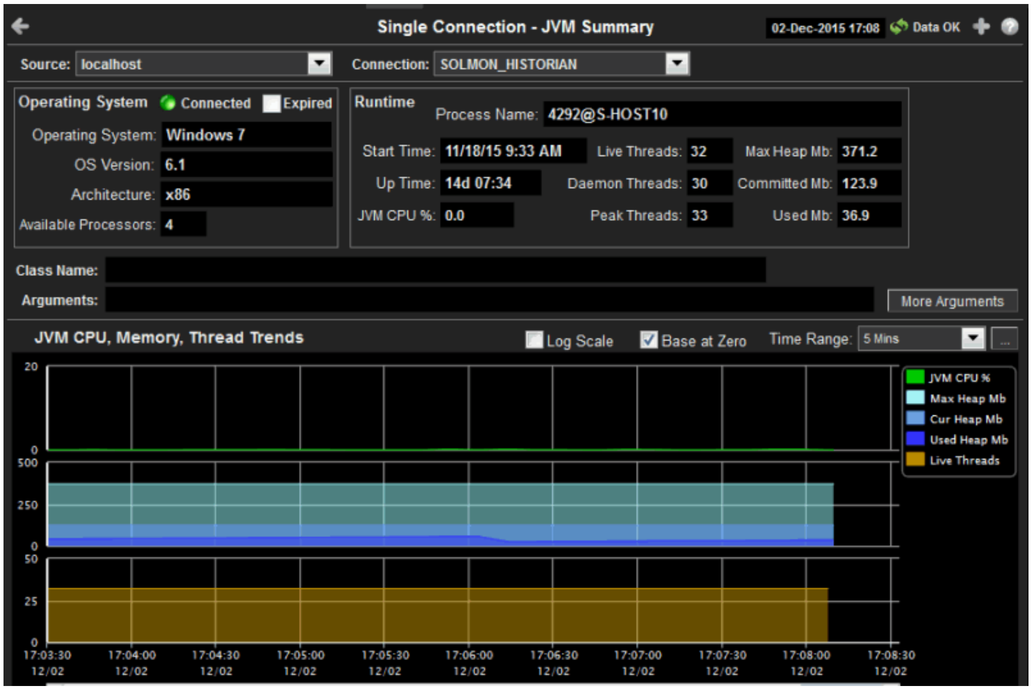
Accesses / sec Traces the number of times pages are accessed, per second.

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.



Single Connection - JVM Summary 02-Dec-2015 17:08 Data OK

Source: localhost Connection: SOLMON_HISTORIAN

Operating System ● Connected □ Expired

Operating System: Windows 7

OS Version: 6.1

Architecture: x86

Available Processors: 4

Runtime

Process Name: 4292@S-HOST10

Start Time: 11/18/15 9:33 AM Live Threads: 32 Max Heap Mb: 371.2

Up Time: 14d 07:34 Daemon Threads: 30 Committed Mb: 123.9

JVM CPU %: 0.0 Peak Threads: 33 Used Mb: 36.9

Class Name:

Arguments:

More Arguments

JVM CPU, Memory, Thread Trends □ Log Scale ☑ Base at Zero Time Range: 5 Mins

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.

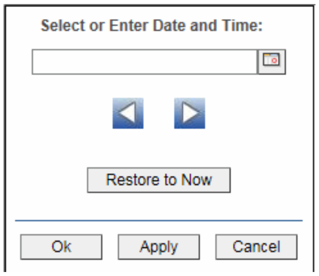
More Arguments Additional arguments used to start the application.

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).

