

5. The table contains the following information for all users:
 - **Users**—the user name of the user
 - **Connections**—number of connection events or “hits”
6. The ViewPoint Reporting Module shows yesterday’s report. To change the date range of the report, click the **Start** or **End** field to access the drop-down calendar.
7. To display a limited group of users, enter the user IDs in the **Search Bar** fields.



Note The search bar fields use pattern matching with operators such as “contains”. For example, “john” will match john_smith, john42, or big_john.

8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected users and date range.



Note These settings will stay in effect for all similar reports during your active login session.

Using SSL-VPN Custom Reports

Custom Reports are available at the unit level for appliances visible on the SSL-VPN tab. Log Viewer must be enabled for the appliance. For information about enabling Log Viewer, see [“Viewing the SSL-VPN Log” on page 332](#).

When configuring a Custom Report on the Resource Activity page, the Template Section acts as a query builder. You select the criteria for the report that you want, and SonicWALL ViewPoint uses your input to query the raw syslog database for the information, and then outputs the report. The Template Section consists of two parts: the Date/Time section and the Report Layout section.

After building your query in the Template Section and clicking the **Generate Report** button, the report is displayed in the Report Section. The Report Section is displayed in the lower half of the page, under the Template Section; this layout is called Split Mode. You can easily toggle between Split Mode and Full Mode. Full Mode can be used to display only the Template Section or only the Report Section in a full page view.

The Report Section displays the report and provides controls for pagination, printing, and exporting the report in PDF or CSV format. You can also click the **Save Template** button in this section if you want to save the settings for this report as a template for reuse later. See the following sections for detailed information:

- [“Toggling Between Split Mode and Full Mode” on page 308](#)
- [“Configuring the Date and Time for Custom Reports” on page 311](#)
- [“Configuring the Report Layout and Generating the Report” on page 314](#)
- [“Generating the Custom Report” on page 320](#)
- [“Viewing a Custom Report” on page 321](#)
- [“Printing a Page or Exporting the Report as a PDF or CSV File” on page 323](#)
- [“Saving the Report Template” on page 324](#)

Toggling Between Split Mode and Full Mode

The Custom Report page contains two main sections, the Template Section and Report Section, which can be displayed together or independently depending on the mode.

When the Custom Report page is initially displayed for a selected appliance, the Template Section is displayed in Full Mode. Split Mode is available, but the Report Section displays no data until a report has been generated. The image below shows the Custom Report > Resource Activity page with the Template Section displayed in Full Mode.

The screenshot displays the 'Custom Report – Resource Activity' page in 'Full Mode'. The page is titled 'Template Section' and includes a '<Split Mode>' link. The main heading is 'Custom Report – Resource Activity', followed by a 'Template' dropdown menu set to '-- Load a Template --'. Below this, the 'Date/Time' section offers two options: 'Dynamic Date Range' (selected) with a 'Today' dropdown, and 'Static Date Range' with 'Start Date' and 'End Date' input fields. Both options include 'Start Time' and 'End Time' dropdowns for hour, minute, and second. The 'Report Layout' section has two tabs: 'Detailed Report' (selected) and 'Summary Report'. Under 'Detailed Report', there is a 'Select report field' dropdown set to 'Destination IP' with an 'Add' button, and a 'Sort by' dropdown set to 'Date/Time' with an 'and' button and another 'Date/Time' dropdown. Below these is a table with columns 'Field', 'Filter', and 'Options'. At the bottom of the page are 'Generate Report' and 'Reset' buttons.

After generating a report, the page automatically changes to Split Mode and displays the report settings in the Template Section in the top half of the page and the report results in the Report Section in the lower portion. The image below shows the Template Section and Report Section displayed in Split Mode.

