Forum Systems Sentry™ Version 9.1

Monitoring and Reporting Guide

Legal Marks

Forum Sentry™ Version 9.1 Monitoring and Reporting Guide, published July 2020.

D-ASF-SE-012218

Table of Contents

List of Figures

INTRODUCTION TO THE MONITORING AND REPORTING GUIDE

Conventions Used

A red asterisk (*) aligned with a field term means that this field is required. In this and other documentation, the Web Administration Interface is referred to as the WebAdmin and the Forum XML Security Appliance™ is referred to as the 'device', 'product' or 'system'.

In this document, all data or commands that must be entered or selected are displayed in boldface. Example:

User name: **johnsmith**
Password: **********

UI screens which display a STATUS column represent the following states:

- Green status light = enabled policy.
- Yellow status light = a required functional element of this policy is disabled.
- Red status light = disabled policy.

Throughout this and other documents in the Documentation Set, repetitive actions such as:

- View / edit a policy.
- Enable / disable a policy.
- Delete a policy.
- Rename a policy.
- Limit display of policies with Search or Max Results fields.

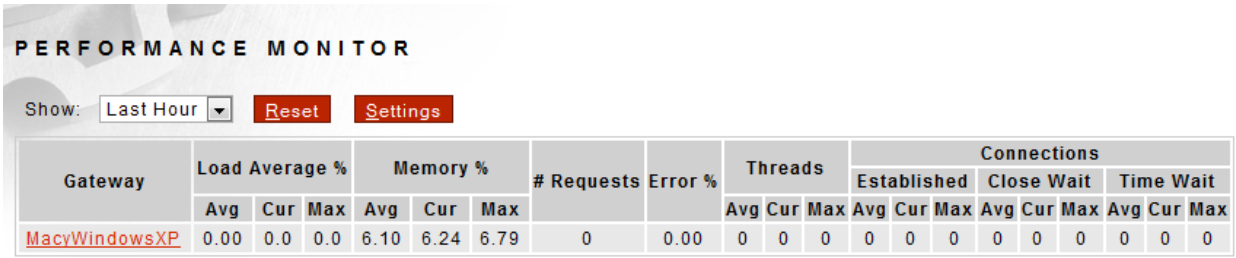
are not shown. For more information, refer to the Common Operations section of the *Forum Systems Sentry™ Version 9.1 Web-based Administration Guide*.

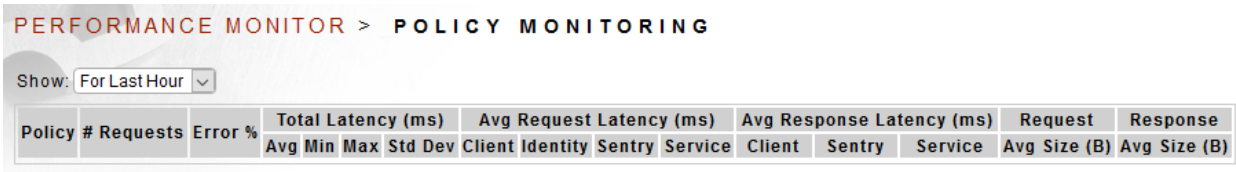
Customers with plug-in licenses on the system, confirm that your Integration License is visible on the General Info screen under the SUPPORTED FEATURES section.

Any specifications and constraints referenced in this volume appear in the Appendices of this volume.

PERFORMANCE MONITOR

The Performance Monitor keeps track of transactions and statistics across all policies on the device and provides the 7 segments of latency metric tracking as well as CPU and memory statistics of the system.





WS MONITORING

The Web Service (WS) Monitoring screen displays a summary of activity for WSDL and XML policies. In the following graphic, only the top WSDL policy is enabled; therefore, only that WSDL policy displays activity data in the Web Service Monitoring screen. Reset the monitoring data without rebooting by selecting the **Reset** button at the bottom of the screen.

Web Monitoring Screen Terms

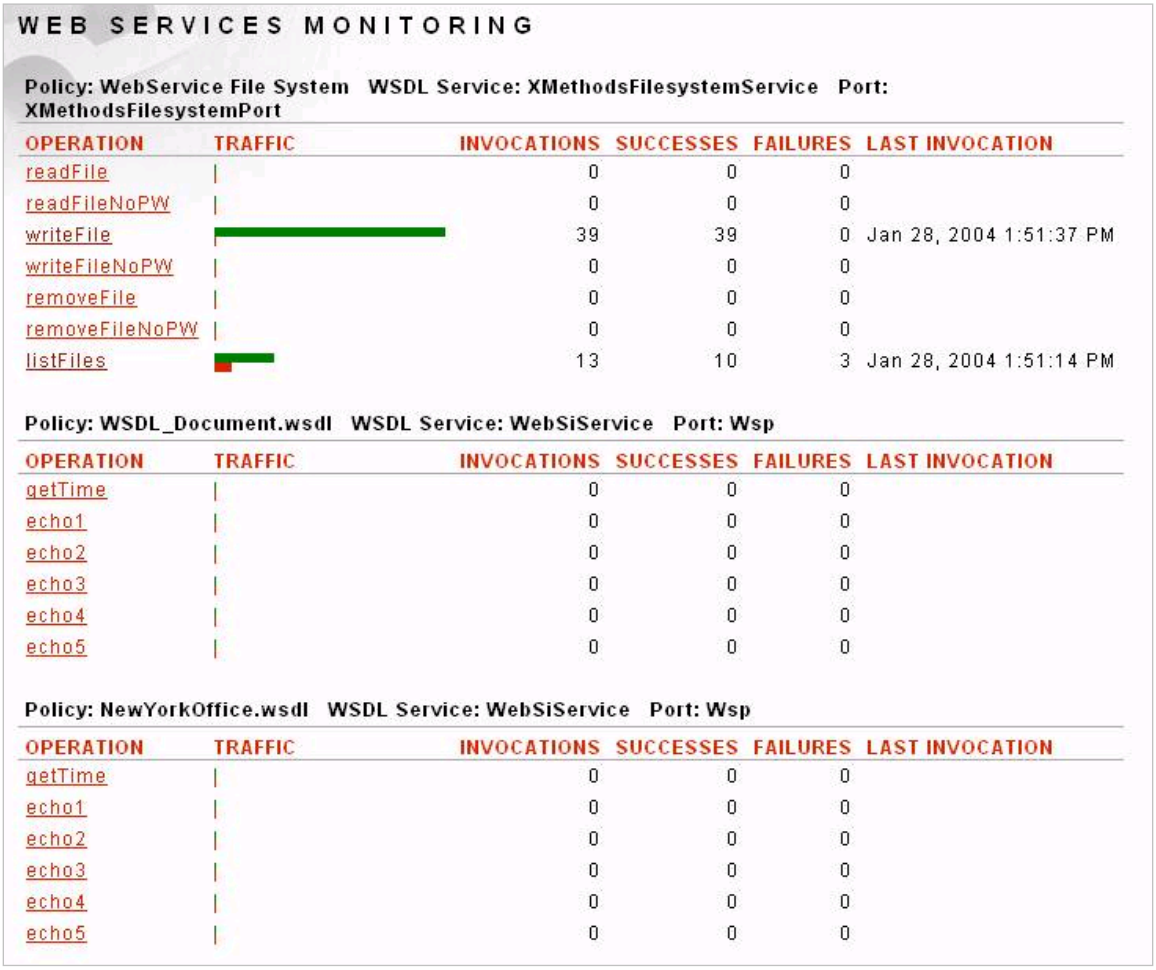
While working with the Web Monitoring screen, please consider the following:

FIELD NAME	DEFINITION
Operation	Operation is the name of each WSDL operation being called in the WSDL policy. **Note:** While two operations with the same name can be monitored separately, Web Services Reporting displays them as a single unit with the two sets of data combined into one.
Client IP	The Client IP column maps which client IP is being graphically represented on the screen.
Traffic	The Traffic column is a double bar chart that represents the frequency that each WSDL operation is accessed. The green bar represents successes, the same data visible under the SUCCESSES column. The red bar represents failures, the same data visible under the FAILURES column.
Invocations	The Invocations column lists the number of invocations for each operation in the WSDL policy.
Successes	The Successes column lists the number of successful requests per operation in the

	WSDL policy.
Failures	The Failures column lists the number of failed requests or responses per operation in the WSDL policy.
Last Invocation	The Last invocation column lists a date/timestamp of the last operation request in the WSDL policy.
Reset	When clicked, resets WS Monitoring data without rebooting the appliance, setting the data back to zero.
Virtual Directory	When monitoring XML Policies that do not have Operations, the statistics are broken out by Virtual Directories.

View Traffic Details

Administrators may view details of any operation or virtual directory that displays traffic (with a progress bar visible).



WEB SERVICES MONITORING

Policy: WebService File System WSDL Service: XMethodsFilesystemService Port: XMethodsFilesystemPort

OPERATION	TRAFFIC	INVOCATIONS	SUCCESSES	FAILURES	LAST INVOCATION
readFile		0	0	0	
readFileNoPW		0	0	0	
writeFile		39	39	0	Jan 28, 2004 1:51:37 PM
writeFileNoPW		0	0	0	
removeFile		0	0	0	
removeFileNoPW		0	0	0	
listFiles		13	10	3	Jan 28, 2004 1:51:14 PM

Policy: WSDL_Document.wsdl WSDL Service: WebSiService Port: Wsp

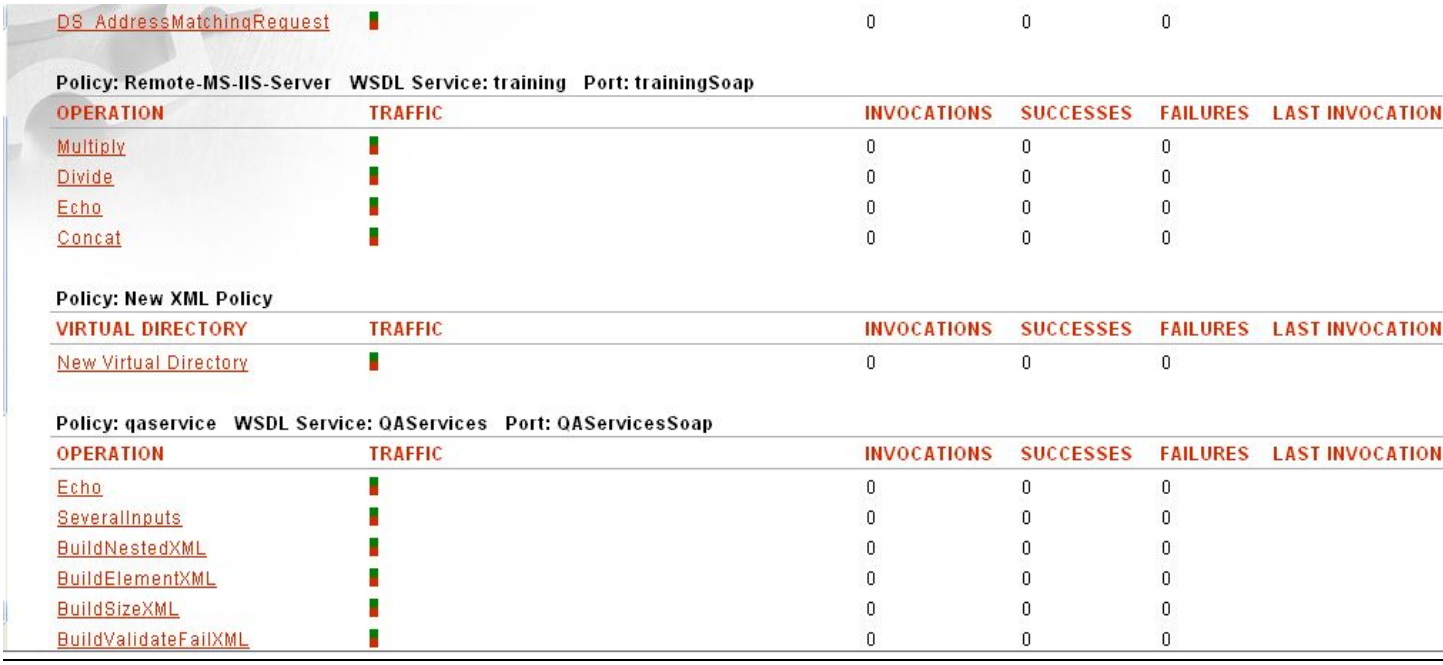
OPERATION	TRAFFIC	INVOCATIONS	SUCCESSES	FAILURES	LAST INVOCATION
getTime		0	0	0	
echo1		0	0	0	
echo2		0	0	0	
echo3		0	0	0	
echo4		0	0	0	
echo5		0	0	0	

Policy: NewYorkOffice.wsdl WSDL Service: WebSiService Port: Wsp

OPERATION	TRAFFIC	INVOCATIONS	SUCCESSES	FAILURES	LAST INVOCATION
getTime		0	0	0	
echo1		0	0	0	
echo2		0	0	0	
echo3		0	0	0	
echo4		0	0	0	
echo5		0	0	0	

Clicking on the Operation or Virtual Directory link in the top WSDL Policy, and the OPERATION DETAIL screen appears, presenting a summary of information for that Operation. Press your browser <**back**> button to return to the WEB SERVICES MONITORING screen.