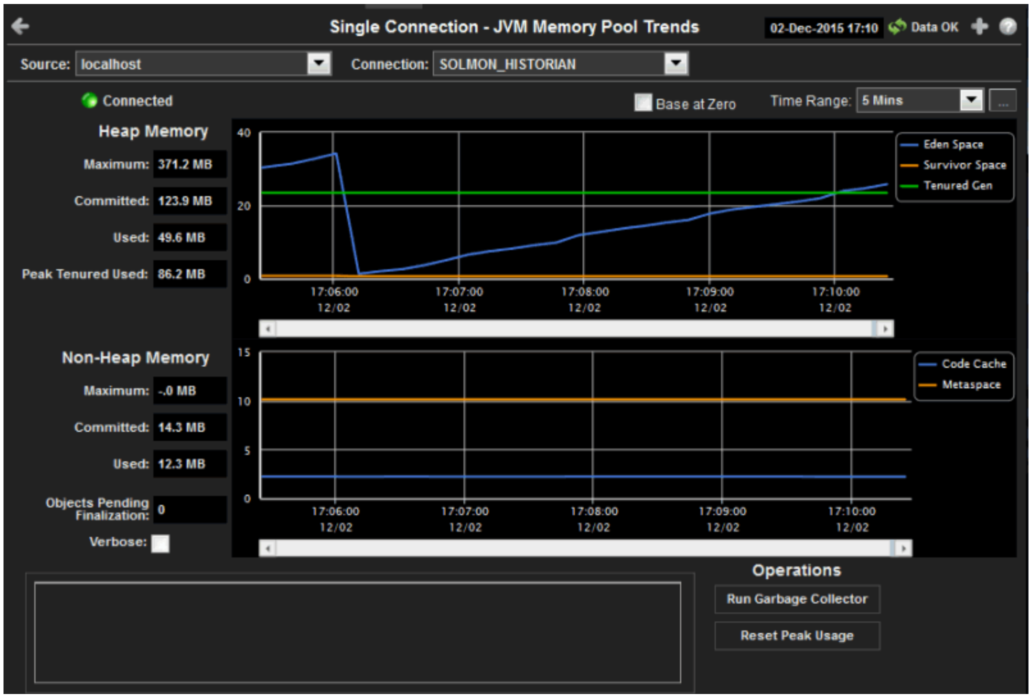
Cur Heap Mb Traces the current amount of memory, in megabytes, used for memory management by the application in the time range specified.

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.



Single Connection - JVM Memory Pool Trends 02-Dec-2015 17:10 Data OK

Source: localhost Connection: SOLMON_HISTORIAN

Connected □ Base at Zero Time Range: 5 Mins

Heap Memory

Maximum: 371.2 MB

Committed: 123.9 MB

Used: 49.6 MB

Peak Tenured Used: 86.2 MB

Non-Heap Memory

Maximum: -.0 MB

Committed: 14.3 MB

Used: 12.3 MB

Objects Pending Finalization: 0

Verbose: □

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:

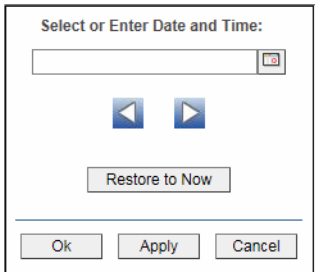
Source Select the type of connection to the RTView Server.

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.

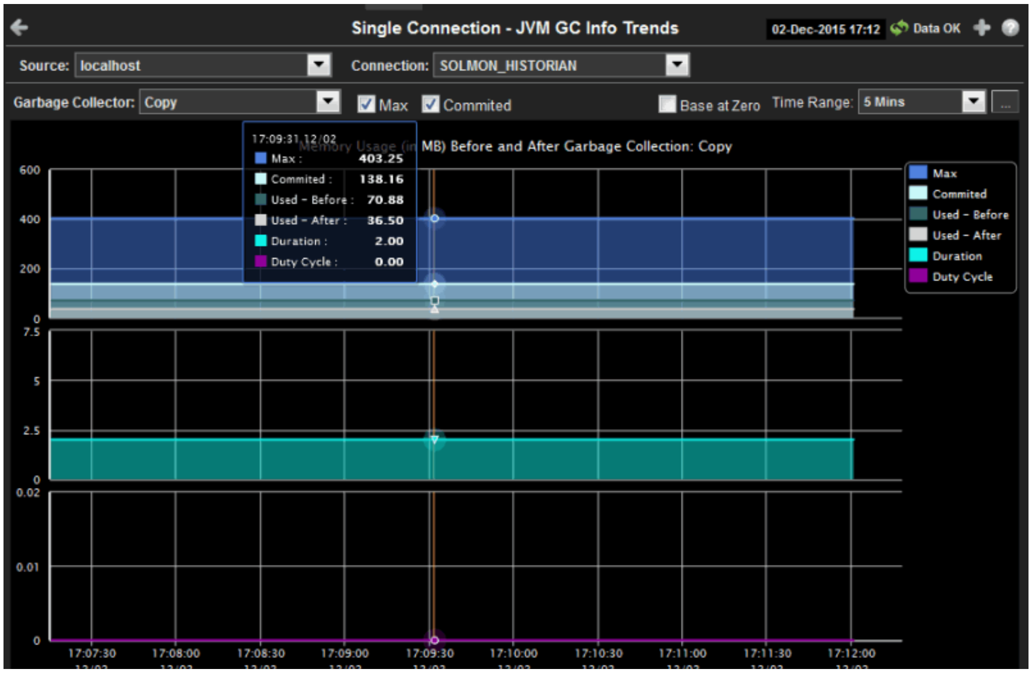
Operations

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.



Single Connection - JVM GC Info Trends 02-Dec-2015 17:12 Data OK

Source: localhost Connection: SOLMON_HISTORIAN

Garbage Collector: Copy ☑ Max ☑ Commited □ Base at Zero Time Range: 5 Mins

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.