Template Section <Full Mode>

Custom Report – Resource Activity Template: – Load a Template –

Date/Time

☒ Dynamic Date Range Week to date Start Time: 00:00:00 End Time: 23:59:59

☐ Static Date Range Start Date: End Date: Start Time: 00:00:00 End Time: 23:59:59

Report Layout

Detailed Report Summary Report

Select report field: User Add Sort by: Date/Time and Date/Time

Field Filter Options

Report Section <Full Mode>

Resource Activity Save Template Print Export

Page 1 / 8

	Date/Time	Destination IP	Source IP	Protocol	User
1	2009-12-09 15:58:13	192.168.151.126	10.195.11.82	N/A	(ip)SP(10
2	2009-12-09 16:08:23	192.168.151.126	10.195.11.82	N/A	(ip)SP(10
3	2009-12-09 16:35:41	127.0.0.1	10.195.11.82	Translation-NoAgent	(ip)SP(10
4	2009-12-09 16:35:41	127.0.0.1	10.195.11.82	Translation-NoAgent	(ip)SP(10
5	2009-12-09 16:35:41	192.168.151.126	10.195.11.82	N/A	(ip)SP(10
6	2009-12-09 16:35:51	192.168.151.126	10.195.11.82	N/A	(man)u(10
7	2009-12-09 16:35:51	127.0.0.1	10.195.11.82	Translation-NoAgent	(man)u(10

At any time, you can change to Full Mode if you want to display either the Template Section or the Report Section individually. From Full Mode, you can easily change back to Split Mode.

To toggle between Split Mode and Full Mode:

1. Select a unit for which Log Viewer is enabled, and then navigate to the **Custom Report** page.
2. On a page that is currently displayed in Full Mode, to change the view to Split Mode click the **<Split Mode>** button at the right side of the section heading.

3. On a page that is currently displayed in Split Mode, do one of the following to change to a Full Mode display of either the Template Section or the Report Section:
 - Click the **<Full Mode>** button to the right of the Template Section heading.
 - Click the **<Full Mode>** button to the right of the Report Section heading.

Configuring the Date and Time for Custom Reports

At the top of the Template Section of the Custom Report page, the Date/Time region provides a way to designate the time period to use when generating the report. You can select either a Dynamic Date Range or a Static Date Range.

Both the Dynamic Date Range and the Static Date Range provide Start Time and End Time settings. By using the Start Time and End Time fields, you can specify the exact hour, minute, and second for both the beginning and the end of the period for the report. When a start and end time is specified for a date range containing multiple days, the start/end times are applied to each day of the period when analyzing data for the report. The default is to include data for the full 24 hours in each day of the date range.

Dynamic Date Range

The **Dynamic Date Range** selection allows you to select from four date ranges and to specify the exact starting and ending times on the days in the selected date range for the log data to be used for the report.

For the **Dynamic Date Range**, you can select from the following four date choices:

- **Today** – Uses log data from the current date, beginning just after midnight
- **Yesterday** – Uses log data from just after midnight of the previous day, up to and including the most recent log message from the current date

- **Week to Date** – Uses log data from the current date, plus the seven preceding days
- **Month to Date** – Uses log data from the same date as the current date in the previous month, up to and including the most recent log message from the current date

When generating a report with a template containing a dynamic date range setting, the dates used when referencing the log data are relative to the current date. Thus, two reports generated from the same template on different days will provide different results.

To select a Dynamic Date Range:

1. Select a unit for which Log Viewer is enabled, and then navigate to the page under **Custom Report** for the report type you want.
2. In the Template Section under Date/Time, select the **Dynamic Date Range** radio button.
3. In the drop-down list, select **Today**, **Yesterday**, **Week to Date**, or **Month to Date**.
4. For the **Start Time**, select the hour, minute, and second from the drop-down lists in the Dynamic Date Range row. These settings specify the earliest data to be included in the report, for each day of the date range.
5. For the **End Time**, select the hour, minute, and second from the drop-down lists. These settings specify the most recent data to be included in the report, for each day of the date range.
6. To change the settings back to the defaults, click **Reset** at the bottom of the Template Section. Note that this will change the Report Layout region as well as the Date/Time region back to default settings.

