

Note Limiting the number of appliances for which the Log Viewer is enabled will increase the overall performance of your SonicWALL ViewPoint system.

Summarizer

This section contains the following subsections:

- "About Summary Data in Reports" on page 73
- "Summarizer Settings and Summarization Interval" on page 73
- "Configuring the Syslog Deletion Schedule Settings" on page 78
- "Configuring Host Name Resolution" on page 79

About Summary Data in Reports

These reports are constructed from the most current available summary data. In order to create summary data, the ViewPoint Reporting Module must parse the raw data files.

When configuring ViewPoint Reporting using the screens on the Console panel under Reports, you can select the amount of summary information to store. These settings affect the database size, be sure there is adequate disk space to accommodate the settings you choose.

Additionally, you can select the number of days that raw syslog data is stored. The raw data is made up of information for every connection. Depending on the amount of traffic, this can quickly consume an enormous amount of space in the database. ViewPoint creates a new 2 GB database for raw syslog data everyday. Be very careful when selecting how much raw information to store. For information on configuring raw data storage, see "Enabling Report Table Sorting" section on page 72.

Summarizer Settings and Summarization Interval

SonicWALL appliances send their syslog packets to SonicWALL ViewPoint via UDP packets. When summarization is enabled, the Summarizer will process those files and store the data in the summary databases at the interval you specify.

See the following sections:

- “Enabling Report Summarization” section on page 74
- “Setting the Reports Data Summarization Interval” section on page 74
- “Using Summarize Now” section on page 76

Enabling Report Summarization

To globally enable the summarization of report data, which is necessary for viewing reports, perform the following:

1. On the **Console** panel, navigate to **Reports > Summarizer.**
2. Under **Summarizer Settings**, select the **Enable Report Summarization** checkbox.
3. Click **Update.**

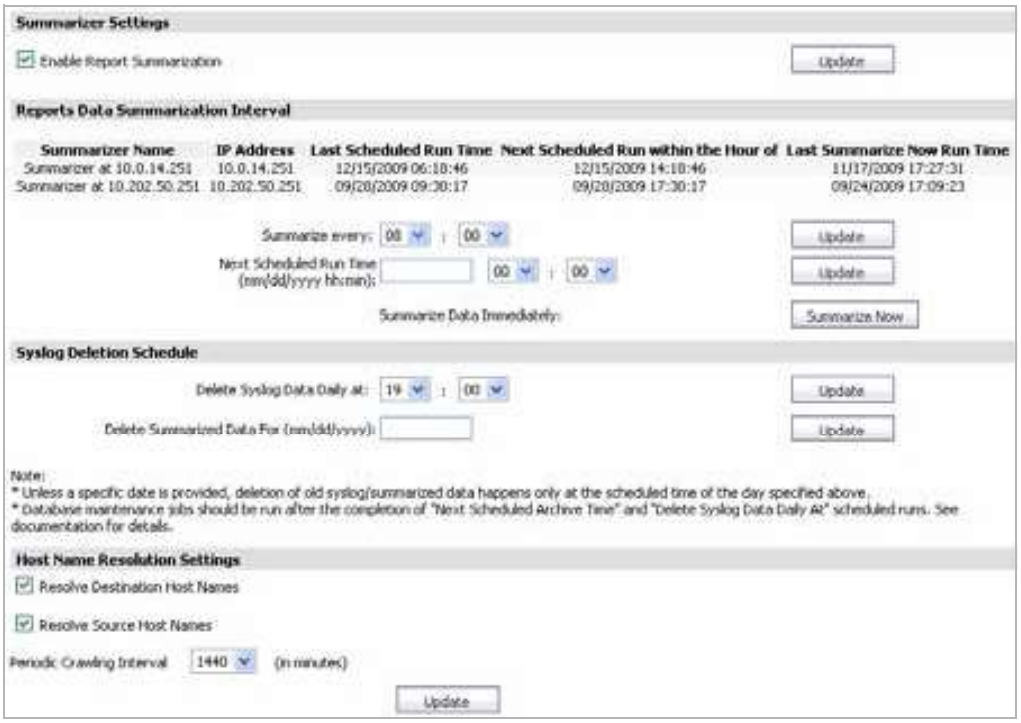
Setting the Reports Data Summarization Interval

The Summarizer will process syslog data sent from SonicWALL appliances and store the processed data in the summary databases at the interval you specify. When an appliance is configured to communicate with ViewPoint, you need to verify that the summarizer is scheduled to collect and process data for this unit at an appropriate interval.

To configure reports for summarization, see the “Selecting Reports for Summarization” section on page 137 in the Scheduling and Configuring Reports chapter.

To configure the summarization interval, perform the following steps:

1. Click the **Console** tab, expand the **Reports** tree and click **Summarizer.** The Summarizer page displays.



2. Under Reports Data Summarization Interval, important information about the Summarizer is displayed. Use the **Summarize every** drop-down lists to specify how often in hours and minutes the ViewPoint Reporting Module should process syslog data and update summary information.
3. Click the **Update** button to the right of this field.
4. To specify the next summarization time, enter a date in the form mm/dd/yyyy in the **Next Scheduled Run Time** field, and select the hour and minute values from the drop-down lists.
5. Click the **Update** button to the right of this field.
6. To update the summary information now, click the **Summarize Now** button. SonicWALL ViewPoint will automatically process the latest information and make it available for immediate viewing.

Note This will not affect the normally scheduled summarization updates on ViewPoint.

For more information about using and verifying the Summarize Now option, see the "Using Summarize Now" section on page 76.

Using Summarize Now

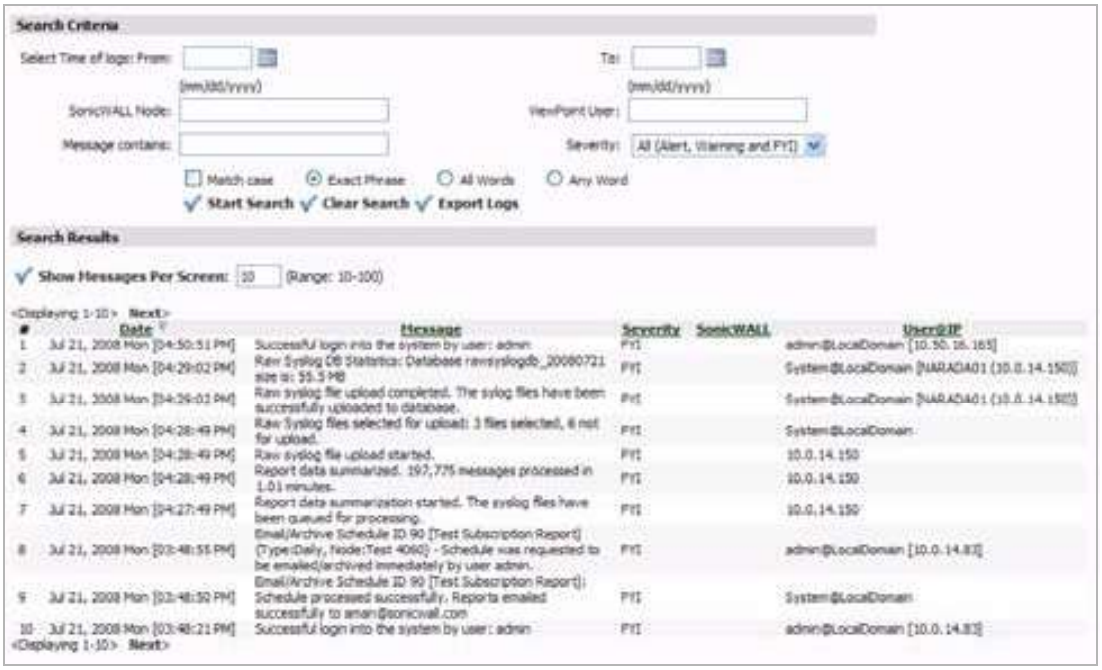
The Summarize Now feature allows the administrator to create instant summary reports without affecting the regularly scheduled summary reports. You can use Summarize Now to test that the Summarizer is gathering data for a managed unit. The SonicWALL ViewPoint Summarize Now feature is located in the **Console** tab under **Reports > Summarizer**. The SonicWALL ViewPoint Summarizer creates summary reports by default every 8 hours. Summary reports can be configured by the administrator to occur every 15 minutes to every 24 hours.

To use the Summarize Now feature, perform the following tasks:

1. Click the **Console** tab, expand the **Reports** tree and click **Summarizer.** Click the **Summarize Now** button.
2. You will see a pop-up window verifying that you want to summarize the data now. Summarizing data using **Summarize Now** is a one-time action and will not affect the scheduled summary. Click **OK** to continue.



3. To verify summarization, navigate to **Log > View Log** in the left pane. Search for the message **Report Data Summarized** to verify that the Summarize Now action has completed.



4. When Summarize Now has completed, click the **UTM** tab at the top of the screen. In the left-most pane, click **MyReportsView** or click an appliance.

Note You may see incomplete data if you view the **Summary** section of a selected report before the **Summarize Now** process is complete. Wait for the **Report Data Summarized** message to be displayed in **Log > View Log**.

5. In the center pane, click a report to expand it, then click the **Summary** option underneath it. For example, click **Bandwidth**, then click **Summary** to review the summarized bandwidth usage data.



	Hour	Connections	Cost (USD)	MBytes	% of MBytes
1	00:00 - 01:00	6031	1.903	3.807	3.6%
2	01:00 - 02:00	6067	1.914	3.828	3.6%
3	02:00 - 03:00	5920	1.877	3.753	3.6%
4	03:00 - 04:00	5977	2.103	4.205	4.0%
5	04:00 - 05:00	5994	1.915	3.831	3.6%
6	05:00 - 06:00	6079	1.925	3.85	3.6%

6. Navigate to the Summary section of other reports in the center pane to see other summarized data.

Configuring the Syslog Deletion Schedule Settings

Syslog files sent from SonicWALL appliances are stored on the ViewPoint system, and are consolidated into the syslog database. The Summarizer processes the syslog data and stores the processed data in the summary database. After summarization and after the configured period of syslog storage, the syslog data can be periodically deleted from the system. This is necessary as the syslog files and database can consume a lot of space on the file system.

This section of the the Summarizer page also provides a way to delete summarized data for a certain date. For example, if summarized data is kept for a long time, such as 90 days, then you could use this option to remove some summarized data from a particular date within the 90 day period if the stored data was becoming too large.



Tip Run your database maintenance jobs soon after the completion of the scheduled tasks configured on this page for summarizing data and deleting old syslog data.

For information about setting the number of days to store syslog files, the syslog database, and the summary database, see the "Configuring Data Storage Settings" section on page 139.

ViewPoint requires large amounts of disk space for raw data storage. In previous versions, the maximum raw syslog database size was 2 GB. ViewPoint now provides enhanced database capacity by creating a new 2 GB database everyday. Each file name includes the date it was created for easy reference. Raw syslog data is used to create Custom Reports for UTM and SSL-VPN appliances.

To configure the syslog and summarized data deletion settings, perform the following:

1. On the **Console** panel, navigate to **Reports > Summarizer.**
2. Under **Syslog Deletion Schedule**, select the time for daily deletion in the hour and minute **Delete Syslog Data Daily at** drop-down lists. Syslog data will be deleted at this time only after being stored for the number of days configured.
3. Click the **Update** button to the right of this field.
4. To delete summarized data from a specific date, enter a date in the form mm/dd/yyyy in the **Delete Summarized Data For** field.
5. Click the **Update** button to the right of this field.