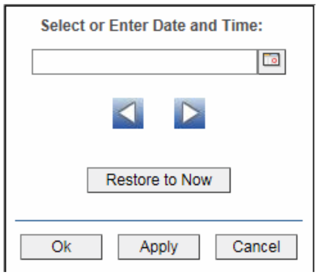
Garbage Collector Select a garbage collection method: **Copy** or **MarkSweepCompact**.

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.

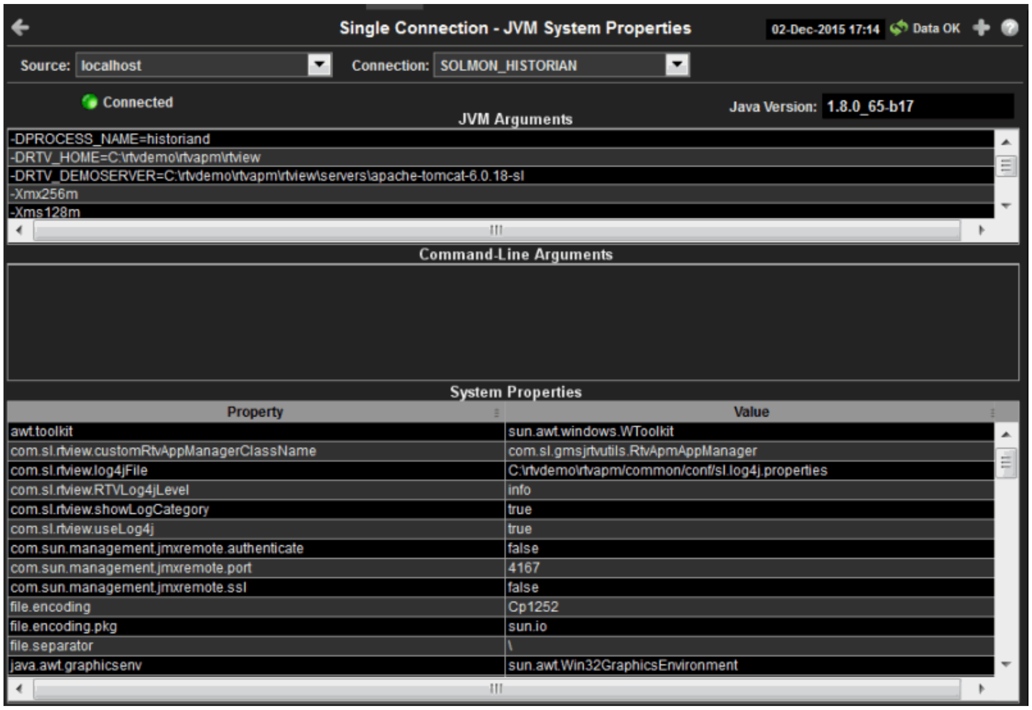
Used - After Traces the amount of memory used after the last garbage collection.

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.



Single Connection - JVM System Properties

02-Dec-2015 17:14 Data OK

Source: localhost

Connection: SOLMON_HISTORIAN

Connected

Java Version: 1.8.0_65-b17

JVM Arguments

```
-DPROCESS_NAME=historiand
-DRTV_HOME=C:\rtvdemo\rtvapm\rtview
-DRTV_DEMOSERVER=C:\rtvdemo\rtvapm\rtview\servers\apache-tomcat-6.0.18-sl
-Xmx256m
-Xms128m
```

Command-Line Arguments

System Properties

Property	Value
awt.toolkit	sun.awt.windows.WToolkit
com.sl.rtview.customRtvAppManagerClassName	com.sl.gmsjrtvutils.RtvApmAppManager
com.sl.rtview.log4jFile	C:\rtvdemo\rtvapm/common/conf/sl.log4j.properties
com.sl.rtview.RTVLog4jLevel	info
com.sl.rtview.showLogCategory	true
com.sl.rtview.useLog4j	true
com.sun.management.jmxremote.authenticate	false
com.sun.management.jmxremote.port	4167
com.sun.management.jmxremote.ssl	false
file.encoding	Cp1252
file.encoding.pkg	sun.io
file.separator	\
java.awt.graphicsenv	sun.awt.Win32GraphicsEnvironment

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.