Static Date Range

The **Static Date Range** selection allows you to specify the exact dates, starting, and ending times on the days in the selected date range for the log data to be used for the report. You can specify a single date or a date range, and indicate the exact hour, minute, and second for both the beginning and the end of the daily period for the report.

A popup calendar makes it easy to select the Start Date and End Date for the date range, as shown below.

To specify a Static Date Range:

1. Select a unit for which Log Viewer is enabled, and then navigate to the page under **Custom Report** for the report type you want.
2. In the Template Section under Date/Time, select the **Static Date Range** radio button.
3. Click the **Start Date** field to access the pop-up calendar.
4. Use the navigation arrows near the top of the calendar to change the year or month. Click the << button to move to the previous year, or hold the button to select from a list of years. Click the >> button to move to the next year, or hold the button to select from a list of years. Similarly, click the < or > to move back or ahead by one month, or hold the button to select from a list of months.
5. Click the desired start date in the calendar. This adds the date to the **Start Date** field and closes the calendar.
6. Click the **End Date** field to access the pop-up calendar.
7. Use the navigation arrows near the top of the calendar to change the year or month.
8. Click the desired end date in the calendar. This adds the date to the **End Date** field and closes the calendar.
9. For the **Start Time**, select the hour, minute, and second from the drop-down lists in the Static Date Range row. These settings specify the earliest data for each day in the date range to be included in the report.

10. For the **End Time**, select the hour, minute, and second from the drop-down lists. These settings specify the most recent data for each day in the date range to be included in the report.
11. To change the settings back to the defaults, click **Reset** at the bottom of the Template Section. Note that this will change the Report Layout region as well as the Date/Time region back to default settings.

Configuring the Report Layout and Generating the Report

Located in the Template Section of the Custom Report page below the Date/Time region, the Report Layout region provides a way to specify the type of data to include, and the format of the report. The Report Layout region has a Detailed Report tab and a Summary Report tab. The report appearance and the way information is organized is quite different between a Detailed Report and a Summary Report.

The Detailed Report tab contains a list of data categories that you can add as report fields, and allows you to specify query values for each. The categories you select will appear as column headings in the report.

The Summary Report tab allows you to structure a report showing the top elements of Resource Activity. You can select the number of top elements, what to base the comparisons on, and the two data categories to evaluate when determining the top elements. The generated report provides graphical output that you can click to drill down for detailed information.

For more information about each of these Report Layout tabs, see the following sections:

- [“Detailed Reports” on page 315](#)
- [“Summary Reports” on page 318](#)

For information about the Filter operators, see the following section:

- [“Filter Operators” on page 319](#)

Detailed Reports

The Detailed Report tab is the default view in the Report Layout region.

For a SSL-VPN Resource Activity report, the **Select report field** drop-down list contains four data categories that you can add as column headings in the report. The categories are:

- **Destination IP** – Adds a column containing the IP address of each accessed resource
- **Protocol** – Adds a column containing the protocol used by the traffic
- **Source IP** – Adds a column containing the IP address of each system which accessed a resource
- **User** – Adds a column containing the user ID

To include a field in the report, select a choice from the list and then click **Add**. When you click **Add**, a row is populated in the table below, which has three column headings: Field, Filter, and Options.



Note

When you place your mouse cursor over the row, under the Field heading, the cursor changes to a “move” cursor. You can drag and drop the rows to rearrange the column ordering in the final report.

In the Filter column, two fields are displayed: an operator field and an input field. The operator field is a drop-down list containing the operator choices for the selected report field. See [“Filter Operators” on page 319](#) for a description of each operator. The input field can be a drop-down list or a standard input field, depending on the selected report field.

The operators and input fields are defined in [Table 7](#) for each report field.