A new feature added to the 9.1 release has been the display of monitoring statistics for XML Policies. This feature did not exist in the previous release. Please see the following figure where XML Policy statistics can be viewed under Policy: New XML Policy label:



WS REPORTS

The Web Services (WS) Reports screen provides a method of capturing, filtering and scheduling data to be presented as either data or a graphical chart.

Administrators may add, edit/view, and delete Web Services Reports as well as view reporting Settings. Administrators may preview the data being queried (if data is currently available) in a Web Services Report (as a Chart) before saving the query criteria. Additionally, Administrators may schedule a Web Services Report for email delivery, and disable Web Services Reporting functionality entirely.

Available Reports

The types of reports available include:

- Number of Hits
- Throughput
- Request Size
- Response Size
- Response Time
- Number of Faults

Number of Hits Report

The Number of Hits report provides a report summary based on the number of hits on each URI and virtual IP address/port listed in the WSDL and XML policies on the system.

Throughput Report

The Throughput report provides a report summary based on bytes per second.

Request Size Report

The Request Size report provides a report summary based on the sizes (in bytes) of requests leaving the system.

Response Size Report

The Response Size report provides a report summary based on the sizes (in bytes) of responses entering the system.

Response Time Report

The Response Time report provides a report summary based on the lifetime of active requests in WSDL and XML policies in the system and the time a response is processed on the WSDL and XML Policies in the system.

Number of Faults Report

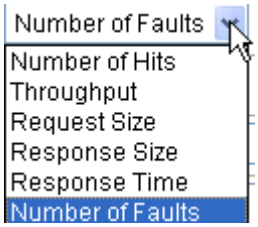
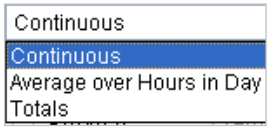
The Number of Faults report provides a report summary based on the number of faults on each URI and virtual IP address/port listed in the WSDL and XML policies on the system.

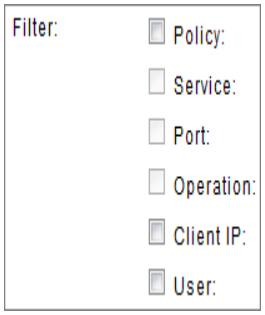
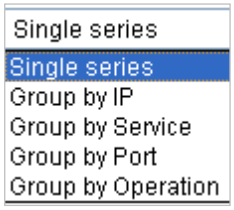
Context-sensitive Help on Charts

By placing your cursor on the XY axis of a chart, the date/time is visible adjacent to a bolded ? through context-sensitive Help.

Web Services Reporting Criteria Screen Terms

While working with the WS Reports screen, please consider the following:

FIELD NAME	DEFINITION
Report Name	The identifier for this Report
Report Type 	Report types can be: • Number of Hits • Throughput • Request Size • Response Size • Response Time • Number of Faults
Time Period 	The Time Period drop down allows users to select which block of time to capture in a report, including: • Today – lists all data captured between current time and 12:00 AM. • Yesterday – lists all data captured during the previous calendar day. • Last 24 hours – lists all data captured between current time and backwards exactly 24 hours. • Week to date – lists all data captured between today and backwards to Sunday. • Last week – lists all data captured from the start of the last week (Sunday) to the end of the last week (Saturday). • Last 7 days – lists all data captured between today and backwards 7 complete days. • Month to date – lists all data captured between today and backwards one complete month. • Last month – lists all data captured during the last calendar month. • Year to date – lists all data captured between today and backwards one year. • Last year – lists all data captured for the previous calendar year. • Custom – after entering values in the From and To fields, lists all the data captured during the From and To blocks of time.
View 	The View drop down allows users to select which view of the data to capture for a report, including: • Continuous –captures data as it is continuously monitored by the system. • Average over Hours in Day –captures aggregated data for each day within a given range of days, averages that data into 24 hourly blocks, and displays the data as a single 24 hour period. For more information, refer to the Example of Average Over Hours in Day Chart. • Totals –captures data and presents it as a cumulative TOTAL per day. No bar chart is visible on a day in which there are no hits.

FIELD NAME	DEFINITION
Filter 	Data can be filtered by: • Policy – users select a specific WSDL or XML policy. • Service – users select the name of the service in the WSDL or the virtual directory of the XML policy. • Port–users select the port of a specific WSDL. • Operation – users select the operation name in a specific WSDL. **Note:** If the WSDL includes same-named operations, checking the **Operation** checkbox aggregates all operations and does not distinguish between same-named operations when creating a Report or Chart. • Client IP – data is filtered by matching client IP entered. • User – user selects username that was used to connect to the system when making the request(s).
Data Series 	The Data Series drop down list allows users to view the presentation of data in the following categories: • Single series – data displayed with no grouping criteria. • Group by IP – data is grouped by the source IP so that multiple data series are displayed, each series corresponds to a different IP. • Group by Service – data is groups by name of Service in WSDLs. • Group by Port – data is groups by port in WSDLs. • Group by Operation – data is groups by operation name in WSDLs.

WSDL Report Delivery Screen Terms

While working with the WS Reports screen, please consider the following:

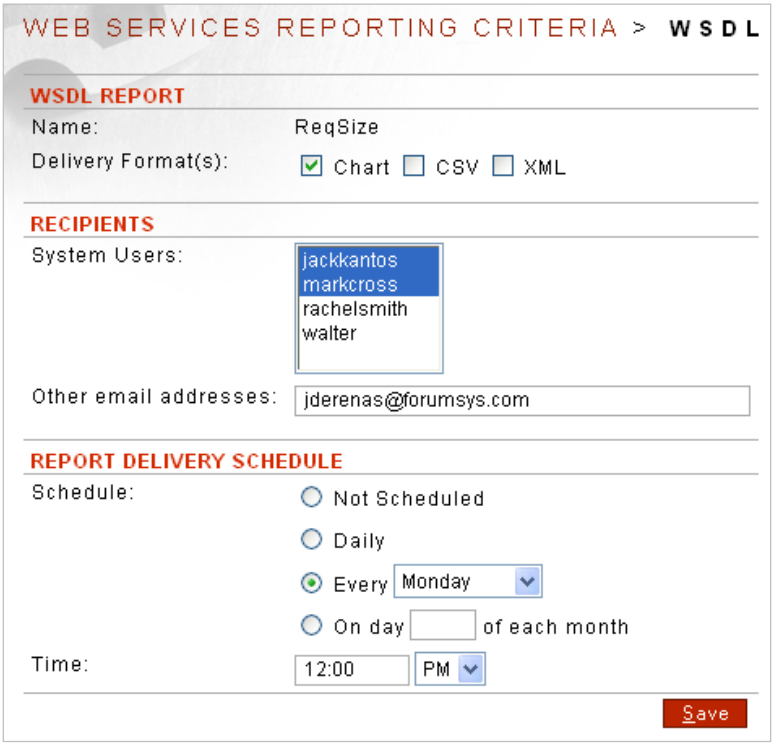
FIELD NAME	DEFINITION
Name	The identifier for this report.
Delivery Format(s)	• With Chart checked, the web services report is delivered as a chart. • With CSV checked, the web services report is delivered as a CSV file. • With XML checked, the web services report is delivered as an XML file.
System Users	One or more selected users who will receive the scheduled report.
Other email address	Email address of an additional recipient of a scheduled report.
Schedule	• With Not Scheduled selected, there is no report delivered. • With Daily selected, the report is delivered once each 24 hour period. • With Every and <day of the week> selected, the report is delivered on each weekday selected. • With On day of each month selected and <numeric value>, entered, the report is delivered on the specified day of the month.
Time	The hour and meridiem selected for report delivery.

Scheduled Reports Delivery Format and Time

Reports may be scheduled at specific intervals and frequencies to be delivered into your inbox. Scheduled reports are delivered in the following formats:

- chart
- comma separated value (csv)
- xml

Reports can be delivered in either one or all formats. Scheduled reports are emailed at the time specified by the Administrator, as the following graphic displays.



Example of Average Over Hours in Day Chart

The following chart captures aggregated data for each day within a given range of days, averages that data into 24 hourly blocks, and displays the data as one 24 hour period:

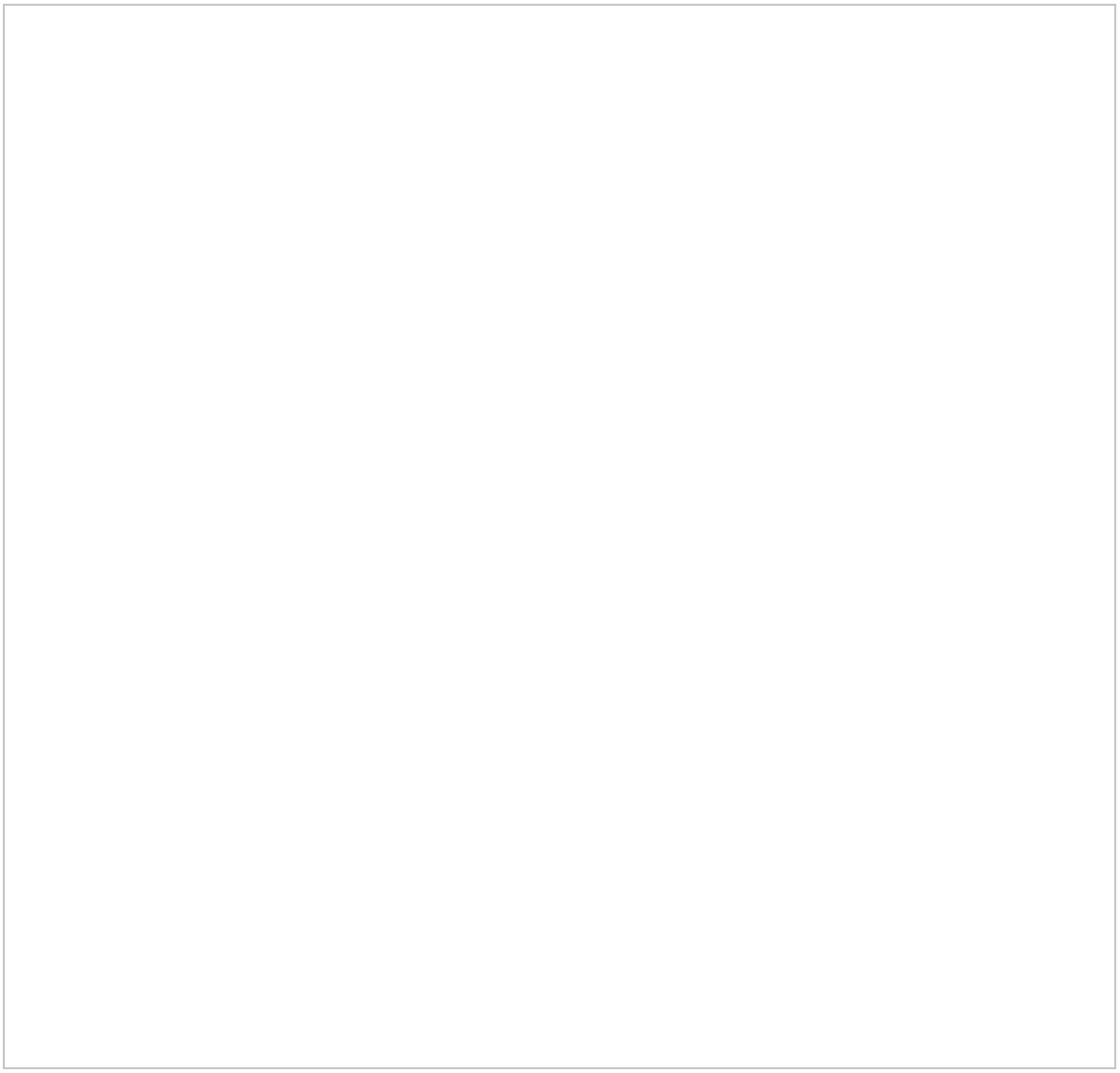
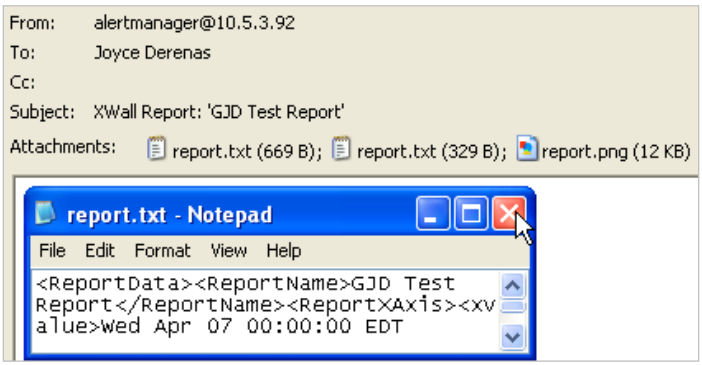
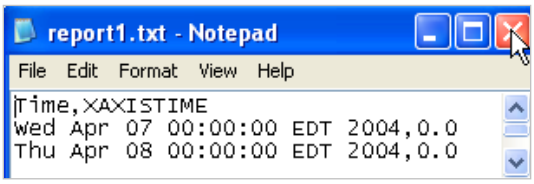