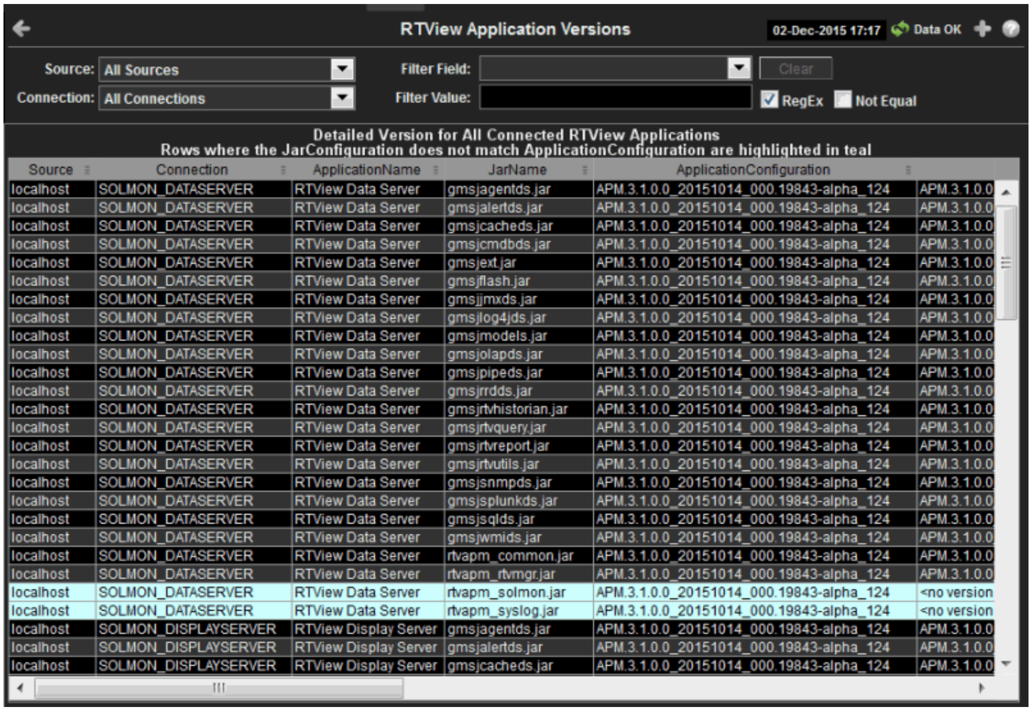
Property Name of the property.

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 information not supported in this version" in the **ApplicationConfiguration** column.



RTView Application Versions

02-Dec-2015 17:17 Data OK

Source: All Sources

Connection: All Connections

Filter Field:

Filter Value:

☑ RegEx ☐ Not Equal

Detailed Version for All Connected RTView Applications
Rows where the JarConfiguration does not match ApplicationConfiguration are highlighted in teal

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.

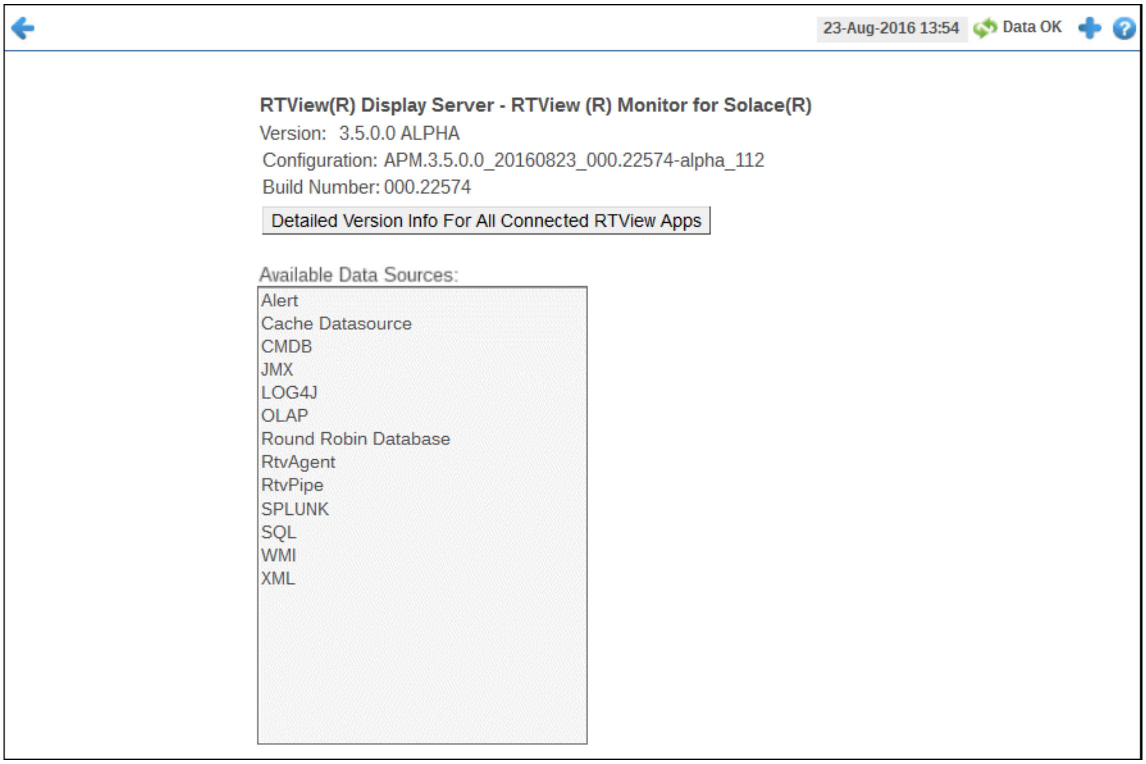
Expired When checked, this connection is expired due to inactivity.