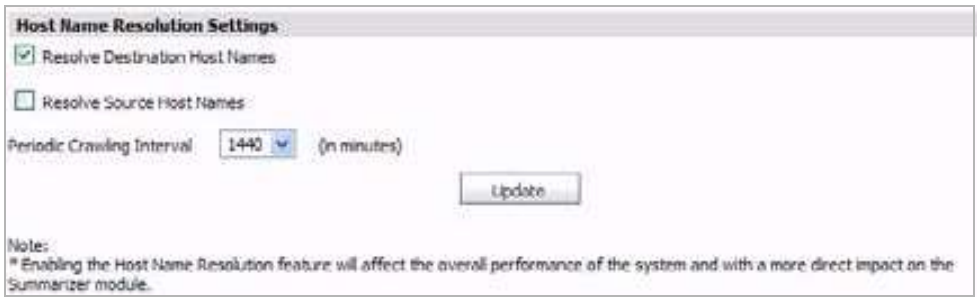
Configuring Host Name Resolution

The Host Name Resolution feature allows the administrator to enable and configure the time period for the name resolution crawler. The name resolution crawler periodically resolves host names for IP addresses found in reporting data. Once the host name is resolved, the name will appear in place of the IP address in reports that contain it. Over time, more host names will appear in the report data as they are added to the list.

The name resolution crawler runs by default every 24 hours (1440 minutes) and can be configured to run every 1 to every 60 hours.

To use the Host Name Resolution feature, perform the following steps:

1. On the **Console** panel, navigate to **Reports > Summarizer**. The Host Name Resolution Settings section is displayed at the bottom of the page.

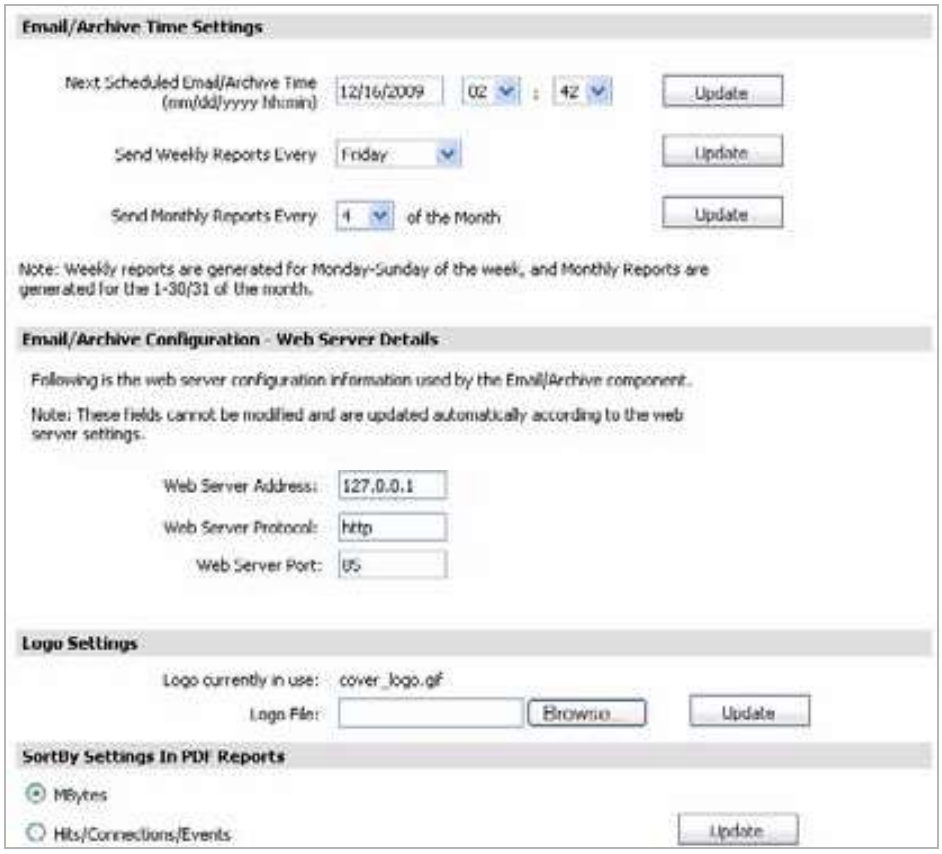


2. To resolve host names for destination IP addresses, select the **Resolve Destination Host Names** checkbox.
3. To resolve host names for source IP addresses, select the **Resolve Source Host Names** checkbox.
4. To set the interval at which the name resolution crawler runs, select the number of minutes in the **Periodic Crawling Interval** drop-down list.

   Performance may be affected while the name resolution crawler is running, especially for the Summarizer module.

Email/Archive

The Console > Reports > Email/Archive page provides global options for setting the time and interval for emailing/archiving scheduled reports, and global settings for the Web server, logo, and PDF sorting options.



Configuring Email/Archive Settings

To configure Email/Archive and Web server settings, perform the following steps:

1. Click the **Console** tab, expand the **Reports** tree and click **Email/Archive.** The Email/Archive page displays.
2. To set the next archive time, enter the date and time in the **Next Scheduled Email/Archive Time** fields and click **Update.**
3. To specify the day to send weekly reports, select the day from the **Send Weekly Reports Every** list box and click **Update.**

4. To specify the date to send monthly reports, select the date from the **Send Monthly Reports Every** list box and click **Update.**
5. If the Web server address, port, or protocol has changed since SonicWALL ViewPoint was installed, the new values will automatically appear in the **Email/Archive Configuration** section. These settings can be modified on the System Interface, and cannot be modified here.
6. Under Logo Settings, you can select a logo to be used on reports. By default, the SonicWALL logo is used. To select another logo, click **Browse** next to the **Logo File** field or type the path and filename into the field, and then click **Update.**
7. Under SortBy Settings for PDF Reports, select one of the following as the sorting criteria for reports and then click **Update.**
   - **Mbytes** - Sort reports by the number of megabytes in each entry
   - **Hits/Connections/Events** - Sort reports by the number of hits, connections, or events, depending on the type of report

Scheduled Reports

The Scheduled Reports page allows you to manage all the report schedules in the system from a central location. This page lists all the schedules in the system, enabling you to monitor the status of these recurring schedules and re-send failed schedules, if needed. For information on adding a new scheduled report, see “Adding or Editing a Scheduled Report” section on page 135.

Under Search Results, the table indicates whether each schedule is enabled, along with information about the last execution time of a schedule, whether it ran successfully and the error that occurred if it failed, the last run type (scheduled or one time run), along with the node, owner and other relevant information.

The Summary section provides status information on your report schedules.

The Search Criteria section provides settings for searching report schedules. Results of your searches are displayed in the Search Results section.

To search for scheduled reports:

1. Click the **Console** tab, expand the **Reports** tree and click **Scheduled Reports**. The **Scheduled Reports** page displays.



2. Define the **Search Criteria** tab. The Search Criteria tab contains the following elements to refine your search:
   - **Schedule Type** - Select from the following schedule types:
     - All Schedules
     - Daily Schedules
     - Weekly Schedules
     - Monthly Schedules
   - **Status** - Select from the following status conditions:
     - All

  - –Failed
  - –In Progress
  - –Success
  - –In Queue
  - –Partial Failure
- **SonicWALL Node** - Select from the following SonicWALL nodes:
  - –All
  - –Per Unit View
- **Owner** - Displays the owner (admin).
- **Name Contains** - Enter a context string to search by keywords.
- **Error Contains** - Enter a context string to search by keywords.
- **Use Condition** - Select from the following conditions:
  - –And
  - –Or
- **Match Case** - Select this checkbox to make your searches case sensitive.

3. Click **Start Search** to begin searching, or click **Clear Search** to reset all fields and start over.

The results of your search are displayed in a table in the Search Results section. You can adjust the number of schedules displayed, go directly to a row of the table, or navigate to other screens by clicking on links within the table.

To work with the search results:

1. To adjust the number of schedules displayed in the table, enter a number of rows to display in the **Show Schedules Per Screen** field, and then click on the checkmark.
2. To go directly to a row of the table, enter the row number in the **Go To Schedule Number** field, and then click on the checkmark.
3. The columns in the table are as follows:
   - The check box allows you select the schedule for emailing or archiving.
   - The notepad icon is a link to the Schedule Properties page.

- **ID** - The schedule ID number used to identify this schedule. You can click on the column heading to sort by this field. An arrow is displayed in the column heading when this field is the basis for sorting, and indicates ascending or descending order.
- **Enabled** - A green check mark indicates that this schedule is enabled, and a red X means that it is disabled.
- **Name** - The name of the report. Click on the highlighted report name link to access the report for editing. You can click on the column heading to sort by this field. An arrow is displayed in the column heading when this field is the basis for sorting, and indicates ascending or descending order.
- **Type** - All, Daily Schedules, Weekly Schedules, and Monthly Schedules.
- **Unit/Group/Devices(s)** - The host name of the SonicWALL appliance.
- **Last Run (Local)** - The date when the report was last generated. You can click on the column heading to sort by this field. An arrow is displayed in the column heading when this field is the basis for sorting, and indicates ascending or descending order.
- **Status** - Includes the following report status options:
  - **Blue**: Queued, waiting to be processed.
  - **Yellow**: Currently processing.
  - **Orange**: Report completed with errors.
  - **Red**: Report failed with errors.
  - **Green**: Report processed successfully.

  You can click on the column heading to sort by this field. An arrow is displayed in the column heading when this field is the basis for sorting, and indicates ascending or descending order.
- **Last Run Type -** Indicates if the most recent run was a scheduled run or a one-time execution. You can click on the column heading to sort by this field. An arrow is displayed in the column heading when this field is the basis for sorting, and indicates ascending or descending order.
- **Last Error** - Displays the error condition from the most recent run, if any. You can click on the column heading to sort by this field. An arrow is displayed in the column heading when this field is the basis for sorting, and indicates ascending or descending order.

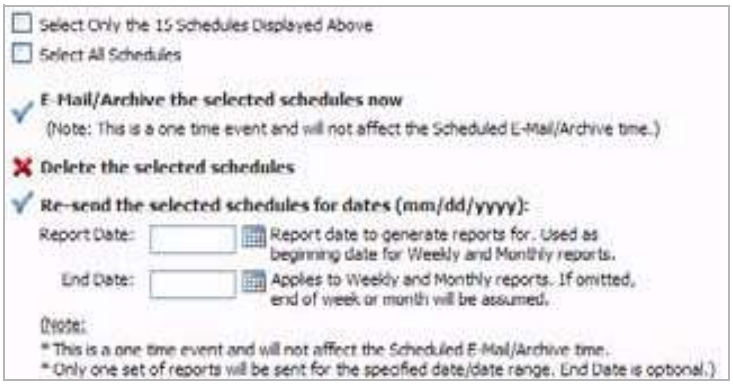
- **Owner** - Indicates the user ID of the user who created the schedule. You can click on the column heading to sort by this field. An arrow is displayed in the column heading when this field is the basis for sorting, and indicates ascending or descending order.

4. To view the properties for a schedule, click the notepad icon in that row. The Schedule Properties page displays.

5. To view the report, click on the name of the report. Your screen will change to the report screen on the UTM or SSL-VPN panel.

Resending Schedules

Apart from selecting multiple schedules for a one-time execution by selecting the appropriate checkboxes and clicking the **Email/Archive the Selected Schedules now**, you can re-send required schedules using the **Re-send the selected schedules for dates** option.