Table 7 Operators and Input Fields for Each Data Type

Data Type	Operators	Input Field
Destination IP	Equals Starts with Ends with Contains	The input field is a standard input field where you can type in the numbers to match, such as 192 or 10.25. Leave the input field blank if you choose not to filter by a certain destination IP address.
Protocol	Equals Start with End with Contains	The input field is a standard input field where you can type in the protocol to match, such as FTP. Leave the input field blank if you choose not to filter by a certain protocol.
Source IP	Equals Starts with Ends with Contains	The input field is a standard input field where you can type in the numbers to match, such as 192 or 10.25. Leave the input field blank if you choose not to filter by a certain source IP address.
User	Equals Start with End with Contains	The input field is a standard input field where you can type in the user ID to match. Leave the input field blank if you choose not to filter by a certain user.

In the Options column, two icons are displayed: an Eye  and an X . You can click the Eye to toggle whether the report field on that row will be displayed in the final report. This allows you to filter the report results based on the selected report field and related filter value, but not display the field as a column. When you click on the Eye icon within a row, the eye closes  to show that this field will not be displayed in the final report. The filter value will still be used to filter results from the raw syslog database to apply towards the report.

For example, you might specify the following Field/Operator/Filter Value: **Protocol=/http**. It would make sense to click the Eye icon to disable the Protocol field from being shown in the report, since it would always just be “http” and would not add any interesting information to the final report. Contrast this with simply specifying the Protocol field and leaving the Filter Value blank, in which case you would want to enable the Eye so that this column would appear in the report showing a variety of protocols such as udp/dns, tcp/http, udp/ntp, or numbered protocols such as udp/389 (the LDAP protocol) or tcp/445 (MS Server Message Block (SMB) file sharing).

Clicking the X icon under Options deletes the selected report field from the table, so it will not be used to generate the report results nor will it be displayed in the report. Use the X icon instead of the Eye when you do not choose to filter the report results based on the field.

The Detailed Report tab also contains the Sort By drop-down list. The list contains the Date/Time option and any other report fields that you have selected from the eight data types. The choice you select will be used to order the results in the report from the first page to the last. The selection in the left drop-down list is used for the first sorting, then the selection in the right drop-down list is used to sort and group the entries within each group resulting from the the first sorting.

To configure a detailed report:

1. Select a unit for which Log Viewer is enabled, and then navigate to the page under **Custom Report** for the report type you want.
2. In Report Layout region of the Template Section of the Custom Report page, select the **Detailed Report** tab.
3. In the **Select report field** drop-down list, select a data type to include in the report, and then click **Add**. A row for this field is populated in the table below. Repeat this step to add other fields.
4. Optionally select an operator from the drop-down list under **Filter** in a table row, and type in or select an input value to be matched when the database is queried. Repeat this step for other rows to add filter values for those fields.
5. To prevent a field from appearing in the final report, click the **Eye** icon in that row so that the eye appears closed. To allow the field to be displayed in the report, click the closed **Eye** icon to return it to normal appearance.
6. To delete a field from the table, click the **X** icon in that row.
7. To sort the report pages by a different field than the default of Date/Time, select the desired field from the **Sort by** drop-down list.
8. To change the settings back to the defaults, click **Reset** at the bottom of the Template Section. Note that this will change the Date/Time region and the Report Layout region back to default settings.

Summary Reports

The Summary Report tab is available in the Report Layout region of the Template Section.

The screenshot shows the 'Report Layout' window with the 'Summary Report' tab selected. At the top, there are two tabs: 'Detailed Report' and 'Summary Report'. Below the tabs, there is a 'Top' drop-down menu set to '5' and a 'Summary Report' label. To the right, there is a 'Summary Base' drop-down menu set to 'Event Count'. Below these, there is a instruction: 'Drag a field below to the right to be a summary group'. On the left, there is a list of fields: 'Destination IP', 'Protocol', 'Source IP', and 'User'. On the right, there are two summary group boxes: 'Level 1 Summary Group' and 'Level 2 Summary Group'. Each box has a red 'X' icon in the top right corner.