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.



RTView(R) Display Server - RTView (R) Monitor for Solace(R)

Version: 3.5.0.0 ALPHA

Configuration: APM.3.5.0.0_20160823_000.22574-alpha_112

Build Number: 000.22574

Available Data Sources:

Alert
Cache Datasource
CMDB
JMX
LOG4J
OLAP
Round Robin Database
RtvAgent
RtvPipe
SPLUNK
SQL
WMI
XML

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
SolCspfNeighborDown 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 Third Party Notice Requirements

** Apache Tomcat is delivered for convenience only as a separate application and is licensed under the Apache License Version 2.0

** Apache HttpClient is embedded in the RTView Core libraries and is licensed under the Apache License Version 2.0

** JEval 0.9.4 is licensed under the Apache License Version 2.0

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean anyform resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in orattached to the work (an example is provided in the Appendix below)

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations,elaborations, or other modifications represent, as a whole, an original workof authorship. For the purposes of this License, Derivative Works shallnot include works that remain separable from, or merely link (or bindby name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean anywork of authorship, including the original version of the Work and anymodifications or additions to that Work or Derivative Worksthereof, that is intentionally submitted to Licensor for inclusion inthe Work by the copyright owner or by an individual or Legal Entityauthorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives,including but not limited to communication on electronic mailinglists, source code control systems, and issue tracking systems that aremanaged by, or on behalf of, the Licensor for the purpose of discussingand improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyrightowner as "Not a Contribution."

"Contributor" shall meanLicensor and any individual or Legal Entity on behalf of whom a Contribution hasbeen received by Licensor and subsequently incorporated within theWork.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor herebygrants to You a perpetual, worldwide, non-exclusive, no-charge,royalty-free, irrevocable copyright license to reproduce, prepareDerivative Works of, publicly display, publicly perform,sublicense, and distribute the Work and such Derivative Works in Sourceor Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor herebygrants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combinationof their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement,then any patent licenses granted to You under this License forthat Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce anddistribute copies of the Work or Derivative Works thereof in anymedium, with or without modifications, and in Source or Objectform, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof,You may choose to offer, and charge a fee for, acceptance ofsupport, warranty, indemnity, or other liability obligations and/orrights consistent with this License. However, in accepting suchobligations, You may act only on Your own behalf and on Your soleresponsibility, not on behalf of any other Contributor, and only ifYou agree to indemnify, defend, and hold each Contributorharmless for any liability incurred by, or claims asserted against,such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at:

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License isdistributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANYKIND, either express or implied. See the License for the specific languagegoverning permissions and limitations under the License.

===

** TreeMap Algorithms v1.0 is used without modifications and licensed by MPL Version 1.1. The source for TreeMap Algorithms can be obtained from http://www.cs.umd.edu/hcil/treemap/

** iTextAsian 1.0 is licensed by MPL Version 1.1 and the source can obtained from: http://itextpdf.com/download.php

MOZILLA PUBLIC LICENSE

Version 1.1

1. Definitions.

1.0.1. "Commercial Use" means distribution or otherwise making the Covered Code available to a third party.

1.1. "Contributor" means each entity that creates or contributes to the creation of Modifications.

1.2. "Contributor Version" means the combination of the Original Code, prior Modifications used by a Contributor, and the Modifications made by that particular Contributor.

1.3. "Covered Code" means the Original Code or Modifications or the combination of the Original Code andModifications, in each case including portions thereof.

1.4. "Electronic Distribution Mechanism" means a mechanism generally accepted in the software development community for the electronic transfer of data.

1.5. "Executable" means Covered Code in any form other than Source Code.

1.6. "Initial Developer" means the individual or entity identified as the Initial Developer in the SourceCode notice required by Exhibit A.

1.7. "Larger Work" means a work which combines Covered Code or portions thereof with code not governed by the terms of this License.

1.8. "License" means this document.

1.8.1. "Licensable" means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.9. "Modifications" means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is:

A. Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.

B. Any new file that contains anypart of the Original Code or previous Modifications.

1.10. "Original Code" means Source Code of computer software code which is described in the Source Code notice required by Exhibit A as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.