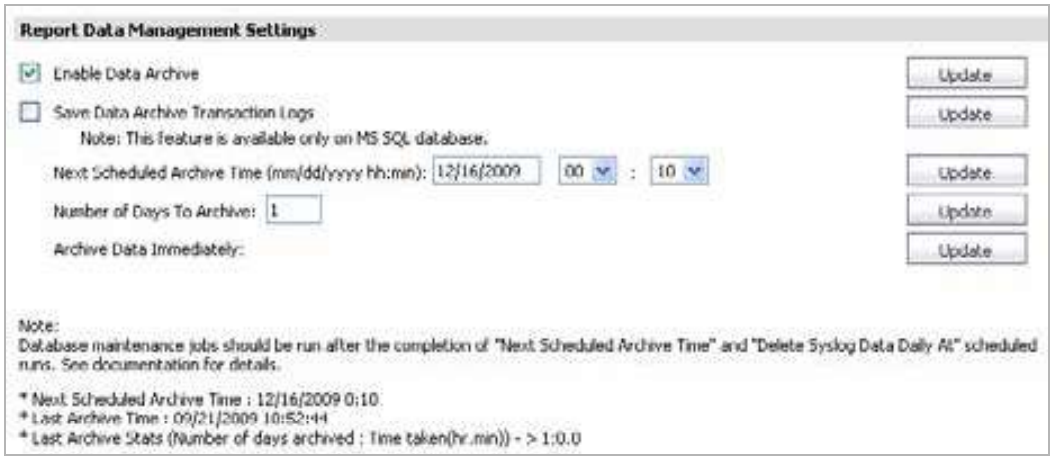
To resend any schedules, follow the procedures below:

1. Select the Schedule Type (Daily, Weekly, or Monthly) from the Search Criteria section and click **Start Search**. This lists all the schedules of the selected type. Select the checkboxes of the schedules you want to resend.
2. Provide a start date (and an end date if applicable). Reports are generated for the specified date/date range.
3. Click **Re-send the selected schedules for dates**. Reports are generated for the specific dates and emailed/archived as a one time option for all the schedules selected.

Management

Report Data Management allows the SonicWALL ViewPoint administrator to backup large amounts of report data incrementally and at specified intervals using MDTA. Typically, the total amount of data stored in an archive is equal to at least 30 days, although best benefits are seen when storing at least 60 days of summarizer data. MDTA allows this archive to be built over time, archiving as little as 1 day of data each time the MDTA process is run.

Note Total days to store summarized data in reports is set separately in the **Console > Reports > Summarizer** screen. Set this field for a value greater than 60 days for best results.



Configuring Report Data Management

As an administrator, you choose the number of days worth of data to archive each time the MDTA process is run. With the exception of the current month, all available data is eligible for archiving. For example, if you specify 3 days as the number of days to archive, MDTA will archive 3 days of data, starting with the oldest available data and will repeat this process every day. In order to obtain optimal performance when viewing reports however, SonicWALL ViewPoint ensures that the current month is always kept in un-archived form.

Step 1 In the ViewPoint Administrator Interface, navigate to **Console > Reports > Management.**

Step 2 Check the box next to **Enable Data Archive** and click the corresponding **Update** button.

Step 3 Configure Data Archiving as follows, clicking the corresponding **Update** button after each line is completed:

Save Data Archive Transaction Logs	Select to save truncated data archive transaction logs during each MDTA operation. Click the **Update** button. This option is deselected by default in order to conserve disk space.
Next Scheduled Archive Time	Schedule an initial date (mm/dd/yyyy) and time (in 24-hour format) for the MDTA operation. Click the **Update** button. MDTA operations will take place every day at the time you specify, starting with your initial date selection.
Number of Days to Archive	Specify the number of days worth of data to consider for each MDTA operation.
Archive Data Immediately	Press this button to immediately start an on-demand MDTA operation. The archive will run immediately but your scheduled archive operation will still take place.



Note High-traffic systems can generate reports that consume large amounts of memory, disk space and CPU time when using MDTA. Set your **Number of Days to Archive** and **Scheduled Archive Time** accordingly. To view when MDTA operations are starting and how long the process is taking, navigate to the **Console > Log > View Log** screen and look (or search) for or “start” and “completed” times for “Report Data Archive.”

CHAPTER 9
Using Diagnostics

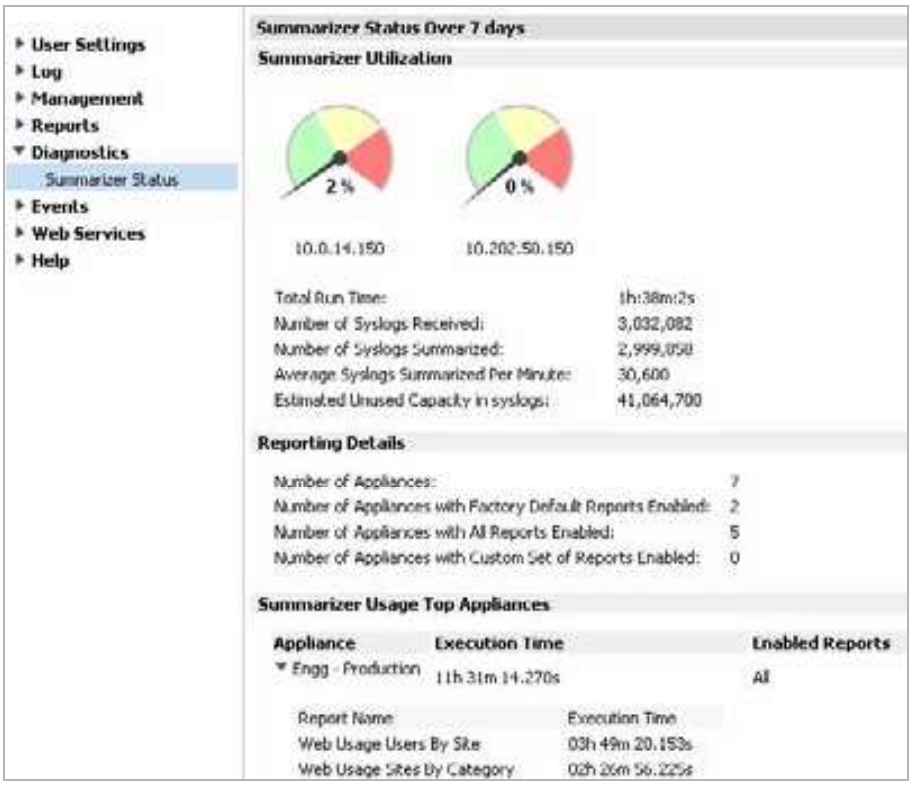
This chapter describes the diagnostic information that ViewPoint provides, including summarizer status information.

This chapter includes the following sections:

- “Summarizer Status” section on page 90

Summarizer Status

The **Summarizer Status** page displays overall summarizer utilization information for the deployment including database and syslog file statistics, and details on the current status of each summarizer.



The Summarizer Status screen provides performance metrics for your network administrator to plan, design, and expand your ViewPoint server deployment. This feature has information on the Syslog Collector and Summarizer metrics. The Summarizer metrics are available only for ViewPoint deployments that have Distributed Summarizer enabled (enabled by default on ViewPoint 5.1). The metrics are available for the past 24 hours, past seven days, and past 30 days.

These metrics are reset (to zero), every 24 hours for daily metrics, every seven days for weekly metrics, and every 30 days for monthly metrics. Weekly metrics are not shown unless the data collection for weekly metrics started earlier than the daily metrics. Similarly, monthly metrics are not shown unless data collection for monthly metrics started earlier than for daily and weekly metrics. ViewPoint will not display metrics for a component if the daily statistics collection started more than 26 hours earlier. This generally indicates that the component is not active.

You can receive alert emails when Summarizer Status shows any abnormalities.

To reach the Summarizer Status screen, navigate to the **Console** panel of ViewPoint and then to **Diagnostics > Summarizer Status.**

The Summarizer Status page is divided into a section showing the overall deployment-wide summarizer status and sections with details for each summarizer. See the following sections:

- Summarizer Status Over 7 Days, page 91
- Details for Summarizer at <IP Address>, page 93

Summarizer Status Over 7 Days

The Summarizer Status Over 7 Days section displays overall summarizer utilization information for the deployment including database and syslog file statistics. Results are calculated over the last 7 days, with historical data available over the last 30 days.

Summarizer Utilization

The top Summarizer Utilization section shows the average utilization of the summarizer over the applicable time period. The Dial Charts show the percent of total capacity used by the Syslog Collector or the Summarizer. The following metrics are also displayed in the Summarizer Utilization section:

Total Run Time: Total amount of time spent generating summarization statistical data and results over the applicable time period.

Number of Syslogs Received: Total number of syslogs received by the Summarizer over the applicable time period.



Note Not all syslogs are summarized – some syslogs, such as “heartbeat messages” are ignored. When **Web Event Consolidation/Home Port Reporting** is enabled, several syslogs may be ignored or alternatively, consolidated into a single syslog. If your appliance is managed by a different Agent, the results are not summarized here.

Number of Syslogs Summarized: Total number of syslogs summarized over the applicable time period.

Average Syslogs Summarizer per Minute: Average number of syslogs summarized per minute over the applicable time period.

Estimated Unused Capacity in Syslogs: The estimated remaining capacity of the summarizer in terms of the number of syslogs it can summarize, based on the time taken and number of syslogs summarized over the applicable time period. This number does not include the discarded syslogs.



Tip Usage Example: For this example, let's assume that the syslogs summarized per minute on a system is **18,108**, and the average number of syslogs received on that system is **91** per firewall, per minute. Divide the number of syslogs per minute (18,108) by the number of syslogs per appliance per minute (91). This yields an estimate of **198** security appliances, assuming that the current appliances are a fair sample of the security appliances on your network.
This simple math gives a reasonable estimate of the total number of security appliances this system should be able to handle, assuming that the Summarizer was to constantly summarize 24 hours (as in the case of a dedicated Summarizer).

Reporting Details

The Reporting Details section shows the number of appliances in the deployment, and the number with the following types of reports enabled:

- Factory default reports
- All reports
- Custom set of reports

Summarizer Usage Top Appliances

The Summarizer Usage Top Appliances section displays information about the appliances in the deployment that used the most summarizer time. Details are given about which reports were generated and their summarizer execution time.

Database Statistics

The size is displayed for each of the following databases:

- Current
- Archive
- Raw Syslog

Syslog File Storage Statistics

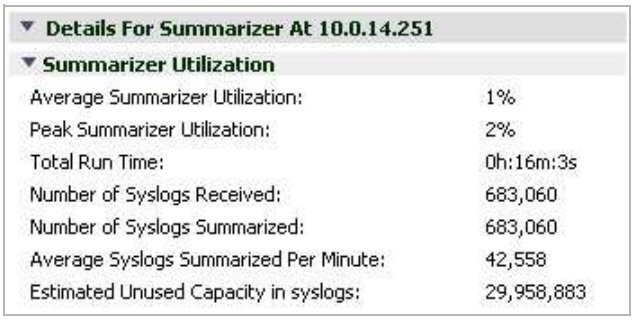
The size is displayed for each of the following syslog directories:

- Current
- Archived
- Bad

Details for Summarizer at <IP Address>

Summarizer Utilization

The Summarizer Utilization section for a specific summarizer shows the same information described above for the entire deployment, but only shows the values for this summarizer.



Reporting Details

The Reporting Details section shows the number of appliances serviced by this summarizer, and the number with the following types of reports enabled:

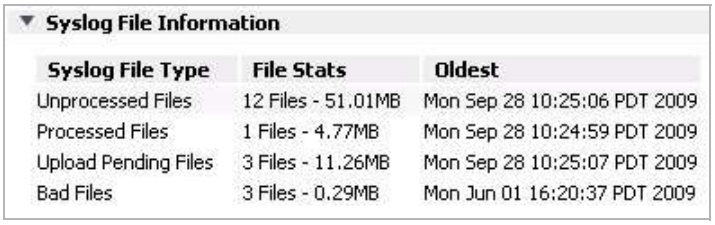
- Factory default reports
- All reports
- Custom set of reports

Summarizer Usage Top Appliances

The Summarizer Usage Top Appliances section displays information about the appliances serviced by this summarizer that used the most summarizer time. Details are given about which reports were generated and their summarizer execution time.