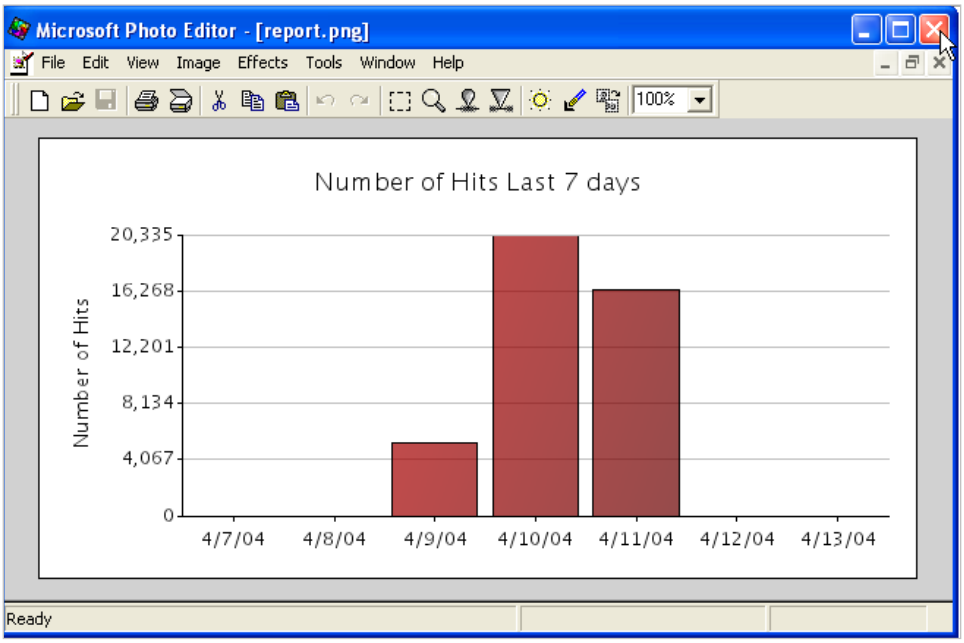
Figure 1: Example of an Average Over Hours in a Day Chart.

Emailed Reports

The following graphics display an inbox with email containing scheduled reports:



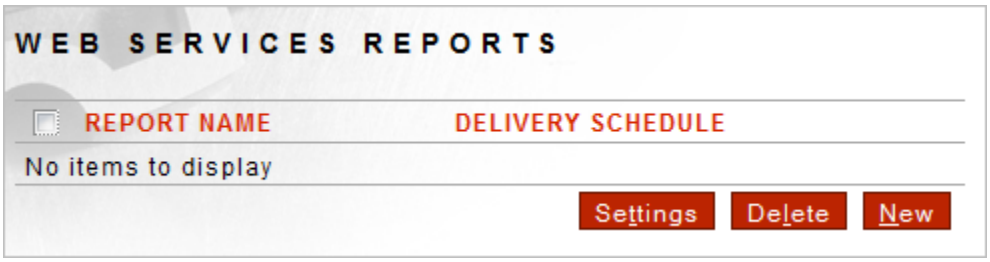


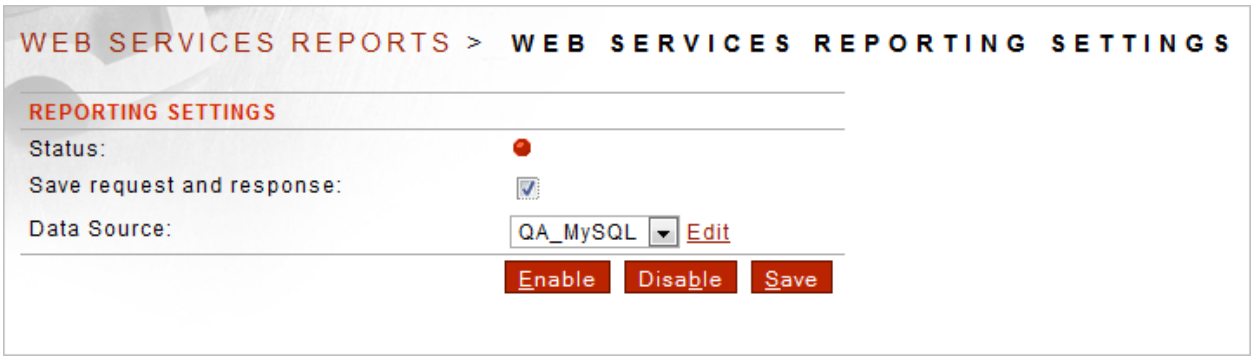


Note: Setting the view option to 100% guarantees clear graphs.

Web Services Report Settings

Administrators may manage settings for reporting by selecting the Settings command from the WEB SERVICES REPORTS screen. The REPORTING SETTINGS screen appears where Administrators may enable or disable databases and save these settings.





Reporting Settings Screen Terms

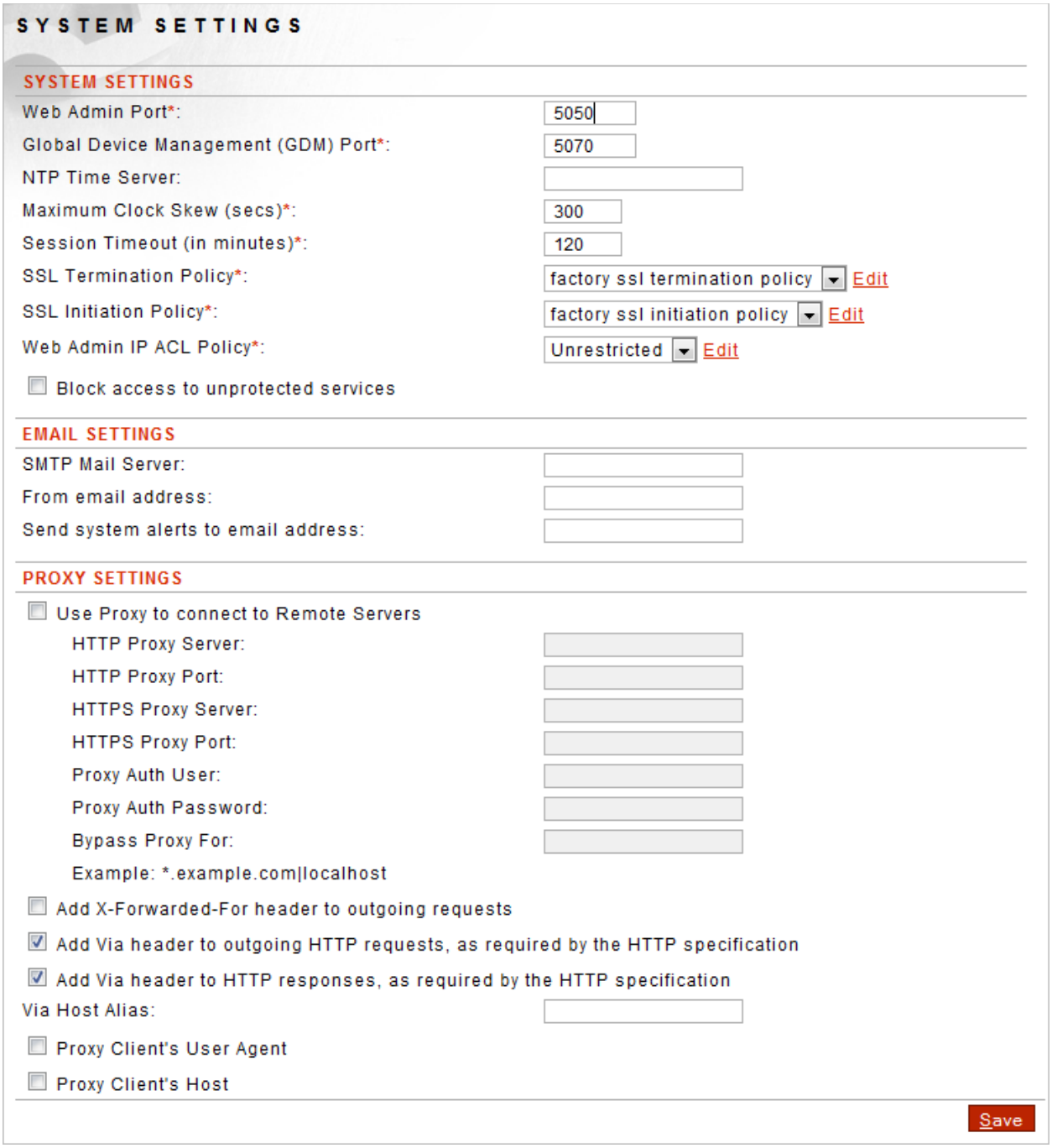
The terms and definitions for Reporting Settings screen include:

FIELD NAME	DEFINITION
Status	The status lights reflect the state of reporting settings after an Administrator has selected desired options, and then selected the Enable or Disable or Save commands. • A green status light indicates that reporting settings are enabled. • A yellow status light indicates that reporting settings are enabled, but either the archiving policy is not properly configured or an archiving database is not enabled. • A red status light indicates that reporting settings are disabled.
Save request and response	When checked, actual SOAP request/response messages, in addition to standard statistics, are saved to the Reporting Database. Forum recommends this option be set only for diagnostics since enabling this option will generate significantly more data in the database.
Data Source	The Data Source (database) that will be used to store the WS Reports data and the saved requests and responses if that option is enabled.