1.10.1. "Patent Claims" means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

1.11. "Source Code" means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of anExecutable, or source code differential comparisons against eitherthe Original Code or another well known, available Covered Code of the Contributor's choice. The Source Code can be in a compressed orarchival form, provided the appropriate decompression or de-archiving software is widely available for no charge.

1.12. "You" (or "Your") means an individual or a legal entity exercising rights under, and complyingwith all of the terms of, this License or a future version of thisLicense issued under Section 6.1. For legal entities, "You"includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, "control"means (a) the power, direct or indirect, to cause the direction or management ofsuch entity, whether by contract or otherwise, or (b) ownershipof more than fifty percent (50%) of the outstanding shares orbeneficial ownership of such entity.

2. Source Code License.

2.1. The Initial Developer Grant.

The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims:

(a) under intellectual property rights (other than patent or trademark) Licensable by Initial Developer to use, reproduce, modify, display, perform, sublicense and distribute the Original Code (or portions thereof) with or without Modifications, and/or as part of a Larger Work; and

(b) under Patents Claims infringed by the making, using or selling of Original Code, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Code (or portions thereof).

(c) the licenses granted in this Section 2.1(a) and (b) are effective on the date Initial Developer first distributes Original Code under the terms of this License.

(d) Notwithstanding Section 2.1(b) above, no patent license is granted: 1) for code that You delete from the Original Code; 2) separate from the Original Code; or 3) for infringements caused by: i) the modification of the Original Code or ii) the combination of the Original Code with other software or devices.

2.2. Contributor Grant.

Subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license

(a) under intellectual property rights (other than patent or trademark) Licensable by Contributor, to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code and/or as part of a Larger Work; and

(b) under Patent Claims infringed by the making, using, or selling of Modifications made by that Contributor either alone and/or in combination with its Contributor Version (or portions of such combination), to make, use, sell, offer for sale, have made, and/or otherwise dispose of: 1) Modifications made by that Contributor (or portions thereof); and 2) the combination of Modifications made by that Contributor with its Contributor Version (or portions of such combination).

(c) the licenses granted in Sections2.2(a) and 2.2(b) are effective on the date Contributor first makes Commercial Use of the Covered Code.

(d) Notwithstanding Section 2.2(b) above, no patent license is granted: 1) for any code that Contributor has deleted from the Contributor Version; 2) separate from the Contributor Version;3) for infringements caused by: i) third party modifications of Contributor Version or ii) the combination of Modifications made by that Contributor with other software (except as part of the Contributor Version) or otherdevices; or 4) under Patent Claims infringed by Covered Code in theabsence of Modifications made by that Contributor.

3. Distribution Obligations.

3.1. Application of License.

The Modifications which You create or to which You contribute are governed by the terms of this License,including without limitation Section 2.2. The Source Code version of Covered Code may be distributed only under the terms of thisLicense or a future version of this License released under Section6.1, and You must include a copy of this License with every copy ofthe Source Code You distribute. You may not offer or imposeany terms on any Source Code version that alters or restricts theapplicable version of this License or the recipients' rightshereunder. However, You may include an additional document offering theadditional rights described in Section 3.5.

3.2. Availability of Source Code.

Any Modification which You create or to which You contribute must be made available in Source Code form under the terms of this License either on the same media as an Executable version or via an accepted Electronic Distribution Mechanism to anyone to whom you made an Executable version available; and if made available via Electronic Distribution Mechanism, must remain available for at least twelve (12) months after the date it initially became available, or at least six (6) months after a subsequent version of that particular Modification has been made available to such recipients. You are responsible for ensuring that the Source Code version remains available even if the Electronic Distribution Mechanism is maintained by a third party.

3.3. Description of Modifications.

You must cause all Covered Code to which You contribute to contain a file documenting the changes You made tocreate that Covered Code and the date of any change. You must includea prominent statement that the Modification is derived, directly orindirectly, from Original Code provided by the Initial Developer and including the name of the Initial Developer in (a) the Source Code,and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

3.4. Intellectual Property Matters

(a) Third Party Claims.

If Contributor has knowledge that a license under a third party's intellectual property rights is required to exercise the rights granted by such Contributor under Sections 2.1 or 2.2, Contributor must include a text file with the Source Code distribution titled "LEGAL" which describes the claim and the party making the claim in sufficient detail that a recipient will know whom to contact. If Contributor obtains such knowledge after the Modification is made available as described in Section 3.2, Contributor shall promptly modify the LEGAL file in all copies Contributor makes available thereafter and shall take other steps (such as notifying appropriate mailing lists or newsgroups) reasonably calculated to inform those who received the Covered Code that new knowledge has been obtained.

(b) Contributor APIs.

If Contributor's Modifications include an application programming interface and Contributor has knowledge of patent licenses which are reasonably necessary to implement that API, Contributor must also include this information in the LEGAL file.

(c) Representations.