Syslog File Information

This section displays syslog file details for the selected summarizer.



The Syslog File Information table is divided into three columns:

- **Syslog File Type**: The type of files being reported on.

  There are ten main syslog file types:

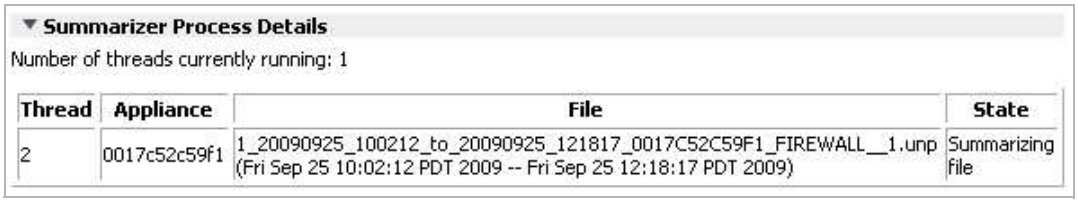
  – Processed Files
  – Unprocessed Files
  – Grouped Files
  – Not Mine Files
  – Infected Files
  – Archived Files
  – Bad Files
  – Upload Pending Files
  – Uploaded Files
  – Bad Upload Files

- **File Stats**: The number of syslog files in the category and their size in Megabytes.
- **Oldest**: The date and time on the oldest file in the category.

Summarizer Process Details

The Summarizer Process Details section shows what tasks the summarizer is performing at the moment the **Console > Diagnostics > Summarizer Status** page displays. Refresh your browser display or leave the page and return to it to update the information.

If the summarizer is currently running, the page displays the thread, appliance identifier, file being used, and state of the summarizer.



If the summarizer is currently idle, the page displays the last run time and next run time.



Keysight, EX-1030
Page 261

Keysight, EX-1030
Page 262

CHAPTER 10
Granular Event Management

This chapter describes how to configure and use the Granular Event Management (GEM) feature in a ViewPoint environment.

This chapter contains the following sections:

- "Granular Event Management Overview" section on page 97
- "Using Granular Event Management" section on page 99
- "Configuring Granular Event Management" section on page 101
- "Viewing Current Alerts" section on page 108

Granular Event Management Overview

Granular Event Management (GEM) provides a customized and controlled manner in which events are managed and alerts are customized and enabled. On the Console panel, GEM allows you to systematically configure each sub-component of your alert in order for the alert to best accommodate your needs.

The GEM alert has multiple sub-components, some of which have further subcomponents. It is not necessary to configure all sub-components prior to creating an alert.

- **Severities**: Severity is used to tag an alert as Critical, Warning, or Information. Severities are included within each Threshold. You can change the severity levels of the threshold elements listed on the Console > Events > Threshold page.

- **Thresholds**: A threshold defines the condition that must be matched to trigger an event and send an alert. Each threshold is associated with a Severity to tag the generated alert as critical, warning, or information.

  One or more threshold elements are defined within a threshold. Each threshold includes the following elements: an Operator, a Value, and a Severity. When a value is received for an alert type, the GEM framework examines threshold elements to find a match for the specified condition. If a match is found (one or more conditions match), the threshold with the highest severity containing a matching element is used to trigger an event.
- **Schedules**: You can use Schedules to specify the day(s) and time (intervals) in which to generate an alert. You can also invert a schedule, which means that the schedule is the opposite of the time specified in it. For example:
  - Generate an alert during weekdays only, or weekends only, or only during business hours.
  - Do not generate an alert during a time period when the unit, network, or database are down for maintenance.

What is Granular Event Management?

The purpose of Granular Event Management is to provide all the event handling and alerting functionality for ViewPoint. The ViewPoint management interface provides screens for centralized event management on the Console panel, including screens for Events > Threshold, Schedule, and Alert Settings. The panel also provides an Events > Alert Settings screen where you can enable or disable alerts.

You can enable or disable an alert at the global or unit level in ViewPoint. At the global level, the alert is then applied to all units. Whenever you add a new unit to ViewPoint, the alerts set at the global level are applied to the new unit.

How Does Granular Event Management Work?

The Granular Event Management framework provides customized event handlingfor specific alerts about database and database log size, and security service subscription licenses. For a list of the predefined alerts, see “Using Granular Event Management” on page 99.

Using Granular Event Management

For convenience and usability, a number of default settings are predefined for severities, schedules, thresholds, and alerts. You can edit the predefined values to customize the settings for thresholds and schedules. The predefined defaults for each panel and screen are as follows:

Table 1 GEM Predefined Default Objects

Panel	Screens	Predefined Default Objects
Console	**Events > Thresholds**	Unit Status
		Database Size Status
		Database Log Size Status (on MySQL DB only)
		Summarizer Utilization
		Summarizer Backed-Up Files
Console	**Events > Schedule**	**Schedule Groups:**
		• 24x7
		• Weekdays 24 hours
		• 8x5
		• Weekend
		Schedules:
		• Schedule: admin
		• Monday 24 hours
		• Monday business hours
		• Tuesday 24 hours
		• Tuesday business hours
		• Wednesday 24 hours
		• Wednesday business hours
		• Thursday 24 hours
		• Thursday business hours
		• Friday 24 hours
		• Friday business hours
		• Saturday 24 hours
		• Sunday 24 hours

Panel	Screens	Predefined Default Objects
Console	**Events > Alert Settings**	Database Info
		Database Size Status
		Database Log Size Status (on MySQL DB only)
		Summarizer Utilization Status
		Summarizer Backed-Up Files Status (on MySQL DB only)

About Alerts

The **Events > Alert Settings** screens are available in the Console and UTM panels. You can enable or disable alerts on these screens.

The GEM framework provides different types of alert types for the respective areas of the ViewPoint application:

- UTM panel: Alert settings for Reporting
- Console panel: Alert settings for the ViewPoint application

Table 2 GEM Alert Types

Panel location	Available Alert Types
Console	Date Base Info
	Database Size Status
	Database Log Size Status (on MySQL DB only)
	Summarizer Utilization Status
	Summarizer Backed-Up Files Status (on MySQL DB only)
UTM	Anti Virus License
	CFS License
	Warranty License
	Anti Spyware License
	Intrusion License

Configuring Granular Event Management

To set up the GEM environment after installing ViewPoint, start with the Events screens on the Console panel. You should examine the Threshold and Schedule screens and make any necessary configuration changes. Then you can enable alerts in the Events screens on the Console panel and UTM panel.

See the following sections:

- “Configuring Events on the Console Panel” section on page 101
- “Enabling or Disabling Alerts on the UTM Panel” section on page 107

Configuring Events on the Console Panel

In the Events screens on the Console panel, you can configure the frequency of subscription expiration and task failure notifications, as well as severities, thresholds, schedules, and alerts for handling events.

See the following sections:

- “Configuring Event Thresholds” on page 101
- “Configuring Event Schedules” on page 104
- “Enabling or Disabling Alerts on the Console Panel” on page 107

Configuring Event Thresholds

In the **Events > Threshold** screen, you can view existing event thresholds and configure their elements, and add custom thresholds. A threshold defines the condition for which an event is triggered. Predefined thresholds have names similar to predefined Alert Types. Each threshold can contain one or more threshold elements. An element consists of an Operator, a Value, and a Severity.

The following tasks are described in this section:

- “Editing an Event Threshold Element” on page 102
- “Enabling/Disabling Event Thresholds and Threshold Elements” on page 103

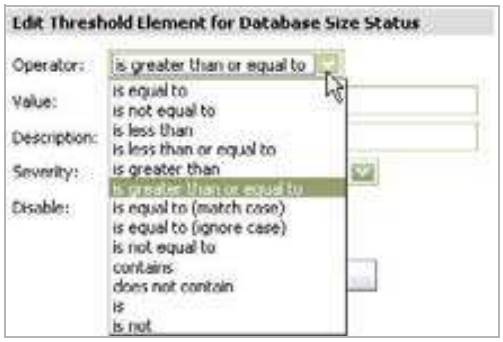
Editing an Event Threshold Element

To edit an existing element of a Threshold, perform the following steps:

1. On the **Events > Threshold** screen, click the **Edit** icon located in the Configure column in the element row.
2. In the Edit Threshold Element window, you can edit the following fields:
   - Operator
   - Value
   - Description
   - Severity
   - Disable

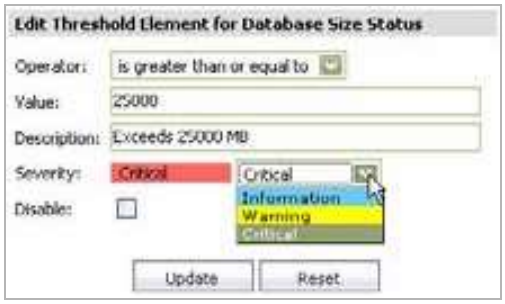


3. In the **Operator** field, select from the drop down menu the type of operator to apply to your threshold element..



4. In the **Value** field, enter the value for your threshold element.
5. In the **Description** field, enter the description for your threshold element.

6. In the **Severity** field, select the severity priority from the drop down menu. These are color coded for your easy reference on the Events > Threshold screen.



7. To disable the threshold element, click the **Disable** check box. See "Enabling/Disabling Event Thresholds and Threshold Elements" section on page 103.
8. Click **Update**.

Enabling/Disabling Event Thresholds and Threshold Elements

The GEM feature provides a **Disable** check box that allows you to disable or enable thresholds or individual elements within that threshold. If it is needed again, you can simply enable it.

You can disable a threshold by disabling all its elements. You can also disable individual elements within a threshold.

To enable or disable Thresholds and/or their elements, perform the following tasks:

1. On the **Console** panel, navigate to the **Events > Threshold** screen. On this screen, you are able to view existing Thresholds. You can also view existing elements within those thresholds by clicking the expand button by a threshold. You have the following two options for the enabling/disabling feature:
   - You can enable or disable a Threshold by disabling/enabling all the elements that exist within it.
   - You can enable/disable the individual elements within a Threshold.
2. To enable or disable a threshold and/or elements, click the edit button  that is on the element level.

3. Select the **Disable** checkbox to disable the element or de-select the **Disable** checkbox to enable the element.



4. Click **Update.**

Configuring Event Schedules

The next component on the Console panel is **Events > Schedule**. In this screen, you can add, delete, or configure schedules and schedule groups.

Schedule groups are one or more schedules grouped within an object. Administrators and Owners can edit these objects. Other users should be able to view or use them only if the **Visible to Non-Administrators** check box is selected.

The following tasks are described in this section:

- "Adding an Event Schedule" on page 104
- "Editing an Event Schedule" on page 106
- "Adding an Event Schedule Group" on page 106
- "Deleting a Schedule or Schedule Group" on page 107

Adding an Event Schedule

In **Events > Schedules** you can add, delete, or configure schedules. You will see your schedules and schedule groups, their descriptions, and whether they are enabled. You can also individually delete one schedule or schedule group at a time by selecting the trash-icon on the right hand side for each row. For quick reference, you can hover your mouse over the descriptions to quickly view the type of schedule and the days and times when it is active.