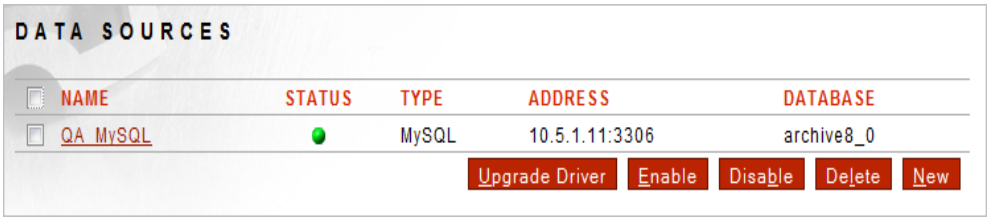
Reports Prerequisites

Before reports can be received, there are a few prerequisites which must be set to enable receiving WS Reports:

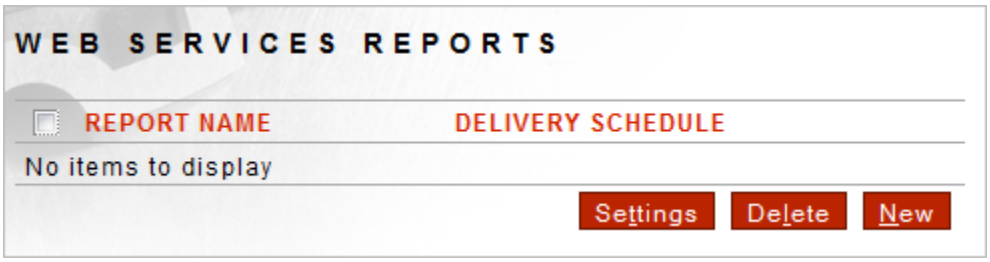
- From the **System Settings** screen, populate the **Email Settings** section, and Save.

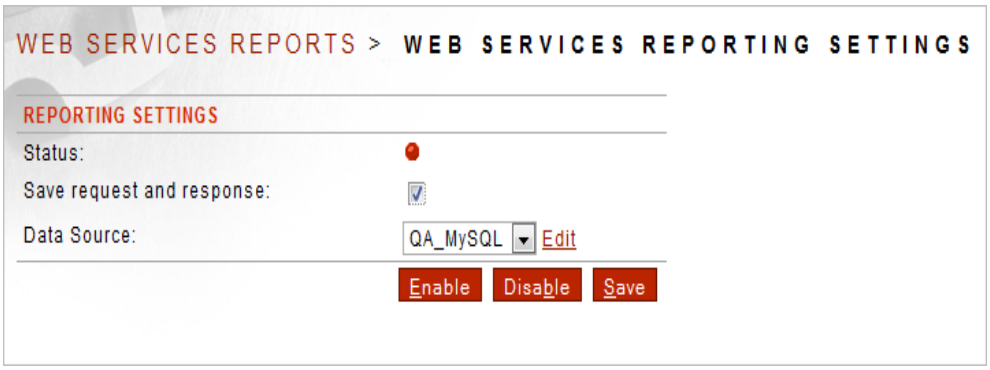


- From the **Data Sources** screen, Create, Test and Save your database configuration.

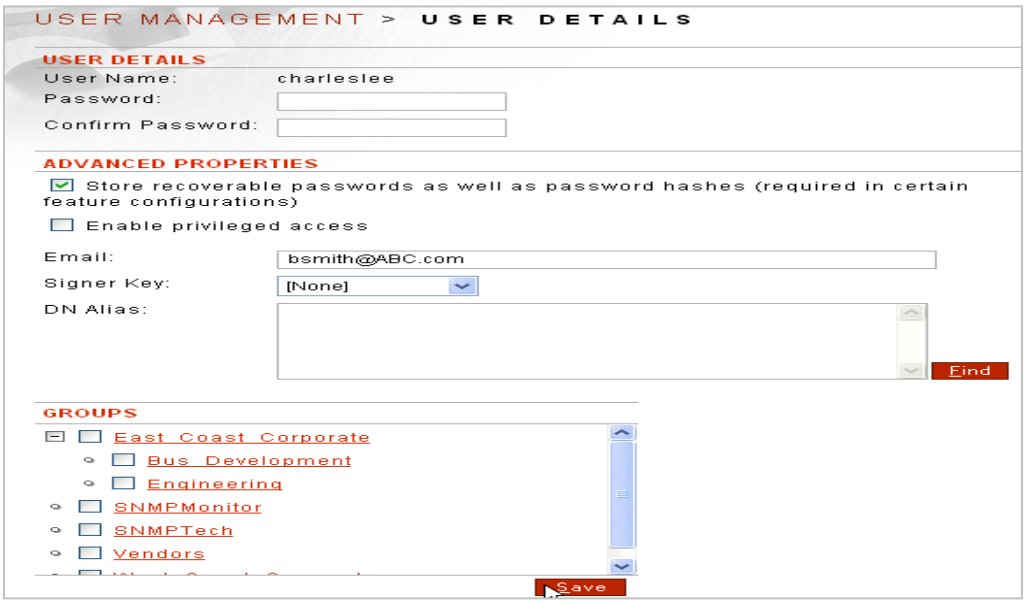


- From the **WS Reports** screen, select **Settings** and Enable one of the databases.





- On the **User Management Screen**, add an email to the user to receive reports.



WS Reports Examples

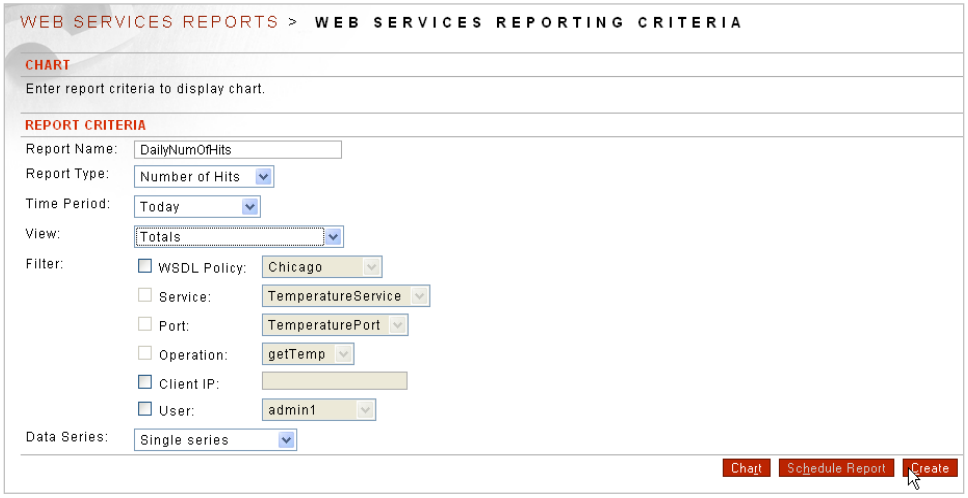
Examples for Web Services Reports include:

- Add a Web Services Report.
- Preview Web Services Report Data when Available.
- Schedule a Web Services Report for Delivery.
- Disable Delivery of a Web Services Report.
- Delete a Web Services Report.
- Enable / Disable all Web Services Reporting Functionality.

Note: For information on editing or viewing a Web Services Report, refer to the Common Operations section of the Forum Systems Sentry™ Version 9.1 Web-based Administration Guide.

Add a Web Services Report

Review the Reports Prerequisites section before creating your first web services report. Follow these steps to add a web services report:



- Navigate to the Reports Prerequisite section and comply with all appropriate settings discussed for enabling Web Services Reports.
- Navigate to the **WS Reports** screen.
- On the WEB SERVICES REPORTS screen, click **New**.
- On the WEB SERVICES REPORTING CRITERIA screen, enter a **name** for this report in the Report Name field.
- From the Report Type drop down list, select a **Report Type**.
- From the Time Period drop down list, select a **Time Period**.
- From the View drop down list, select a **View** of the data to be captured.
- From the Filter area, select a number of **filtering criteria** or skip them all. This example skips all the filtering options.

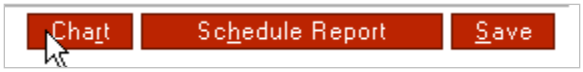
Note: Role-based access control, managed by the Active Role at the bottom of the screen, allows users to view WSDL policies appropriate to their level of access.

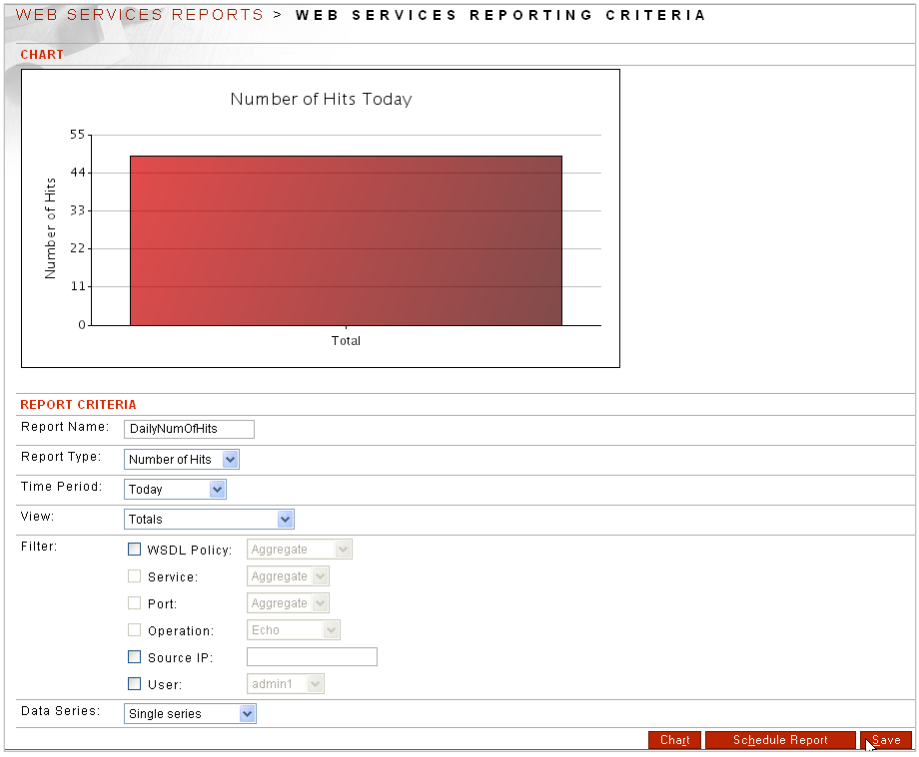
- From the Data Series drop down list, select an **option** to view the presentation of the data by a number of methods.
- Click **Create**.

Continue with the next instruction.

Preview Web Services Report Data when Available

Because there are so many options available when querying and capturing report data, Administrators may wish to preview the report before saving it. If the data is not currently available, a message stating this appears; otherwise, a preview of the report displays. Follow these steps to preview a web services report when data is available:





- Click **Chart**. The WEB SERVICES REPORTING CRITERIA screen refreshes with a chart of data visible at the top of the screen.

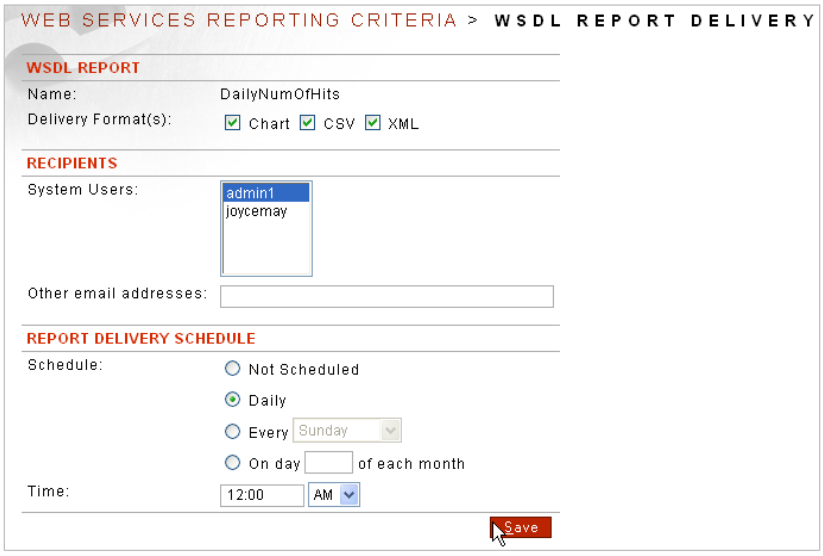
If the displayed Web Services Report is as you expected, click **Save**.

If not, change some of the REPORT CRITERIA options, and select **Chart** again.
Navigate to the Web Services Reports screen to view the newly created report with a notation that this report is not scheduled for delivery.

Continue with the next instruction.