Contributor represents that, exceptas disclosed pursuant to Section 3.4(a) above, Contributorbelieves that Contributor's Modifications are Contributor'soriginal creation(s) and/or Contributor has sufficient rights togrant the rights conveyed by this License.

3.5. Required Notices.

You must duplicate the notice in Exhibit A in each file of the Source Code. If it is not possible to put such notice in a particular Source Code file due to its structure, then You must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If You created one or more Modification(s) You may add your name as a Contributor to the notice described in Exhibit A. You must also duplicate this License in any documentation for the Source Code where You describe recipients' rights or ownership rights relating to Covered Code. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear than any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

3.6. Distribution of Executable Versions.

You may distribute Covered Code in Executable form only if the requirements of Section 3.1-3.5 have been met for that Covered Code, and if You include a notice stating that the Source Code version of the Covered Code is available under theterms of this License, including a description of how and whereYou have fulfilled the obligations of Section 3.2. The noticemust be conspicuously included in any notice in an Executable version,related documentation or collateral in which You describerecipients' rights relating to the Covered Code. You may distribute theExecutable version of Covered Code or ownership rights under a licenseof Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this Licenseand that the license for the Executable version does not attempt tolimit or alter the recipient's rights in the Source Code version fromthe rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. You herebyagree to indemnify the Initial Developer and every Contributorfor any liability incurred by the Initial Developer or such Contributoras a result of any such terms You offer.

3.7. Larger Works.

You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Code.

4. Inability to Comply Due to Statute or Regulation.

If it is impossible for You to comply with any of the terms of this License with respect to some or all ofthe Covered Code due to statute, judicial order, or regulationthen You must: (a) comply with the terms of this License to the maximumextent possible; and (b) describe the limitations and the codethey affect. Such description must be included in the LEGAL filedescribed in Section 3.4 and must be included with all distributions of theSource Code. Except to the extent prohibited by statute orregulation, such description must be sufficiently detailed for a recipient ofordinary skill to be able to understand it.

5. Application of this License.

This License applies to code to which the Initial Developer has attached the notice in Exhibit A and to related Covered Code.

6. Versions of the License.

6.1. New Versions.

Netscape Communications Corporation ("Netscape") may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

6.2. Effect of New Versions.

Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms ofthat version. You may also choose to use suchCovered Code under the terms of any subsequent version of the Licensepublished by Netscape. No one other than Netscape has the right tomodify the terms applicable to Covered Code created under this License.

6.3. Derivative Works.

If You create or use a modified version of this License (which you may only do in order to apply it to code which is not already Covered Code governed by this License), You must (a)rename Your license so that the phrases "Mozilla","MOZILLAPL", "MOZPL", "Netscape", "MPL", "NPL" or anyconfusingly similar phrase do not appear in your license (except to note that your licensediffers from this License) and (b) otherwise make it clear that Yourversion of the license contains terms which differ from theMozilla Public License and Netscape Public License. (Filling in thename of the Initial Developer, Original Code or Contributorin the notice described in Exhibit A shall not of themselves bedeemed to be modifications of this License.)

7. DISCLAIMER OF WARRANTY.

COVERED CODE IS PROVIDED UNDER THIS LICENSE ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE COVERED CODE IS FREE OF DEFECTS, MERCHANTABLE, FIT FOR A PARTICULAR PURPOSE OR NON-INFRINGING. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE COVERED CODE IS WITH YOU. SHOULD ANY COVERED CODE PROVE DEFECTIVE IN ANY RESPECT, YOU (NOT THE INITIAL DEVELOPER OR ANY OTHER CONTRIBUTOR) ASSUME THE COST OF ANY NECESSARY SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED CODE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

8. TERMINATION.

8.1. This License and the rights granted hereunder will terminate automatically if You fail to comply withterms herein and fail to cure such breach within 30 days of becomingaware of the breach. All sublicenses to the Covered Code which areproperly granted shall survive any termination of this License.Provisions which, by their nature, must remain in effect beyond thetermination of this License shall survive.

8.2. If You initiate litigation by asserting a patent infringement claim (excluding declatory judgment actions) against Initial Developer or a Contributor (the Initial Developeror Contributor against whom You file such action is referred to as"Participant") alleging that:

(a)such Participant's Contributor Version directly or indirectly infringes any patent, then any and allrights granted by such Participant to You under Sections 2.1and/or 2.2 of this License shall, upon 60 days notice fromParticipant terminate prospectively, unless if within 60 days after receipt ofnotice You either: (I) agree in writing to pay Participant amutually agreeable reasonable royalty for Your past and future use ofModifications made by such Participant, or (ii) withdraw Yourlitigation claim with respect to the Contributor Version against suchParticipant. If within 60 days of notice, a reasonable royalty andpayment arrangement are not mutually agreed upon in writing by theparties or the litigation claim is not withdrawn, the rights granted byParticipant to You under Sections 2.1 and/or 2.2 automaticallyterminate at the expiration of the 60 day notice period specified above.