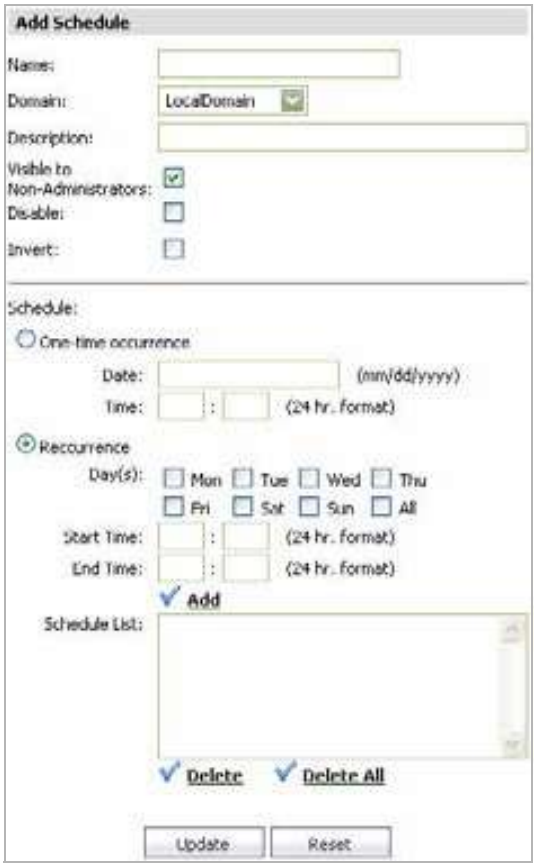
To add an event schedule, perform the following steps:

1. On the **Events > Schedules** screen, click **Add Schedule.**
2. Select the **Visible to Non-Administrators** check box if you want the schedule to be visible and usable by non-administrators.
3. To temporarily disable a schedule, select the **Disable** checkbox.

4. Click **Invert** to create a schedule that is “off” during the dates and times that you specify.
5. In the Schedule field, you can create one or more schedules. For each schedule, configure either:

- **One Time Occurrence**
  - Fill in the **Date** and **Time** fields.
- **Recurrence**
  - Fill in **Days**, **Start Time**, and **End Time** fields.

6. Click **Add** to add this schedule to the **Schedule List** text box.



7. To delete an entry from the Schedule List text box, select the entry that you want to delete, and then click **Delete**. Click **Delete All** to delete all entries.
8. Click **Update** when you are finished.

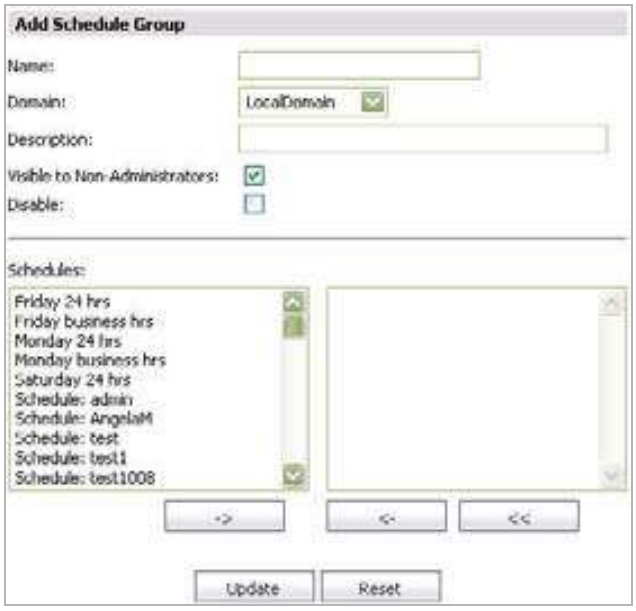
Editing an Event Schedule

To edit an existing schedule, click the **Edit** icon on the right side of the **Events > Schedule** screen. The screen and procedure for editing are the same as those for adding a schedule. See "Adding an Event Schedule" section on page 104.

Adding an Event Schedule Group

You can combine several schedules into a schedule group on the **Events > Schedule** screen. To add a schedule group, perform the following steps:

1. On the **Events > Schedule** screen, click the **Add Schedule Group** button.
2. Enter the name of your schedule group in the **Name** field.
3. Enter a description of your schedule group in the **Description** field.
4. Click the **Visible to Non-Administrators** check box to allow this schedule group to be viewed and used by non administrators.
5. Click the **Disable** check box to temporarily disable the schedule group.
6. In the **Schedules** field, select the schedule(s) to add to your schedule group, and then use the arrow buttons to move the selected schedule into or out of the group. To move multiple schedule groups and/or schedules all at once, hold the CTRL button on your keyboard while making your selections.



7. Click **Update**.

Deleting a Schedule or Schedule Group

You can delete schedules or schedule groups, or you can remove schedules from schedule groups.

To delete an event schedule, schedule group, or remove a schedule from a schedule group:

1. Navigate to the **Events > Schedule** screen.
2. Click the check boxes of the schedule groups or schedules that you want deleted. When you click the schedule group check box, the schedules within that schedule group will be deleted as well.
3. To remove a schedule from a schedule group, click the expand button on the schedule group, and select the schedules you wish to remove within that group.
4. To delete the selected schedule group(s) or remove the selected schedules from a group, click the **Delete Schedule Group(s)/Remove Schedules from Group** button.
5. To delete the selected schedule(s), click the **Delete Schedule(s)** button.

Enabling or Disabling Alerts on the Console Panel

The **Console > Events > Alert Settings** screen provides predefined alerts that apply to ViewPoint as a whole. You can hover your mouse over these to display information about them. You can enable or disable these alerts by selecting or clearing the checkbox in the **Enable** column for the alert.

Enabling or Disabling Alerts on the UTM Panel

You can enable or disable alerts for events pertaining to security services licenses on the UTM panel.To enable or disable an alert:

1. To enable an alert, select the checkbox under **Enabled** in the row for the alert.
2. To disable an alert, clear the checkbox under **Enabled** in the row for the alert.
3. Click **Enable/Disable Alert(s).**

Viewing Current Alerts

You can view a list of current alerts on the **Events > Current Alerts** page of the panel. Select a global view or unit to view current alerts for your selection.



Alert Listing

Severity	Unit Name	Description
Warning	Test 4060	The Intrusion subscription has not been activated for this device

CHAPTER 11
Web Services

This chapter provides information about the Web Services feature. Web Services is a software system designed to support interoperability between ViewPoint and other network appliances, servers, and devices through an application programming interface (API).

Web Services is located in the Console panel of the ViewPoint management interface:



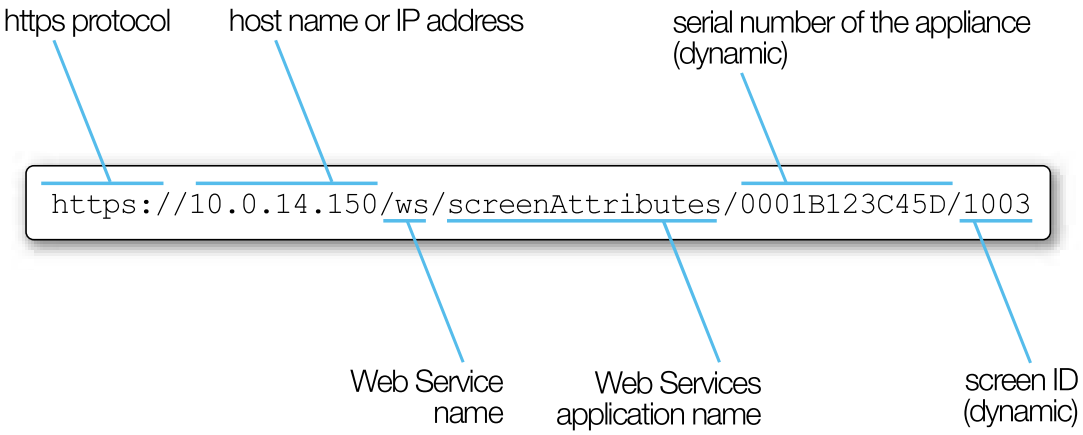
This chapter includes the following sections:

- "URI Basics" section on page 110
- "Settings" section on page 111
- "Status" section on page 112

URI Basics

The URI is a HTTPS string which is used to identify Web Services resources. Each URI is composed of both static and dynamic parts which differ based on each particular deployment.

The following provides a typical, though not comprehensive, URI example:



Note For more information on configuring and using Web Services in your deployment, download the *GMS Web Services Technote* at: <http://www.sonicwall.com/us/support.html>

Settings

The Settings screen allows configuration of a secure HTTPS Public URI for use with Web Services features. The public URI specified here is used to access Web Services and to ensure proper embedded cross-links between Web Services applications.

To configure Web Services Settings:

1. Navigate to the **Web Services > Settings** screen on the Console panel.



2. Choose which deployment you wish to configure from the drop-down list in the **GMS Deployment** section.
3. Enter the public server name and port in the **Public URI** section. This field is typically pre-populated during the ViewPoint install/setup process.
4. Click the **Update** button to save your changes.

Status

The status screen allows the administrator to view, enable, and disable individual Web Services across one or more ViewPoint deployments.

To view and configure Web Services status:

1. Navigate to the **Web Services > Status** screen on the Console panel.



2. Select or deselect the **Enabled** checkbox for the service(s) you wish to enable or disable.
3. Click the **Update** button to save your changes.
4. The Web Services table, in the **Web Services > Status** screen gives the following information about each Web Service:

Feature	Description
Enabled	If selected, this feature is currently enabled
Service	Indicates the name of the Web Service
URI	Indicates the full URI used to access this Web Service
Description	Provides a description of the Web Service

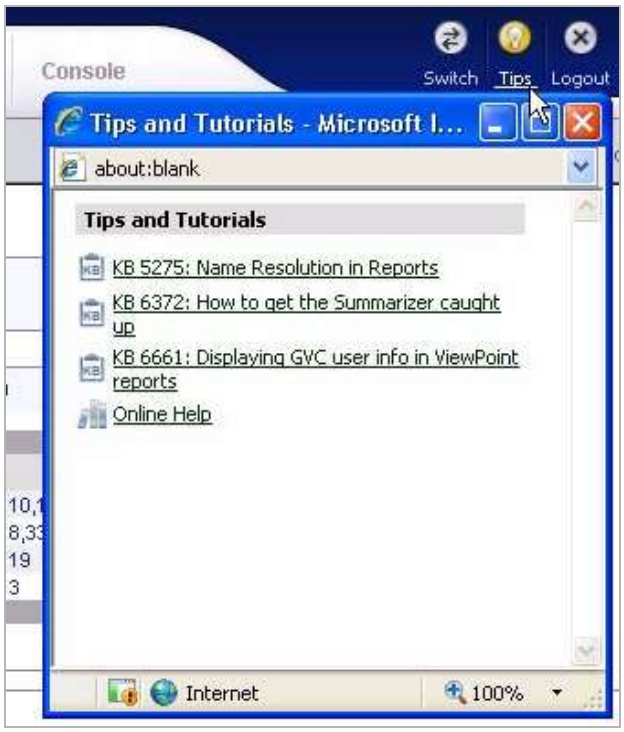
CHAPTER 12
Using ViewPoint Help

To access the ViewPoint online help, click the blue help button 

in the top-right corner of the ViewPoint user interface.

Tips and Tutorials

Tips and tutorials are available in some pages of the user interface, and are denoted by a “Lightbulb” icon:



To access tips and tutorials:

1. Navigate to the page where you need help.
2. If available, click the Lightbulb icon in the upper right-hand corner of the window. Tips, tutorials, and online help are displayed for this topic.

About ViewPoint

The **Console > Help > About** page displays the version of ViewPoint being run, who the ViewPoint is licensed to, database information, and the serial number of the ViewPoint.