Schedule a Web Services Report for Delivery

Continuing with the last operation, follow these steps to add a web services report scheduled for delivery:



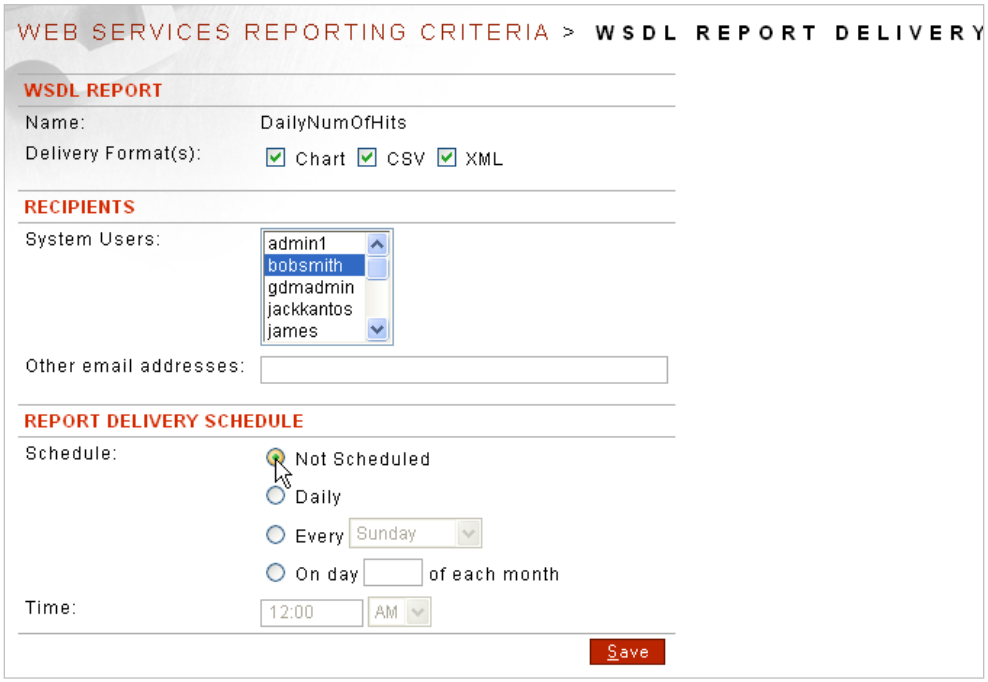
- Click **Schedule Report**.
- On the WSDL REPORT DELIVERY screen, aligned with Delivery Format(s), select **one** or **all** of the checkmarks adjacent to the Chart, CSV or XML option.
- From the System Users text box, select a **System User name** to receive the email alert.
- From the Other email addresses text field, enter **one** or **more** email addresses for others to receive an email alert.
- If entering multiple email addresses, separate with a comma.
- Under the REPORT DELIVERY SCHEDULE area, from the Schedule section, select **one** radio button for the Not Scheduled, Daily, Every or On Day < > of each month delivery option.

Note: If selecting the **Every** option, from the drop down list, select a day of the week for delivery. If selecting the **On day < >** of each month option, enter a numeric value for the day of the month delivery option.

- From the Time text box, overwrite **12:00** and change the delivery time to a new time. Maintain the HH:MM format.
- From the meridiem drop down list, select **AM** or **PM**.
- Click **Save**.

Disable Delivery of a Web Services Report

Follow these steps to disable delivery of a web services report:



- From the Navigator, select the **WS Reports** screen.
- On the WEB SERVICES REPORTS screen, click a Web Services Report name.
- On the WEB SERVICES REPORTING CRITERIA screen, click **Schedule Report**.
- On the WSDL REPORT DELIVERY screen, from the REPORT DELIVERY SCHEDULE area of the screen, aligned with Schedule, select the **Not Scheduled** radio button, and then click **Save**.

Delete a Web Services Report

Follow these steps to delete a Web Services Report:

- From the Navigator, select the **WS Reports** screen.
- On the WEB SERVICES REPORTS screen, check the **checkbox** prefacing the report name to delete and select **Delete**.
- The “Are you sure you want to delete the selected web service report?” message appears.
- Click **OK**.

Disable or Enable All Web Services Reporting Functionality

Follow these steps to disable all web services reporting functionality:

- From the Navigator, select the **WS Reports** screen.
- On the WEB SERVICES REPORTS screen, select **Settings**.
- On the REPORTING SETTINGS screen, select **Disable**.
- Select **Save**.

SNMP MANAGEMENT

A Simple Network Management Protocol (SNMP) is provided for read-only access to statistics and system information via an SNMP-capable manager.

The MIBS are located on the SNMP screen as links for easy copying and pasting. These are:

- SMI MIB
- General Information MIB
- Statistics MIB
- Appliance MIB

These MIB files include the Forum Systems MIBS and standard MIBS that apply to system and interface information.

SNMP management supports read-only access via v1, v2c and v3. Using SNMP requires the system Management IP address, the Forum private MIB files and an SNMP client application.

The SNMPMonitor group is a system group that provide members with access privileges to query SNMP information.

Note: Customers with the Forum software port will not see the Appliance MIB link; this link is only visible to customers running the system or the Type PCI-card.

SNMP Master Agent Command on the CLI

Administrators may review the SNMP configuration from the CLI with the following command:

COMMAND	DESCRIPTION
show snmp	Displays snmp name, location and contact.

Supported SNMP Traps

When starting up the system from Power UP using the system or a software port, SNMP traps allow the system to send an SNMP message, confirming that the system is up and running.

The Send Test Trap command is used to send a trap to the Management station to verify that traps can be sent successfully. The Send Test Trap command requires that the Trap IP Address has been entered and saved on the SNMP SETTINGS screen.

The traps supported in this release include:

- Coldstart (standard SNMPv2 trap)
- Shutdown (Forum)
- SNMP Traps as IDP Actions

SNMP Settings Screen Terms

While working with the SNMP Settings screen, please consider the following:

FIELD NAME	DEFINITION
GENERAL SETTINGS	
Contact	Contact name of the SNMP device.
Location	Location for the SNMP device.
Port	The port for the SNMP device. The default port is 161.
Trap IP Address	SNMP Manager's IP address
Community String	The community string desired for this SNMP integration. Default if public.
Maximum Octet String length	Each SNMP community is named by a string of octets. Octets are not characters. Default maximum string length is 1400.
Enabled	Check to enable an SNMP listener on the system. Uncheck to disable an SNMP listener on the system.
SNMPV3 SECURITY SETTINGS	
Use SNMPv3 Security	When checked, SNMP v3 security settings are used. When unchecked, SNMP v2c is used. Note: Customers using the HP Openview Management station must not select the Use SNMPv3 Security option.
Authentication	The authentication algorithm to use for this SNMP policy: • SHA • MD5
Encryption	The encryption algorithm to use for this SNMP policy: • AES • DES
MIBS	• The SMI MIB link is used to open, cut and paste the SMI MIBs. • The General Information MIB link is used to open, cut and paste the General Information MIBs. • The Statistics MIB link is used to open, cut and paste the Statistics MIBs. • The Appliance MIB link is used to open, cut and paste the Appliance MIBs.

SNMPWALK Syntax

The following table displays snmpwalk version commands supported on the system:

VERSION	SYNTAX AND EXAMPLE	LEVEL OF SUPPORT
snmpwalk -v1	-c public DEVICE_IP	public read-only access
	`-c public 162.93.84.129`	
snmpwalk -v2c	-c public DEVICE_IP	public read-only access
	`-c public 162.93.84.129`	
snmpwalk -v3 *	-l authpriv -u FORUM_USER -a SHA -A FORUM_USER_PASSWORD -x DES -X FORUM_USER_PASSWORD DEVICE_IP	secure authenticated queries
	`-l authpriv -u johncole -a SHA -A password -x DES -X password 162.93.84.129`	

* Forum MIBS are available only using v3 authpriv queries with SHA and DES algorithms.

Community String

The community string is "public" for v1 and v2c. If you are using the snmpwalk utility, you need to set up your ENVIRONMENT variable MIBS="ALL".

Troubleshoot SNMPWALK Command

With no authentication or network connectivity errors, and the dataset simply empty, please check that the following criteria has been met:

Have you set up the Forum Systems MIBS on the SNMP client machine? The MIBS are located on the SNMP screen as links for easy cutting and pasting. These include the SMI MIB, General Information MIB, Statistics MIB and the Appliance MIB.

If you are using the snmpwalk utility, you need to set up the ENVIRONMENT variable MIBS="ALL".

Sample SNMPWALK Command

The following is a sample snmpwalk configuration:

```
$ snmpwalk -v3 -l authpriv -u johncole -a SHA -A password -x DES
-X password 162.93.84.129 forumsysGeneralStatsMib
```

yields the following statistics information:

FORUMSYS-GENERAL-STATS-MIB::fsgsDocSizeAverage.0 = Counter64: 0 bytes
FORUMSYS-GENERAL-STATS-MIB::fsgsDocSizeMin.0 = Counter64: 0 bytes
FORUMSYS-GENERAL-STATS-MIB::fsgsDocSizeMax.0 = Counter64: 0 bytes
FORUMSYS-GENERAL-STATS-MIB::fsgsDocProcessPass.0 = Counter64: 0 documents
FORUMSYS-GENERAL-STATS-MIB::fsgsDocProcessFail.0 = Counter64: 0 documents
FORUMSYS-GENERAL-STATS-MIB::fsgsDocChars.0 = Counter64: 0 bytes
FORUMSYS-GENERAL-STATS-MIB::fsgsDocProxies.0 = Counter64: 0 documents
FORUMSYS-GENERAL-STATS-MIB::fsgsDocTotalErrors.0 = Counter64: 0
FORUMSYS-GENERAL-STATS-MIB::fsgsDocSigCreatePass.0 = Counter64: 0 signatures
FORUMSYS-GENERAL-STATS-MIB::fsgsDocSigCreateFail.0 = Counter64: 0 signatures
FORUMSYS-GENERAL-STATS-MIB::fsgsDocSigVerifyPass.0 = Counter64: 0 signatures
FORUMSYS-GENERAL-STATS-MIB::fsgsDocSigVerifyFail.0 = Counter64: 0 signatures
FORUMSYS-GENERAL-STATS-MIB::fsgsDocElemEncryptPass.0 = Counter64: 0 elements
FORUMSYS-GENERAL-STATS-MIB::fsgsDocElemEncryptFail.0 = Counter64: 0 elements
FORUMSYS-GENERAL-STATS-MIB::fsgsDocContEncryptPass.0 = Counter64: 0 encryptions
FORUMSYS-GENERAL-STATS-MIB::fsgsDocContEncryptFail.0 = Counter64: 0 encryptions
FORUMSYS-GENERAL-STATS-MIB::fsgsDocElemDecryptPass.0 = Counter64: 0 elements
FORUMSYS-GENERAL-STATS-MIB::fsgsDocElemDecryptFail.0 = Counter64: 0 elements
FORUMSYS-GENERAL-STATS-MIB::fsgsDocTransforms.0 = Counter64: 0 transformations
FORUMSYS-GENERAL-STATS-MIB::fsgsDocTransformChars.0 = Counter64: 0 bytes
FORUMSYS-GENERAL-STATS-MIB::fsgsDocValidPass.0 = Counter64: 0 documents
FORUMSYS-GENERAL-STATS-MIB::fsgsDocValidFail.0 = Counter64: 0 documents
FORUMSYS-GENERAL-STATS-MIB::fsgsDocArchPass.0 = Counter64: 0 documents
FORUMSYS-GENERAL-STATS-MIB::fsgsDocArchFail.0 = Counter64: 0 documents
FORUMSYS-GENERAL-STATS-MIB::fsgsDocArchiveChars.0 = Counter64: 0 bytes
FORUMSYS-GENERAL-STATS-MIB::fsgsCryptAccelEnabled.0 = INTEGER: true(1)
FORUMSYS-GENERAL-STATS-MIB::fsgsCryptRsaExponPass.0 = Counter64: 0 operations
FORUMSYS-GENERAL-STATS-MIB::fsgsCryptRsaExponFail.0 = Counter64: 0 operations
FORUMSYS-GENERAL-STATS-MIB::fsgsCryptRsaCrtPass.0 = Counter64: 3 operations
FORUMSYS-GENERAL-STATS-MIB::fsgsCryptRsaCrtFail.0 = Counter64: 0 operations
FORUMSYS-GENERAL-STATS-MIB::fsgsCryptPaddings.0 = Counter64: 0 paddings
FORUMSYS-GENERAL-STATS-MIB::fsgsCryptSignedHiBits.0 = Counter64: 0 operations
FORUMSYS-GENERAL-STATS-MIB::fsgsCryptMallocErrors.0 = Counter64: 0

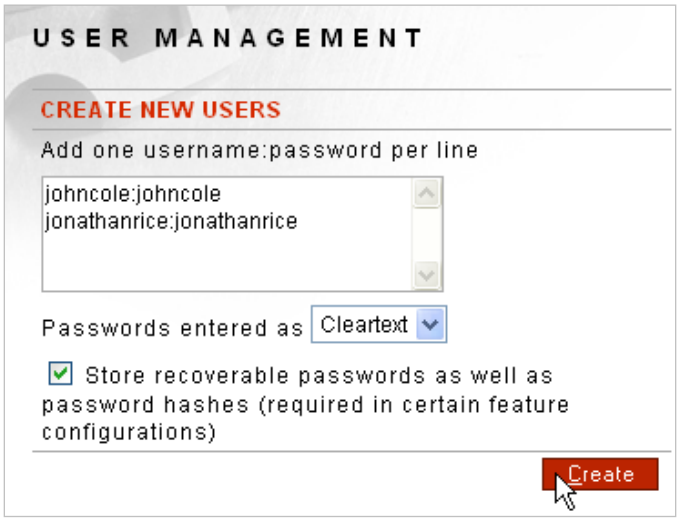
SNMP Configuration Examples

The example for configuring SNMP is Configure SNMP Security Settings and Send Test Trap.