(b)any software, hardware, or device, other than such Participant's Contributor Version, directly orindirectly infringes any patent, then any rights granted to You by suchParticipant under Sections 2.1(b) and 2.2(b) are revoked effective as ofthe date You first made, used, sold, distributed, or had made,Modifications made by that Participant.

8.3. If You assert a patent infringement claim against Participant alleging that such Participant's Contributor Version directly or indirectly infringes any patent wheresuch claim is resolved (such as by license or settlement) prior to theinitiation of patent infringement litigation, then thereasonable value of the licenses granted by such Participant underSections 2.1 or 2.2 shall be taken into account in determining the amount orvalue of any payment or license.

8.4. In the event of termination under Sections 8.1 or 8.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or any distributor hereunder prior to termination shall survive termination.

9. LIMITATION OF LIABILITY.

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU, THE INITIAL DEVELOPER, ANY OTHER CONTRIBUTOR, OR ANY DISTRIBUTOR OF COVERED CODE, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO ANY PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTY'S NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

10. U.S. GOVERNMENT END USERS.

The Covered Code is a "commercial item," as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consistingof "commercial computer software" and "commercialcomputer software documentation," as such terms are used in 48 C.F.R. 12.212 (Sept.1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1through 227.7202-4 (June 1995), all U.S. Government End Users acquireCovered Code with only those rights set forth herein.

11. MISCELLANEOUS.

This License represents the complete agreement concerning subject matter hereof. If any provision of thisLicense is held to be unenforceable, such provision shall bereformed only to the extent necessary to make it enforceable. ThisLicense shall be governed by California law provisions (except to theextent applicable law, if any, provides otherwise), excluding itsconflict-of-law provisions. With respect to disputes in which atleast one party is a citizen of, or an entity chartered or registered todo business in the United States of America, any litigationrelating to this License shall be subject to the jurisdiction of theFederal Courts of the Northern District of California, with venue lyingin Santa Clara County, California, with the losing partyresponsible for costs, including without limitation, court costs andreasonable attorneys' fees and expenses. The application of the UnitedNations Convention on Contracts for the International Sale ofGoods is expressly excluded. Any law or regulation which provides thatthe language of a contract shall be construed against the draftershall not apply to this License.

12. RESPONSIBILITY FOR CLAIMS.

As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

13. MULTIPLE-LICENSED CODE.

Initial Developer may designate portions of the Covered Code as "Multiple-Licensed". "Multiple-Licensed" means that the Initial Developer permits you to utilize portions of the Covered Code under Your choice of the NPL or the alternative licenses, if any, specified by the Initial Developer in the file described in Exhibit A.

EXHIBIT A -Mozilla Public License.

``The contents of this file are subject to the Mozilla Public License Version 1.1 (the "License");you may not use this file except in compliance with the License. You mayobtain a copy of the License at http://www.mozilla.org/MPL/

Software distributed under the License is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governingrights and limitations under the License.

The Original Code is ____.

The Initial Developer of the Original Code is _________________________.

Portions created by ______________________ are Copyright (C) ______ _______________________. All Rights Reserved.

Contributor(s): ______________________________________.

Alternatively, the contents of this file may be used under the terms of the _____ license (the "[___] License"), in which case the provisions of [______] License are applicable instead of those above. If you wish to allow use of your version of this file only under the terms of the [____] License and not to allow others to use your version of this file under the MPL, indicate your decision by deleting the provisions above and replace them with the notice and other provisions required by the [___] License. If you do not delete the provisions above, a recipient may use your version of this file under either the MPL or the [___] License."

[NOTE: The text of this Exhibit A may differ slightly from the text of the notices in the Source Code files of the Original Code. You should use the text of this Exhibit A rather than the text found in the Original Code Source Code for Your Modifications.]

==

**MD Datejs

Copyright © 2006-2010 Coolite Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to dealin the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE ANDNONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT,TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THESOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

==

**JQuery

Copyright © 2009 John Resig

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE ANDNONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLEFOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OFCONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THESOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

==

** JCalendar 1.3.2

This product uses JCalendar 1.3.2. JCalendar is distributed pursuant to the terms of the Lesser General Public License. The source code for the JCalendar may be obtained from http://www.toedter.com/en/jcalendar/index.html

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the library's name and an idea of what it does.

Copyright (C) year name of author

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public

License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

signature of Ty Coon, 1 April 1990

Ty Coon, President of Vice

That's all there is to it!

APPENDIX C Limitations

This chapter defines the limitations experienced when using iPad Safari.

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.