To access the ViewPoint online help, click the blue help button 

in the top-right corner of the ViewPoint user interface.

CHAPTER 13
ViewPoint Reporting Features

This chapter describes how to use ViewPoint reporting, including the type of information that can appear in reports. A description of the available features in the user interface is provided. Settings for reporting on the Console panel are described.

This chapter includes the following sections:

- "ViewPoint Reporting Overview" section on page 115
- "Navigating ViewPoint Reporting" section on page 119
- "Showing Domain Names in Reports" section on page 130
- "Managing ViewPoint Reports on the Console Panel" section on page 131

ViewPoint Reporting Overview

Monitoring critical network events and activity, such as security threats, inappropriate Web use, and bandwidth levels, is an essential component of network security. ViewPoint Reporting complements SonicWALL's Internet security offerings by providing detailed and comprehensive reports of network activity.

The ViewPoint Reporting Module is a software application that creates dynamic, Web-based network reports. The ViewPoint Reporting Module generates both real-time and historical reports to offer a complete view of all activity through SonicWALL Internet security appliances. With ViewPoint Reporting, you can monitor network access, enhance security, and anticipate future bandwidth needs.

You can search saved reports by using the report search bar, available in most report screens in the ViewPoint UI. The search bar provides pre-populated quick settings for the search field, and a drop-down calendar for the start and end dates. The search operator field offers a comprehensive list of search operators that varies depending on the search field, which can be either text-based or numeric.

You can search all columns of report data except columns that contain computed values, such as %, Cost, or Browse Time. ViewPoint waits until you click Search before it begins building the new report.

The ViewPoint Reporting Module:

- Displays bandwidth use by IP address and service
- Identifies inappropriate Web use
- Provides detailed reports of attacks
- Collects and aggregates system and network errors
- Shows VPN events and problems
- Tracks Web usage by users and by Web sites visited
- Provides detailed daily firewall logs to analyze specific events.



Note The ViewPoint Reporting Module receives its information from the stream of syslog data sent by each SonicWALL appliance and stores it in the SonicWALL ViewPoint database or as files on the hard-disk.

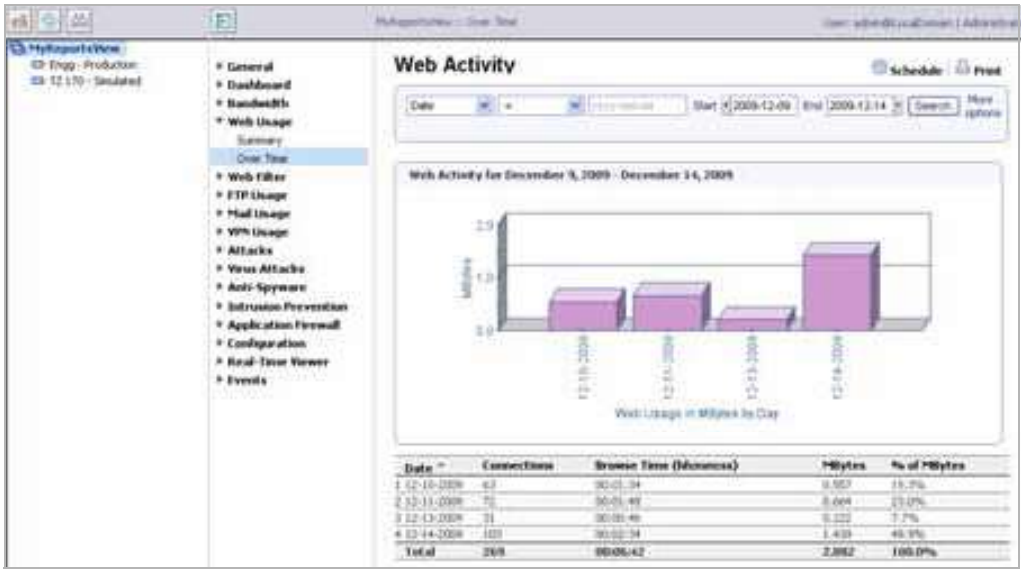
Keysight, EX-1030
Page 282

Viewing ViewPoint Reports

The ViewPoint reports are available on the **UTM** and **SSL-VPN** tabs of the ViewPoint interface:



The ViewPoint Reports view is divided into three panes:



- A list of individual units referred to as the TreeControl: In the left pane, you can select the top level view or a unit to display reports that apply to the selected view or unit. The top level view is **MyReportsView.**
- A list of reports: The middle pane provides a list of available reports that changes according to your selection in the TreeControl pane. The reports are divided into categories. You can click on the plus sign next to a category to view the list of reports in that category. You can click on an individual report name to view that report.

- The report: The right pane displays the report that you selected in the middle pane for the view or unit that you selected in the TreeControl. For most reports, the search bar is provided at the top of the pane. Above the search bar a link to the Scheduler is provided. You can change the time for the report to run by clicking the **Schedule** link or its clock icon in the upper right. A quick access link to your system's printer is also available in the upper right corner. To print the report, click the **Print** link or icon. To access the display settings for the report, click **More Options** to the right of the search bar.

The SonicWALL ViewPoint reporting feature provides the following configurable reports:

Table 3 Configurable Reports

General	Provides general unit and license status.
Dashboard	Provides a high-level activity summary.
Custom Report*	Provides Internet Activity and Website Filtering reports with details from raw data *Custom Reports are only available at the unit level.
Bandwidth	Provides bandwidth usage reports.
Services*	Provides events and usage by service protocol. *Services reporting is only available at the unit level.
Web Usage	Provides Web usage reports.
Web Filter	Provides web filter event reports.
FTP Usage	Provides FTP usage reports.
Mail Usage	Provides mail usage reports.
VPN Usage	Provides VPN usage reports.
Attacks	Provides attack event reports.
Virus Attacks	Provides virus attack event reports.
Anti-Spyware	Provides spyware event reports.
Intrusion Prevention	Provides intrusion event reports.
Application Firewall	Provides Application Firewall reports.
Authentication	Provides login reports.

Navigating ViewPoint Reporting

ViewPoint Reporting is a robust and powerful tool you can use to view detailed reports for individual SonicWALL appliances.

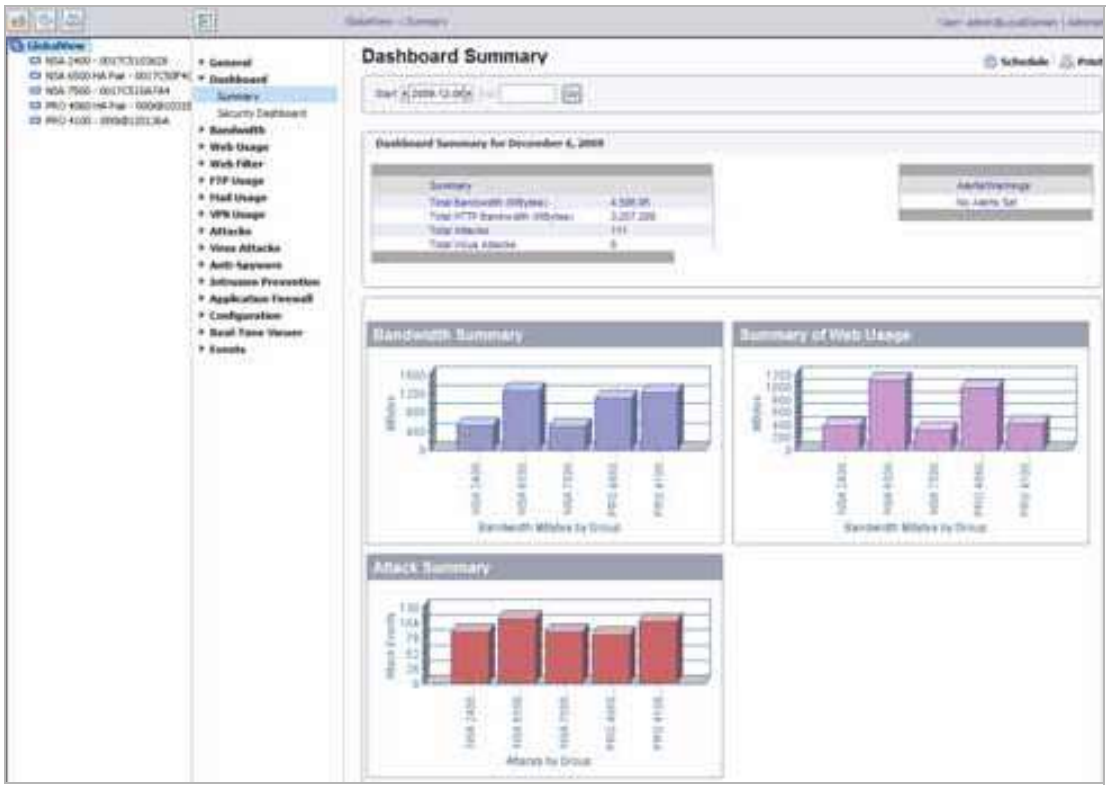
This section describes each view and what to consider when making changes. It also describes the Search Bar and display options for interactive reports, as well as other enhancements provided in SonicWALL ViewPoint . See the following sections:

- "Global Views" on page 120
- "Unit View" on page 121
- "Using Interactive Reports" on page 122
- "Searching for a Report" on page 123
- "Collapsible TreeControl Pane" on page 128
- "Enabling/Disabling Scheduled Reports" on page 128
- "Combined Reports" on page 128
- "Improved Navigation" on page 129

Global Views

From the Global view of the UTM Panel, Summary and Over Time reports are available for all SonicWALL appliances connected to SonicWALL ViewPoint.

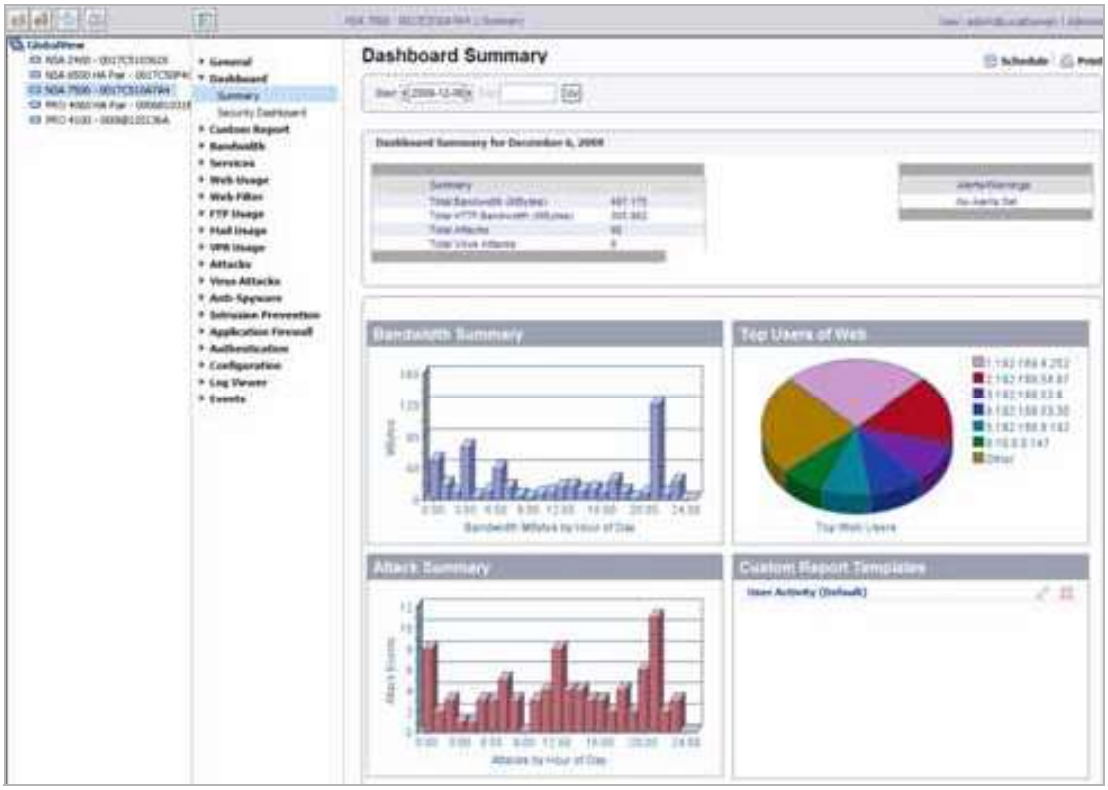
To open the Global view, click the **MyReportsView** icon in the upper-left hand corner of the left pane. .