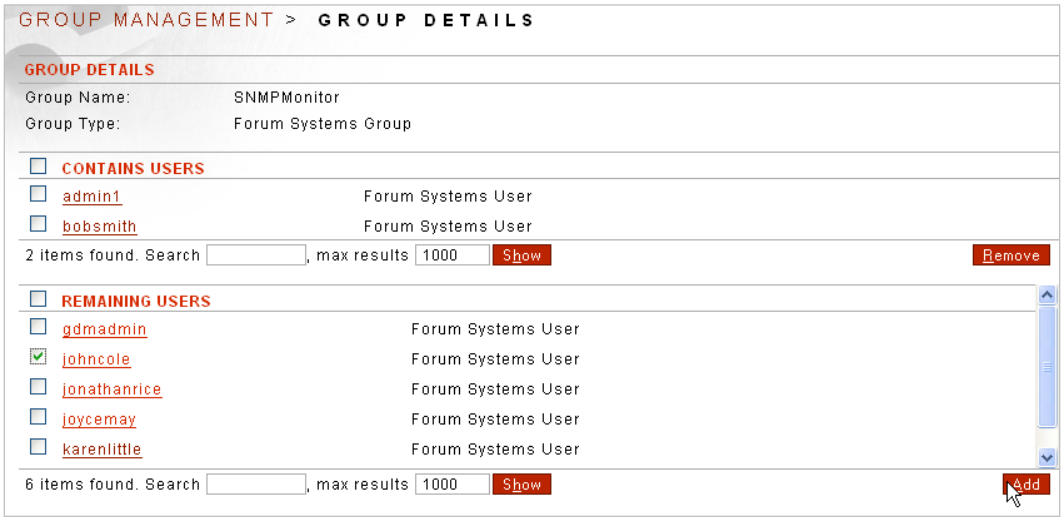
Configure SNMP Security Settings and Send Test Trap

To configure SNMP on the system:

- Create user policies from the Users screen, with the Store recoverable passwords as well as password hashes (required in certain feature configurations) checkbox checked. User passwords for users who will be assigned to the SNMPMonitor group or SNMPTech group must be entered in cleartext, are case sensitive, may be from 8 to 255 alphanumeric characters, and may include the '@' character, underscores and dashes. Additionally, the Store recoverable passwords as well as password hashes checkbox must be checked. When checked, a copy of the cleartext password is stored on the system. SNMP users must be configured for use with basic auth in order to use SNMP.

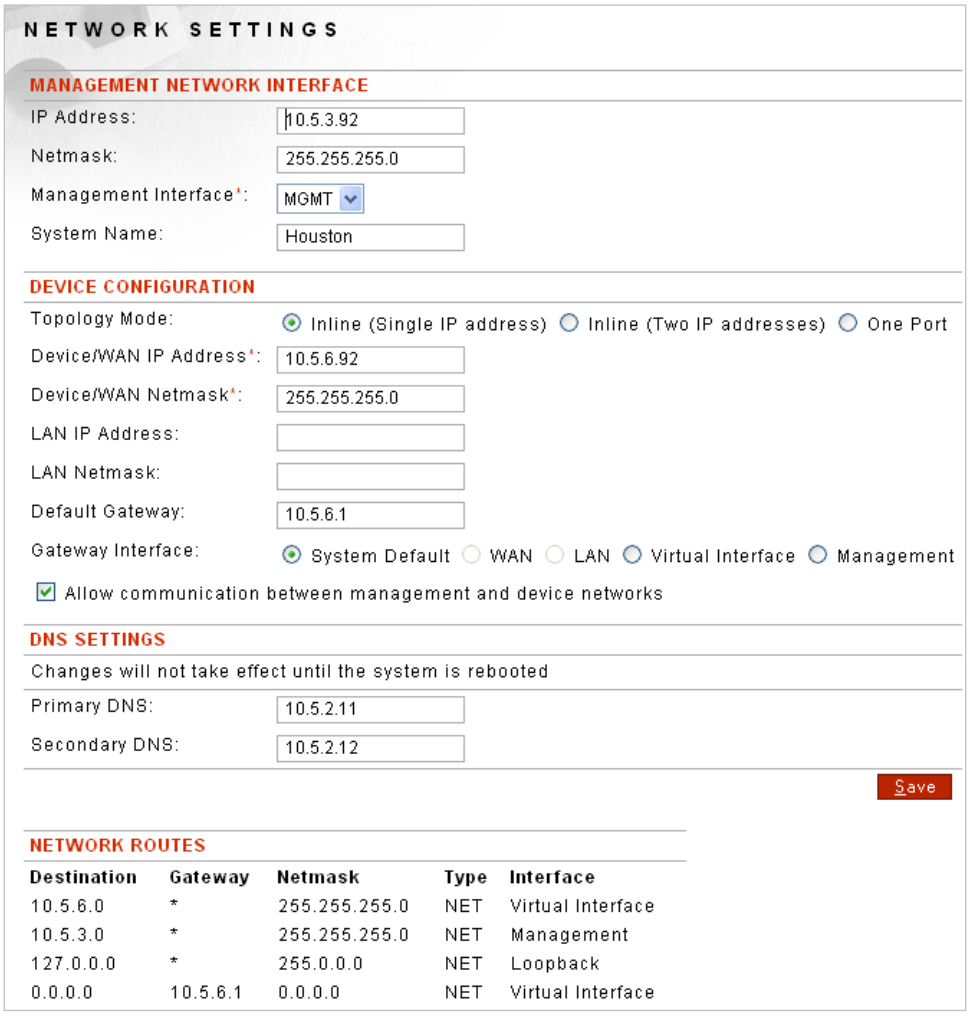


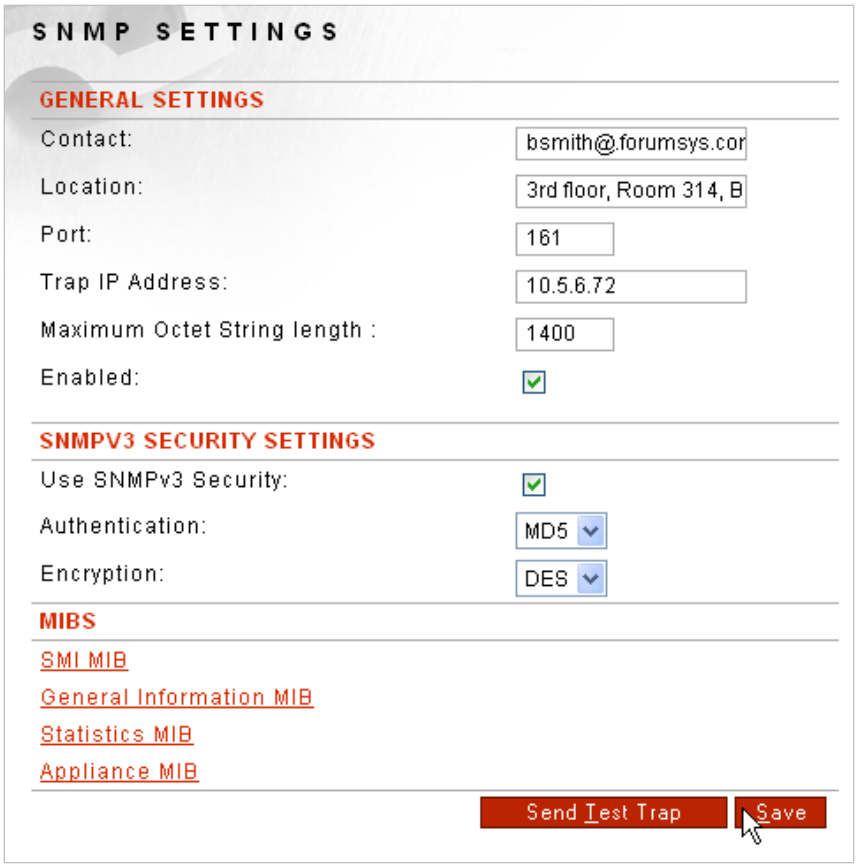
- Associate these users with the SNMPMonitor Group from the Groups screen.



Note: For more information on creating Users and Groups, refer to the Users and Groups sections of the *Forum Systems Sentry™ Version 9.1 Access Control Guide*.

- From the Network screen, enter the System name and Save.





- From the Navigator, select the **SNMP** screen.
- On the SNMP SETTINGS screen, fill in appropriate **values**, select the **Enabled** checkbox and then click **Save**.

Note: View SNMP security configuration settings from the CLI in enable mode by using the show snmp command. For more information, refer to the Network section of the *Forum Systems Sentry™ Version 9.1 System Management Guide*.

The refreshed screen now included a Send Test Trap button.

- Select **Sent Test Trap**. The screen refreshes with the "Test trap sent." message visible at the top of the screen.

STATISTICS

The Statistics screen displays a variety of system and system data for document processing, and mimics the output from the show statistics command on the CLI. Reset the statistics data without rebooting by selecting the **Reset** button at the bottom of the screen. Monitoring the Statistics screen provides a quick and easy way to determine if traffic is being processed through the system.

Statistics Screen Terms

The following table displays a definition for each statistic displayed on the screen:

DESCRIPTION	DEFINITION
Average document size in bytes *****	The average document size for all processed documents since the system was last initialized.
Smallest document size in bytes *****	The minimum document size for all processed documents since the system was last initialized.
Largest document size in bytes *****	The document size is the length of the document after it has been read from the network and decoded. For FTP, the document size is updated after a pgp encryption, decryption, signature or verification.
Documents processed successfully	The count of all documents processed without any errors since the system was last initialized.
Documents processed with errors	The count of documents encountering processing errors since the system was last initialized. A processed document is an xml document to which a task list has been applied. For FTP, the counter is incremented after a successful pgp encryption, decryption, signature or verification.
Megabytes processed	The count of bytes for all documents processed since the system was last initialized.
Documents proxied	The count of documents proxied since the system was last initialized. FTP does not use this statistic.
Errors encountered	The count of all errors encountered while processing documents since the system was last initialized. Ftp does not use this statistic.
Elements successfully encrypted ******	The count of document elements that were successfully encrypted since the system was last initialized.
Reset	When clicked, resets Statistics data without rebooting the appliance, setting the data back to zero.