As you navigate the SonicWALL ViewPoint reports screens with the MyReportsView view selected and view different reports, the settings that you specify are maintained in effect throughout the session.

Unit View

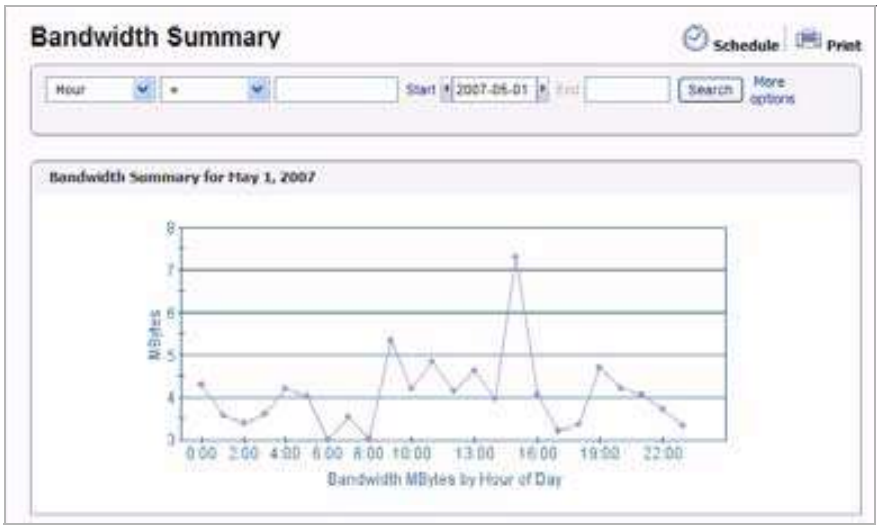
From the Unit view of the UTM panel, reports contain detailed data for the selected SonicWALL appliance. To open the Unit view, click the **UTM** tab. Then, click a SonicWALL appliance in the left pane of the SonicWALL ViewPoint interface. The report page for the SonicWALL appliance displays.

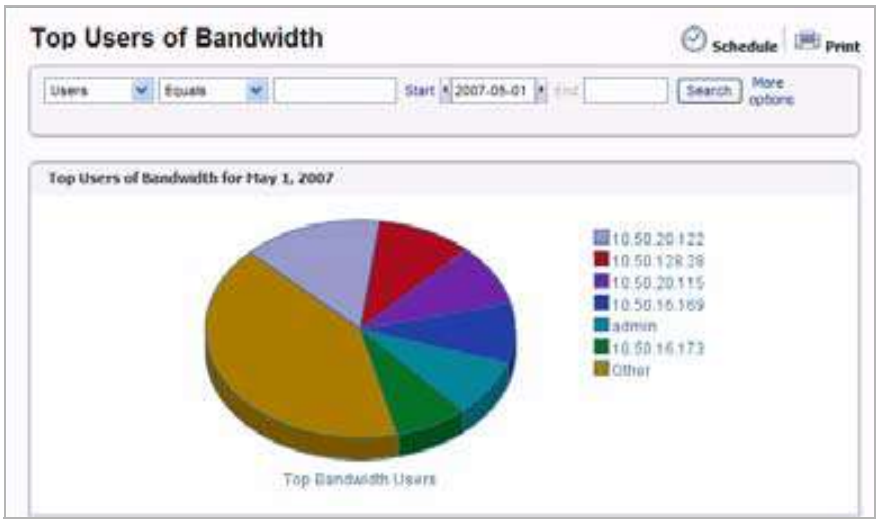


As you navigate the UTM panel with a single SonicWALL appliance selected and change settings, those settings will remain in effect throughout the session.

Using Interactive Reports

ViewPoint provides interactive reporting to create a clear and visually pleasing display of information. The following figures provide examples of an interactive report graph and a pie chart for Summary and Top Users. You can control the way the information is displayed by adjusting the settings which are collapsed in the search bar.





Keysight, EX-1030
Page 288

Searching for a Report

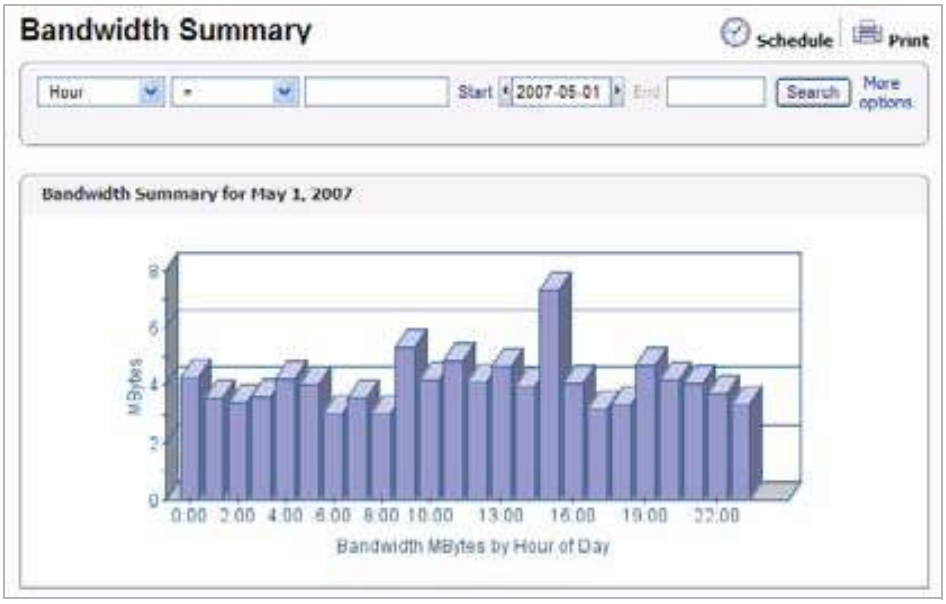
The search bar feature provides search and configuration capabilities for every report. In addition to the original quickset functions, the search bar has intuitive search fields to provide context-based searching.



The search bar contains a number of helpful components that allow you to specify search parameters and locate a report with ease. The components of the search bar include:

- A column drop-down list: The searchable column drop-down list contains all the searchable columns of a report. It is context-based, containing different options in different reports. The column drop-down list defines criteria for the search and filter functions.
- An operator drop-down list: There are two types of operator sets. If the content of the selected column is character-based, a character-based list is displayed. If the column contains numerical data, a list with mathematical symbols is displayed.
- A search text field: You can input a search string into this field.
- Start date and end date calendar fields: You can also search for reports by date. Clicking on the **Start** field displays a drop-down calendar where you can select day, month, and year by using the side arrows to navigate. You may also navigate through dates by clicking on the arrows located beside the **start date** and the **end date** fields.
- Detailed drop-down menu

The collapsed and expanded Search Bar views are shown below:

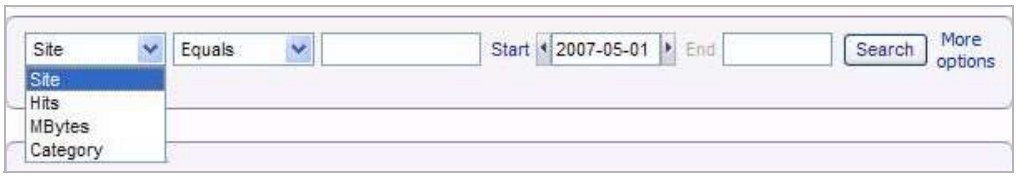




Keysight, EX-1030
Page 290

The search bar feature consists of a column drop-down list, an operator drop-down list, a search text field, and a detailed pull-down menu. Search/Filter functions can be performed by utilizing various components reporting at unit level.

The drop-down list contains all the searchable columns of a report. It is context-based, meaning that it contains different options in different reports. The column drop-down list defines criteria for search and filter functions to work on.



There are two different operator sets. If the content of the selected column is character-based, the character based operators will show:

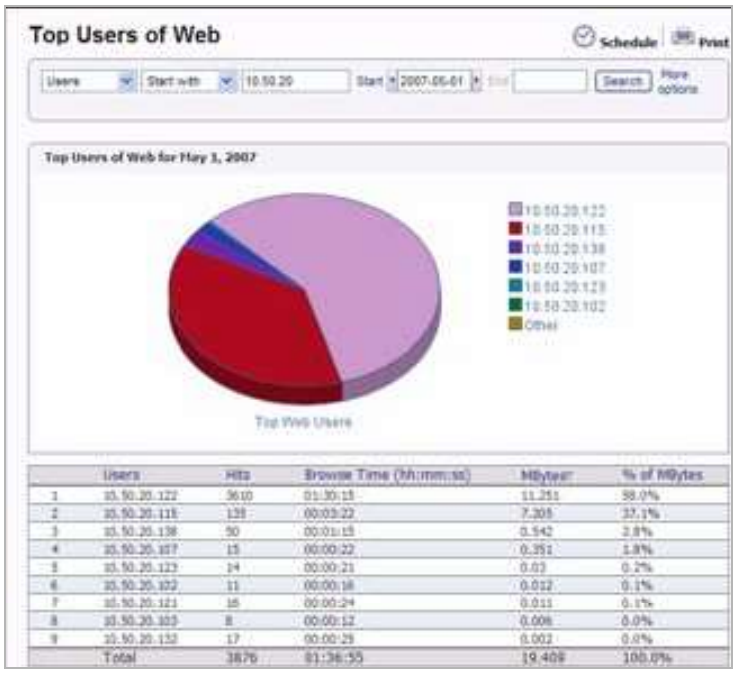


A character-based list contains **Equals**, **Start with**, **End with**, and **Contains** operators. If the content of the selected column contains numerical data, a list with mathematical symbols plus the **between** operator selection will display:

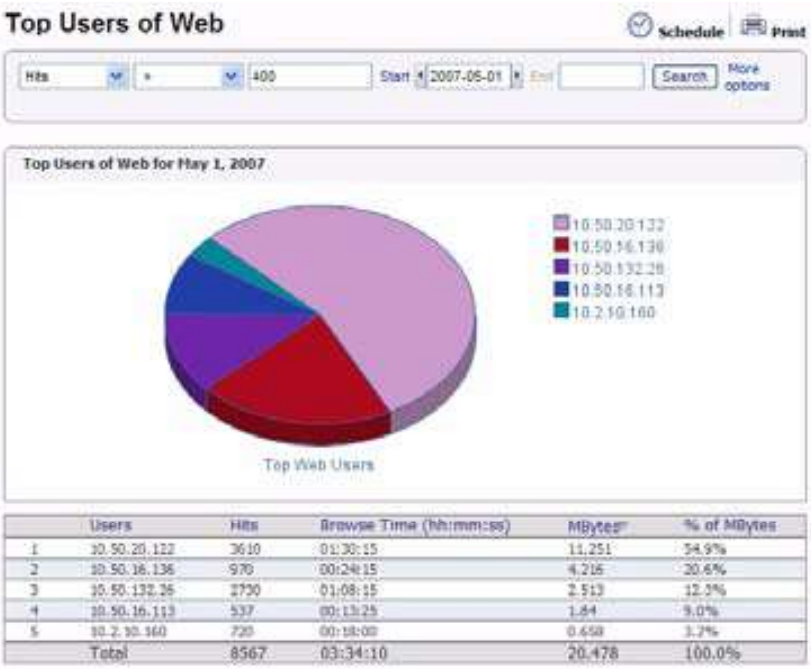


Keysight, EX-1030
Page 291

A generated report is shown below with user name (Users) starting with (Start With) “10.50.20” (the value of the search text field).



A generated report is shown below in which the Hit count (Hits column) is greater than (>) “100” (the value of the search field).



Keysight, EX-1030
Page 292

The calendar module of the search bar is shown below. You can use the calendar module to easily select a date for the Start or End field. You can also manually type in a date. For single day reports, the End field is disabled.



The detailed options are “per report” based. For example, if you select “PIE” as the chart type for report A, you will still see Bar chart in report B if the bar chart was the existing chart type. The detailed drop-down menu can be expanded by clicking **More Options** as shown in the red circle below.

As Figure 1 and Figure 2 show, the options in the detailed drop-down menu are context-based. Figure 1 shows the detailed options of the “Web Usage By User” report. As you can see, Figure 2 contains different options because it is specific to the By User report.

Figure 1 Context-based Detail Options



Keysight, EX-1030
Page 293

Figure 2 Web Usage by User - Report Display Settings



Collapsible TreeControl Pane

The unit TreeControl pane can be collapsed to free up screen space by clicking on the the small arrow button to the right of the Add Unit, Modify Unit, Refresh, and Find buttons above the TreeControl pane. The panel can be brought back by clicking the same button.

Enabling/Disabling Scheduled Reports

ViewPoint allows you to disable a scheduled report without deleting it. This allows you to re-use the report at a later time without having to create it again. To enable or disable a report, navigate to the **Configuration > Scheduled Reports** page under the **UTM** tab. This screen shows all the scheduled reports on the current appliance. Select the checkbox in the row for a report(s) that you wish to disable, and click the **Disable Selected Scheduled Reports** button above the table. After confirmation, the check mark in the Enabled column is grayed out. To re-enable the report, use the **Enable Selected Scheduled Reports** button above the table.

Combined Reports

Users familiar with ViewPoint 4.0 will find two categories of reports that are no longer visible on the function tree: the **Browse Time** report and the **ROI** report. The information from these two reports have been folded into the **Web Usage** and **Bandwidth** reports, respectively. The **Web Usage** report pages now feature a **Browse Time** column. The **Bandwidth** report pages feature a **Cost($)** column that displays all the information previously displayed by the ROI reports.

Keysight, EX-1030
Page 294

Improved Navigation

To save time, ViewPoint now features linked reports. **Web Usage** and **Web Filter** reports now link their **By User** and **By Site** pages. It is now possible to navigate directly from the **Web Usage > By User page** to a **Web Usage > By Site** page or from the **Web Filter > By User page** to a **Web Filter > By Site** page detailing the information of the site that the user has been browsing. Click the **Plus** sign next to the entry in the User column to show details, and hover the mouse over a site. A sticky tooltip will display with a link to the corresponding site's report page. This makes navigating from one report to the next much easier and makes retrieving detailed information simple.

Sample Navigation Use Case

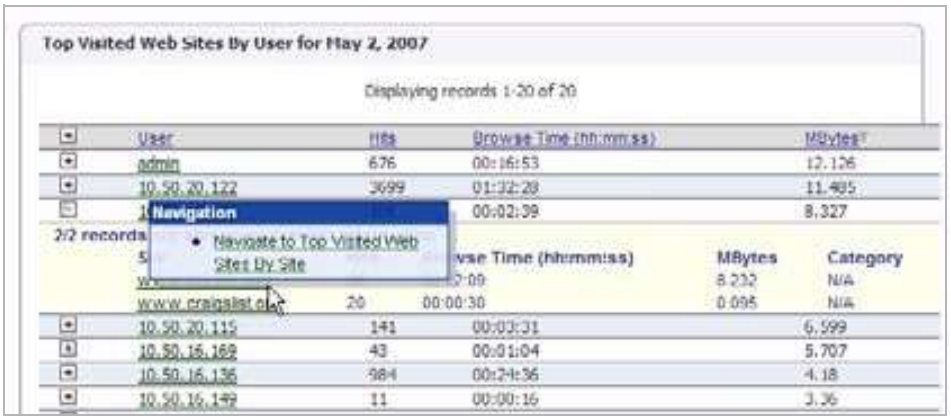
This sample use case demonstrates the improved navigation feature. In this use case you will open up the **Web Usage > By User** report and observe what sites the top browser has been visiting. Then you will move directly from the **By User** report to a detailed **By Site** report.

1. Navigate to the **Web Usage > By User** report from the **UTM** tab.



2. Click the **Plus** button next to any IP address in the User column. This displays detailed information about the sites that the user at that address has been visiting.

3. Hover your mouse over a site in this list. Click the **Navigate to Top Visited Web Sites By Site** link to navigate directly to the **Web Usage > By Site** report page.



The **Web Usage > By Site** report page shows detailed information about Web traffic to this site. Information in this report include the IP addresses of users who have browsed that site, as well as how much time they have spent browsing.

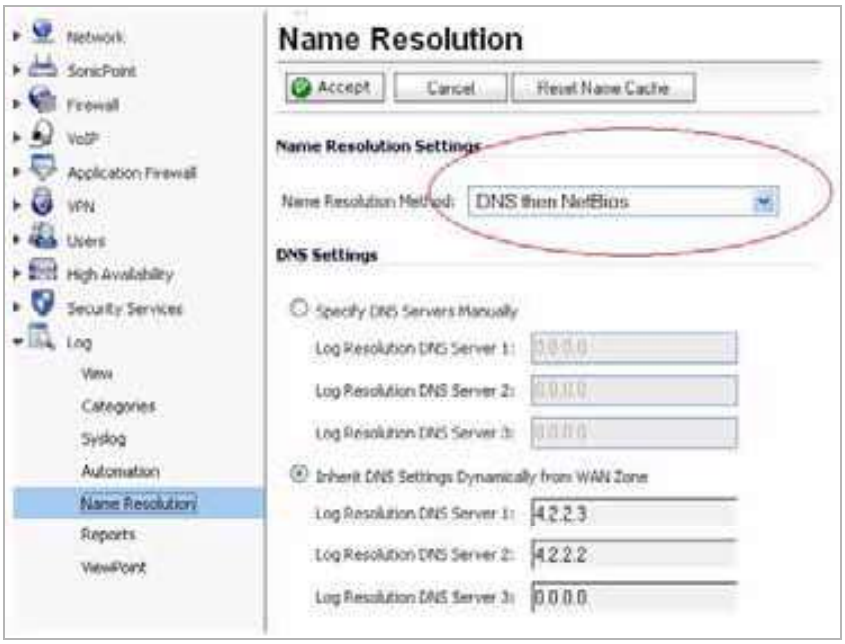
Showing Domain Names in Reports

Reports sometimes show the domain names of systems or websites, and sometimes show only the IP address. This is caused by different firmware versions on the appliances for which reports are being generated.

The reporting subsystem consumes the contents of src, dst, dstname, and other tags from the syslog messages. The syslog format and tags depend on the version of the firmware.

For firmware that includes name resolution, the reports will list the domain.

Note In SonicWALL ViewPoint 5.1 and above, the Name Resolution option on the UTM appliance (where the firmware supports it) is enabled when a unit is added. This does not apply to already existing appliances in the system.



Managing ViewPoint Reports on the Console Panel

There are management settings for the ViewPoint Reporting Module on the ViewPoint **Console** panel. The UTM panel contains limited configuration screens, used for managing scheduled reports and per-unit settings.The Reports section on the Console panel is divided into sections that allow you to manage system-wide settings, including the following:

Table 4 Console > Reports

Section	Settings
Settings	Report Settings/Options
	Log Viewer Settings
Summarizer	Summarizer Settings

Section	Settings
	Reports Data Summarization Interval
	Syslog Deletion Schedule
	Host Name Resolution Settings
Email/Archive	Email/Archive Time Settings
	Days to Store Archived/Published reports
	Email/Archive Configuration - Web Server Details
	Logo Settings
	SortBy Settings In PDF Reports
Scheduled Reports	Summary
	Search Criteria
	Search Results
Management	Report Data Management Settings

The Reports section of the Console panel controls settings for syslog data collection, summarizer configuration, email and archiving, scheduling reports, and archiving report data.

- For information about syslog data collection settings, see the "Enabling Report Table Sorting" section on page 72 in the Managing Reports in the Console Panel chapter.
- For information about the summarizer, see the following sections in the Managing Reports in the Console Panel chapter:
  - "About Summary Data in Reports" section on page 73
  - "Summarizer Settings and Summarization Interval" section on page 73
- For information about Email and Archiving settings, see the "Configuring Email/Archive Settings" section on page 81 in the Managing Reports in the Console Panel chapter.
- For a description of how to schedule reports in the Console panel, see the "Scheduled Reports" section on page 82 in the Managing Reports in the Console Panel chapter.
- For information about archiving report data using the Move Data to Archive (MDTA) feature, see the "Management" section on page 87 in the Managing Reports in the Console Panel chapter.

CHAPTER 14
Scheduling and Configuring Reports

This chapter provides information about scheduling automatic reports and configuring data summarization settings. It also contains instructions for configuring settings for the Dashboard > Summary report and describes how to view the list of current alerts on the **Events > Current Alerts** page. This chapter also describes how to export compliance reports in PDF format. The settings described in this chapter are applied on a per-unit basis.

This chapter includes the following sections:

- "Configuring Scheduled Reports" section on page 134
- "Selecting Reports for Summarization" section on page 137
- "Configuring Inheritance for Reporting Screens" section on page 138
- "Configuring Data Storage Settings" section on page 139
- "Configuring Summarization Data for Top Usage" section on page 140
- "Configuring Summarization Data for Bandwidth Reports" section on page 141
- "Configuring Dashboard Summary Reports" section on page 142
- "Viewing Current Alerts" section on page 144
- "Scheduling PDF Compliance Reports" section on page 144

Configuring Scheduled Reports

SonicWALL ViewPoint Reporting can automatically send reports to any email addresses that you specify. This section contains the following:

- “Viewing or Managing Scheduled Reports” on page 134
- “Adding or Editing a Scheduled Report” on page 135

To create scheduled email reports in PDF format as *Compliance Reports*, see the “Scheduling PDF Compliance Reports” section on page 144.

Viewing or Managing Scheduled Reports

To view , delete, or enable/disable currently scheduled reports, perform the following steps:

1. Click the **UTM** tab and select a SonicWALL appliance.
2. Expand the **Configuration** tree and click **Scheduled Reports**. The Scheduled Reports page displays.



3. On the Scheduled Reports page, to add a new scheduled report, click **Add Scheduled Report**. See “Adding or Editing a Scheduled Report” on page 135.
4. To edit a report, click the pencil icon in that row. See “Adding or Editing a Scheduled Report” on page 135.
5. To delete a report, select the checkbox in that row and then click **Delete Selected Scheduled Reports**.
6. To disable a scheduled report, select the checkbox in that row and then click **Disable Selected Scheduled Reports**.
7. To enable a disabled report, select the checkbox in that row and then click **Enable Selected Scheduled Reports**.
8. To select all reports in the list, click **Select All Scheduled Reports**.