DESCRIPTION	DEFINITION
Elements failing encryption **	The count of document elements that failed encryption since the system was last initialized.
Successful content encryptions **	The count of content encryptions that were successful since the system was last initialized.
Failed content encryptions **	The count of content encryptions that failed since the system was last initialized.
Elements successfully decrypted **	The count of document elements that were successfully decrypted since the system was last initialized.
Elements failing decryption **	The count of document elements that failed decryption since the system was last initialized.
Signatures successfully created **	The count of all signatures passing creation while processing documents since the system was last initialized.
Signatures failing creation **	The count of all signatures failing creation while processing documents since the system was last initialized.
Signatures successfully verified **	The count of all signatures passing verification since the system was last initialized.
Signatures failing verification **	The count of all signatures failing verification since the system was last initialized.
Document transformations **	The count of successful document transformations since the system was last initialized.
Megabytes transformed **	The count of bytes involved in successful document transformations since the system was last initialized. The bytes of the document after the transformation are used not the ones from he incoming document.
Documents successfully validated **	The count of documents successfully validated since the system was last initialized.
Documents failing validation **	The count of documents failing validation since the system was last initialized.
Documents successfully archived **	The count of documents successfully archived since the system was last initialized.
Documents failing archival **	The count of documents failing an archive operation since the system was last initialized.

DESCRIPTION	DEFINITION
Megabytes archived **	The count of bytes for all documents successfully archived since the system was last initialized. The number of megabytes archived includes the size of the document if chosen to be archived and the length of each element being archived.
Documents virus scanned	The count of documents scanned for viruses since the system was last initialized.
Documents failing virus scan	The count of documents in which a virus was detected since the system was last initialized.

* When processing attachments only the document to be processed within the attachment counts as the document size.

****** Statistics for security operations apply to every successful operation generated by a task. Every xml element selected on the task to operate on the document counts.

Note: Statistics counters are reset to 0 whenever the system is rebooted or the user selects **Reset** from the Statistics screen. Counters reflect values for the current running session of the system. Statistics counters apply to XML and OpenPGP processing.

JMX REMOTE

Java Management Extensions (JMX) technology provides a modular way to expose management and monitoring functionality in server applications and distributed components. When coupled with the JMX Remote API, JMX provides another broadly accepted option for monitoring the health of the product.

All of our statistics have been centralized and represented as JMX artifacts, and they can be viewed either via SNMP using the SNMP screen or using JMX. The JMX Remote API allows third-party monitoring systems to connect to a system and view the JMX statistics. Support and settings for the JMX Remote API are collected in the JMX Remote screen.

The protocol for JMX Remote is RMI/JRMP (pronounced RMI over JRMP) - this is one of the mandatory protocols that must be supported for the JMX Remote API to be used. The default port number for RMI is 1099, but users can choose any other valid and available port to connect. In the special case of a software port running on Linux, if the software is not running as user root, then only port numbers of 1024 and above are allowed.

Users have the option to use a clear text connection or SSL using Forum Systems SSL policies to specify whether X.509 authentication is used. Users may also use basic username/password authentication and/or a combination of both.

Note: Forum Systems strongly recommends that SSL with mutual authentication is used for any administrative interaction with the software.

JMX Remote works in a similar fashion as SNMP in that appliance statistics are only available on an appliance platform; not on a software port.

JMX Remote Screen Terms

When viewing the JMX Remote screen, the following information is presented:

Field Name	Definition
GENERAL SETTINGS	
Port	The Port number of the JMX remote server.
Enabled	When checked, the JMX remote server is enabled. When unchecked, the JMX remote server is not enabled.
SECURITY SETTINGS	
Basic Authentication	When checked, the JMX remote server is authenticated through Basic Auth. When unchecked, Basic Auth is not required to authenticate the JMX remote server, but SSL authentication will still be used if enabled.
Use SSL	When checked, an SSL handshake negotiates the connection from the JMX remote server to the system. When unchecked, there is no SSL handshake.
SSL Termination Policy	The name of the SSL Termination policy applied during the SSL handshake.
JMX CONNECTION URL	
JMX Connection URL	The JMX Connection URL is the connection string that the monitoring application can use to connect to the JMX Remote API that is exposed in the product. It is there displayed for convenience.

Overview of JMX

JMX manages three separate layers (instrumentation, agent, and distributed services) for application management. Users working on the WebAdmin need only focus on the following layers.

The Instrumentation Layer

The instrumentation layer exposes the application by using introspection to create metadata received from the Agent layer. The JMX agent invokes attributes and other operational methods defined in the interface. The Instrumentation layer links the managed resource (your application) and the rest of the JMX framework.

The Agent Layer

The agent layer provides services, such as dynamic loading and monitoring.

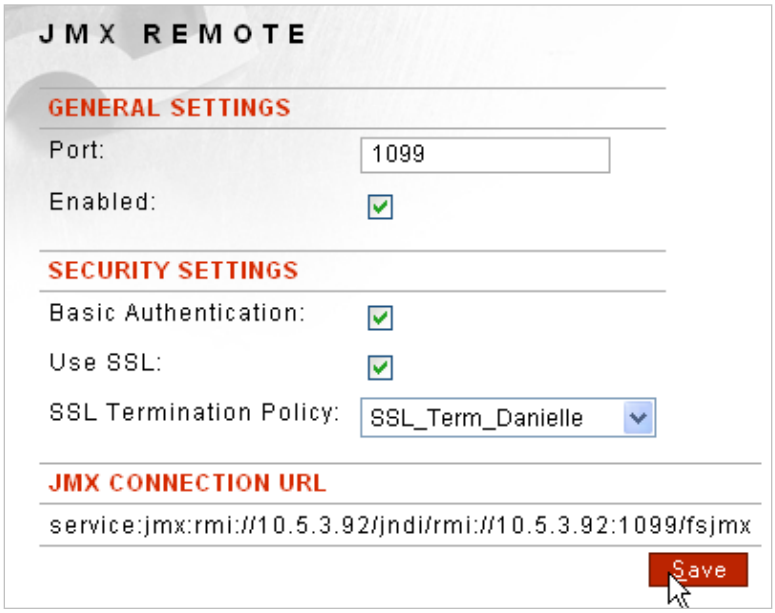
JMX Remote Configuration Example

The example for configuring JMX Remote includes:

- Configure JMX Remote Policy.

Configure JMX Remote

Follow these steps to configure a JMX Remote Server to the system:



- From the Navigator, select the **JMX Remote** screen.
- On the JMX REMOTE screen, retain the default port number of 1099.
- Check the **Enabled** checkbox to enable the JMX Remote Server.
- To use Basic Auth for authenticating the JMX remote server to the system, check the **Basic Authentication** checkbox.
- To use an SSL handshake for connections, check the **Use SSL** checkbox.
- Apply an SSL Termination policy by selecting an **SSL Termination policy** from the drop down list.
- Click **Save**.

CENTRAL LOGGING TO FORUM SENTRY CONTROL CENTER

If you have an instance of Forum Sentry Control Center running in your environment, you can choose to configure centralized logging and monitoring to the Forum Sentry Control Center instance. This feature provides system monitoring metrics including CPU utilization, Memory Utilization, Policy Health metrics for Policy transactions, Latency metrics for policies, and centralized consolidated logging.

To configure a Forum Sentry instance to send monitoring and logging information to a central Forum Sentry Control Center machine, go to the Diagnostics->Config screen.

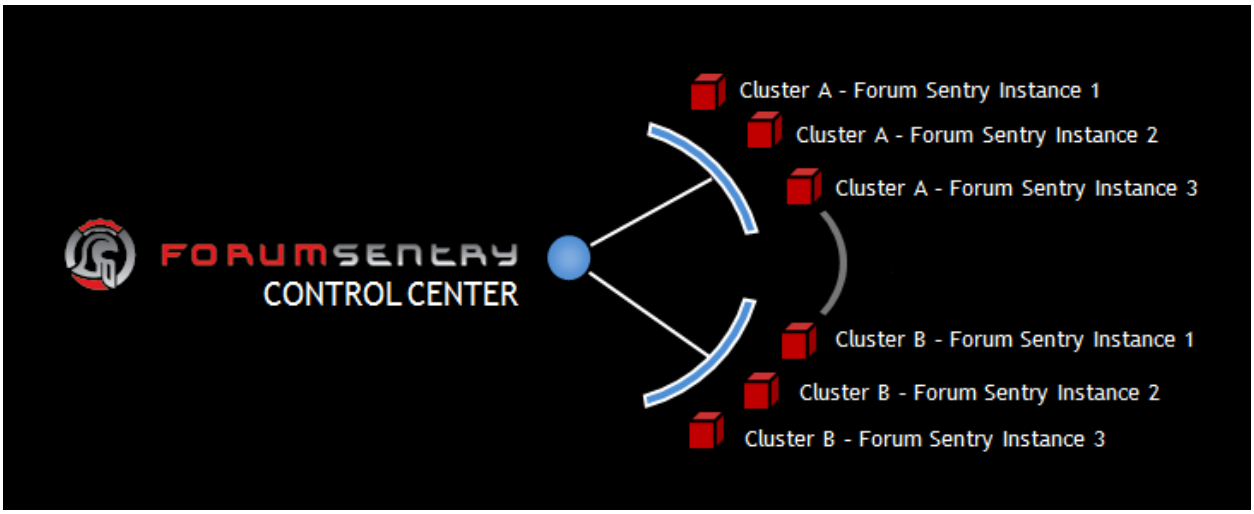
Diagnostics Config Screen Terms

When viewing the Config screen for Central diagnostics, the following information is presented:

Field Name	Definition
Mode	Configure the mode of this instance as to whether to send centralized monitoring statistics to a Forum Sentry Control Center machine. If running Forum Sentry XML Gateway, this setting will appear as: **Send Metrics** **Disabled** If running Forum Sentry Control Center, this setting will appear as: **Gather Metrics** **Disabled**
Remote/Listener Policy	If running on a Forum Sentry XML Gateway, this setting will be the Remote Policy to use to send metrics to the Forum Sentry Control Center If running on Forum Sentry Control Center, this setting will show the listener policy settings for inbound connections and metrics.

PERFORMANCE MONITORING VIA FORUM SENTRY CONTROL CENTER

The Forum Sentry Control Center provides 3 levels of drill-down performance monitoring enabling comprehensive visibility of all Sentry instances running in the environment. To view the Performance Monitor, go to Diagnostics->Performance Monitor.



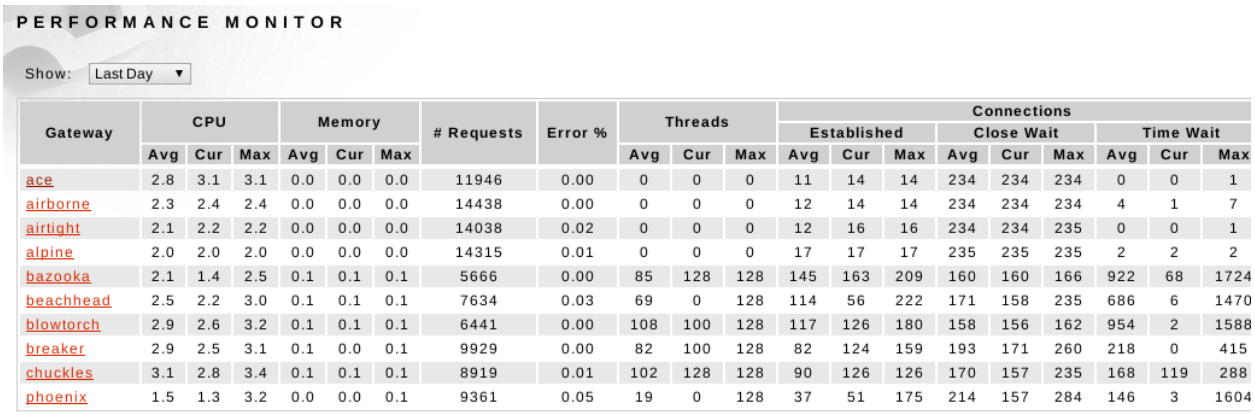
Setup Requirements for Enabling Centralized Logging and Reporting

The Forum Sentry Command Center uses a database to store central logs and monitoring statistics. This database must first be installed and populated with the schema. The database types supported are listed under the Diagnostics->Logging->Data Sources tab and each relevant set of SQL schema for creating the database schema is also provided on that screen.

Once the database has been properly configured, go to the Data Sources policy screen and create a new data source that points to the database. Then go to the Diagnostics->Config screen and choose the data source policy just created and configure the listener settings for how Sentry instances will communicate metrics to the central Command Center.

Performance Monitoring Per System

The Performance Monitoring screen shows metrics for each gateway that is publishing to the Forum Sentry Command Center.



PERFORMANCE MONITOR

Show: Last Day

Gateway	CPU			Memory			# Requests	Error %	Threads			Connections								
												Established			Close Wait			Time Wait		
	Avg	Cur	Max	Avg	Cur	Max			Avg	Cur	Max	Avg	Cur	Max	Avg	Cur	Max	Avg	Cur	Max
ace	2.8	3.1	3.1	0.0	0.0	0.0	11946	0.00	0	0	0	11	14	14	234	234	234	0	0	1
airborne	2.3	2.4	2.4	0.0	0.0	0.0	14438	0.00	0	0	0	12	14	14	234	234	234	4	1	7
airtight	2.1	2.2	2.2	0.0	0.0	0.0	14038	0.02	0	0	0	12	16	16	234	234	235	0	0	1
alpine	2.0	2.0	2.0	0.0	0.0	0.0	14315	0.01	0	0	0	17	17	17	235	235	235	2	2	2
bazooka	2.1	1.4	2.5	0.1	0.1	0.1	5666	0.00	85	128	128	145	163	209	160	160	166	922	68	1724
beachhead	2.5	2.2	3.0	0.1	0.1	0.1	7634	0.03	69	0	128	114	56	222	171	158	235	686	6	1470
blowtorch	2.9	2.6	3.2	0.1	0.1	0.1	6441	0.00	108	100	128	117	126	180	158	156	162	954	2	1588
breaker	2.9	2.5	3.1	0.1	0.0	0.1	9929	0.00	82	100	128	82	124	159	193	171	260	218	0	415
chuckles	3.1	2.8	3.4	0.1	0.1	0.1	8919	0.01	102	128	128	90	126	126	170	157	235	168	119	288
phoenix	1.5	1.3	3.2	0.0	0.0	0.1	9361	0.05	19	0	128	37	51	175	214	157	284	146	3	1604

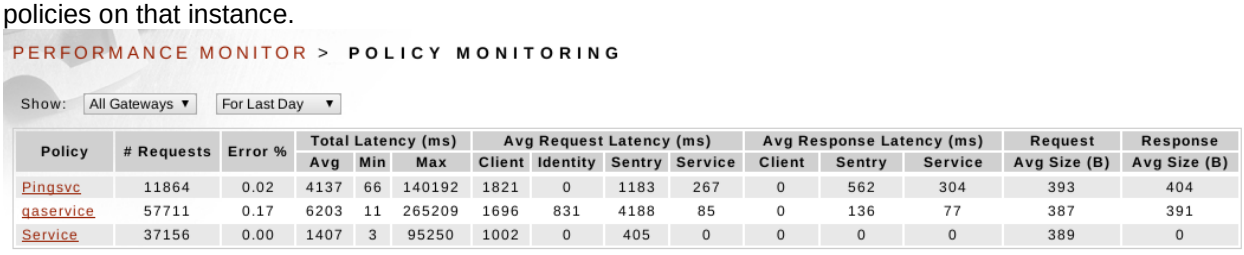
Performance Monitor Screen Terms

When viewing the Performance Monitor screen for Central diagnostics, the following information is presented:

Field Name	Definition
Show	Duration of time to aggregate results being shown.
Gateway	Name of the Gateway reporting metrics
CPU	Average, Current, and Maximum values of the CPU utilization from the machine, averaged over 1 minute.
Memory	Average, Current, and Maximum values of the memory utilization from the machine
#Requests	# of total requests for the Gateway machine in the time scope allocated
Error%	% of errors this policy has seen on the connection and HTTP error code levels
Threads	Average, Current, and Maximum value of allocated worker threads on the machine
Established Connections	Average, Current, and Maximum number of Established connections on the machine
Close Wait Connections	Average, Current, and Maximum number of connections currently in the CLOSE_WAIT state.
Time Wait Connections	Average, Current, and Maximum number of connections currently in the TIME_WAIT state.

Policy Monitoring

When you drill down from the top level gateway, the subsequent screen breaks down the metrics from policies on that instance.



PERFORMANCE MONITOR > POLICY MONITORING

Show: All Gateways For Last Day

Policy	# Requests	Error %	Total Latency (ms)			Avg Request Latency (ms)				Avg Response Latency (ms)			Request	Response
			Avg	Min	Max	Client	Identity	Sentry	Service	Client	Sentry	Service	Avg Size (B)	Avg Size (B)
Pingsvc	11864	0.02	4137	66	140192	1821	0	1183	267	0	562	304	393	404
qaservice	57711	0.17	6203	11	265209	1696	831	4188	85	0	136	77	387	391
Service	37156	0.00	1407	3	95250	1002	0	405	0	0	0	0	389	0

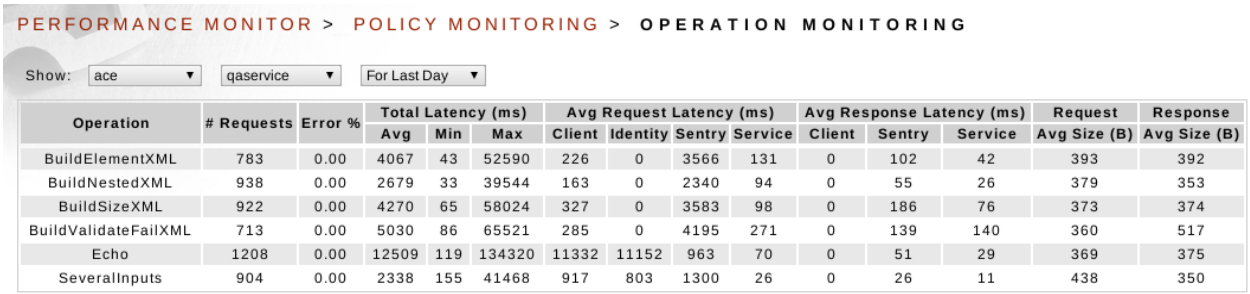
Policy Monitor Screen Terms

When viewing the Performance Monitor screen for Central diagnostics, the following information is presented:

Field Name	Definition
Show	Choose to show all gateways or a specific gateway over the time interval specified
Policy	The name of the gateway policy
# Requests	The number of request that have been made to this policy within the selected time interval
Error %	Number of requests that resulted in a network or HTTP error response
Total Latency	The total latency of transactions to this policy displayed as the average, minimum, and maximum latency values for this time interval
Ave Request Latency	The components of the latency metric for the request portion of the transaction. • **Client:** the time the client takes to write the data over the network to sentry • **Identity:** the time it takes to communicate to an identity system to authorize the transaction • **Sentry:** the time it takes Sentry to process the message • **Service:** the time it takes to write the post-processed request to the back-end server
Ave Response Latency	The components of the latency metric for the request portion of the transaction. • **Client:** the time it takes Sentry to write the processed response back to the client • **Sentry:** the time it takes Sentry to process the response message • **Service:** the time it takes to receive and read the response from the back-end system
Request Avg Size	Average size of the requests to this policy over the specified time interval
Response Avg Size	Average size of the responses for this policy over the specified time interval

Operation Monitoring

When you drill down from the Policy Monitoring screen you can view the operation monitoring for WSDL based services.



Operation	# Requests	Error %	Total Latency (ms)			Avg Request Latency (ms)				Avg Response Latency (ms)			Request	Response
			Avg	Min	Max	Client	Identity	Sentry	Service	Client	Sentry	Service	Avg Size (B)	Avg Size (B)
BuildElementXML	783	0.00	4067	43	52590	226	0	3566	131	0	102	42	393	392
BuildNestedXML	938	0.00	2679	33	39544	163	0	2340	94	0	55	26	379	353
BuildSizeXML	922	0.00	4270	65	58024	327	0	3583	98	0	186	76	373	374
BuildValidateFailXML	713	0.00	5030	86	65521	285	0	4195	271	0	139	140	360	517
Echo	1208	0.00	12509	119	134320	11332	11152	963	70	0	51	29	369	375
SeveralInputs	904	0.00	2338	155	41468	917	803	1300	26	0	26	11	438	350

Operation Monitoring Screen Terms

When viewing the Operation Monitoring screen for Central diagnostics, the following information is presented:

Field Name	Definition

Show	Choose to show all gateways or a specific gateway over the time interval specified
Operation	Names of the operations defined in the selected WSDL policy
# Requests	The number of request that have been made to this policy within the selected time interval
Error %	Number of requests that resulted in a network or HTTP error response
Total Latency	The total latency of transactions to this policy displayed as the average, minimum, and maximum latency values for this time interval
Ave Request Latency	The components of the latency metric for the request portion of the transaction. • **Client:** the time the client takes to write the data over the network to sentry • **Identity:** the time it takes to communicate to an identity system to authorize the transaction • **Sentry:** the time it takes Sentry to process the message • **Service:** the time it takes to write the post-processed request to the back-end server
Ave Response Latency	The components of the latency metric for the request portion of the transaction. • **Client:** the time it takes Sentry to write the processed response back to the client • **Sentry:** the time it takes Sentry to process the response message • **Service:** the time it takes to receive and read the response from the back-end system
Request Avg Size	Average size of the requests to this policy over the specified time interval
Response Avg Size	Average size of the responses for this policy over the specified time interval
Show	Choose to show all gateways or a specific gateway over the time interval specified
Policy	The name of the gateway policy
# Requests	The number of request that have been made to this policy within the selected time interval
Error %	Number of requests that resulted in a network or HTTP error response
Total Latency	The total latency of transactions to this policy displayed as the average, minimum, and maximum latency values for this time interval

APPENDIX

Appendix A - Constraints in Monitoring and Reporting Guide

ELEMENT	CONSTRAINTS	CHAR COUNT
WS Report Name	Unique & case sensitive. Accepts the '@' character, underscores and dashes.	1-80
User Password for users assigned to the SNMPMonitor Group	Must be created in cleartext. Unique & case sensitive. Accepts the '@' character, underscores and dashes. Additionally, the Enable for use with basic auth checkbox must be checked.	8-255

Appendix B - Specifications in Monitoring and Reporting Guide

ELEMENT	SPECIFICATIONS
SNMP Octet String length	Default maximum Octet String length is 1400.

Appendix C - Database Dictionary for Reporting Tables

The following tables list common database terms, definitions and conventions used in the Reporting database.

TABLE NAME	FIELD NAME	DATA TYPE	DESCRIPTION
REPORTMETA			Reporting meta data
	ID	NUMBER(16)	Record Key (sequence)
	SERVERPOLICY	VARCHAR2(80)	Name of Network listener policy associated with the WSDL Policy
	WSDLPROJECT	VARCHAR2(80)	Name of WSDL Policy
	WSDLSERVICE	VARCHAR2(80)	Service name from the WSDL file
	WSDLPORT	VARCHAR2(80)	Port binding name from WSDL
	WSDLOPERATION	VARCHAR2(80)	Name of Operation from WSDL file
	REQUESTTAGNAME	VARVCHAR2(80)	Name of Operation input parameter from WSDL
	RESPONSETAGNAME	VARCHAR2(80)	Name of Operation output parameter from WSDL

TABLE NAME	FIELD NAME	DATA TYPE	DESCRIPTION
REPORTDOC			Reporting XML documents
	AUTOID	NUMBER(16)	Primary Key
	REQUEST	BLOB	XML request document
	RESPONSE	BLOB	XML response document

TABLE NAME	FIELD NAME	DATA TYPE	DESCRIPTION
REPORTSTATS			Reporting statistics
	AUTOID	NUMBER(16)	Primary Key (sequence)
	ID	NUMBER(16)	Record Key (sequence)
	REQUESTTIME	NUMBER(32)	Device System time in milliseconds since 1/1/1970
	SOURCEIP	VARCHAR2(16)	Source IP address of client
	SOURCEPORT	NUMBER(16)	Source Port number of client
	SOURCEUSER	VARCHAR(32)	Name of Authenticated client
	REQUESTLENGTH	NUMBER(16)	Request length in Bytes
	RESPONSESTATUS	NUMBER(8)	HTTP code
	RESPONSELENGTH	NUMBER(16)	Response length in Bytes
	RESPONSEPROCTIME	NUMBER(16)	Number of milliseconds for the response to process

INDEX