The Top drop-down list provides selections for the number of entries to display in the report. For example, if the User field is selected below as a Summary Group, and 5 is selected in the Top drop-down list, the report will provide entries for the top five users. For all Custom Reports, available numbers in the Top drop-down list are 5, 10, 20, 50, and 100.

The Summary Base drop-down list offers a selection of traffic types that will be used to determine the top usage for the selected field. For a SSL-VPN Resource Activity report, the only Summary Base choice is **Event Count**.

Below the Top and Summary Base fields, you can create one or two Summary Groups from the choices listed on the left side. For a SSL-VPN Resource Activity report, the choices are **Destination IP**, **Protocol**, **Source IP**, or **User**.

To select a field for a Summary Group, simply drag and drop the desired field from the list to either the Level 1 Summary Group or Level 2 Summary Group boxes. When the field name is dragged to one of these, the operator drop-down list and filter input value field are displayed, allowing you to specify values to match when the data is searched. See [“Filter Operators” on page 319](#) for a description of each operator.

Either the Level 1 Summary Group field or the Level 2 Summary Group field can be used alone; the resulting report will look the same in both cases.

When both the Level 1 and Level 2 Summary Group fields are populated, the report will display the top entries for the Level 2 field for each of the top entries for the Level 1 field. For example, if User is dragged to the Level 1 Summary

Group and Domain is dragged to the Level 2 Summary Group, and 5 is selected in the Top drop-down list, the generated report will display the top five domains visited by each of the top five users.

To configure a summary report:

1. Select a unit for which Log Viewer is enabled, and then navigate to the page under **Custom Report** for the report type you want.
2. In Report Layout region of the Template Section of the Custom Report page, select the **Summary Report** tab.
3. In the **Top** drop-down list, select the number of entries to be displayed in the report.
4. In the **Summary Base** drop-down list, use the default, **Event Count**.
5. To specify the field for the **Level 1 Summary Group**, click and drag the desired field from the list on the left to the **Level 1 Summary Group** field, and then release your mouse button to drop the field into position. The filter operator and input field are displayed next to the field name.



6. To specify the field for the **Level 2 Summary Group**, click and drag the desired field from the list on the left to the **Level 2 Summary Group** field, then release your mouse button to drop the field into position. The filter operator and input field are displayed next to the field name.
7. To specify a filter operator and filter value for a Summary Group, select the operator from the drop-down list next to the field and type a filter value into the input field to the right of the operator.
8. To change the settings back to the defaults, click **Reset** at the bottom of the Template Section. Note that this will change the Date/Time region as well as the Report Layout region back to default settings.

Filter Operators

When configuring the Report Layout on either the Detailed Report tab or the Summary Report tab, you can specify filter values to be matched in the database during report generation. Depending on the selected field type, text string or numeric, several filter operators are available. The filter operators are used with a filter input value to determine which data should be included in the report.

The operators are defined as shown in [Table 8](#).

Table 8 *Filter Operators*

Operator	Definition
Equals	Only data that exactly matches the filter input text will be included in the report
Start with	Data that begins with the input text will be included in the report
End with	Data that ends with the input text will be included in the report
Contains	Data that contains the input text will be included in the report
=	Only data that exactly matches the filter input numerical value will be included in the report
>	Data values that are greater than the input numerical value will be included in the report
>=	Data values that are greater than or equal to the input numerical value will be included in the report
<=	Data values that are less than or equal to the input numerical value will be included in the report
<	Data values that are less than the input numerical value will be included in the report
!=	Data values that are not equal to the input numerical value will be included in the report

Generating the Custom Report

The Generate Report button at the bottom of the Template Section is used to create the report. Before clicking Generate Report, use the Template Section to specify the time period for the report and the contents and layout of the report.


Note

Custom Reports are available at the unit level and Log Viewer must be enabled for the appliance. For information about enabling Log Viewer, see [“Viewing the SSL-VPN Log” on page 332](#).

To generate a custom report:

1. Select a unit for which Log Viewer is enabled, and then navigate to the page under **Custom Report** for the report you want.

2. In the **Date/Time** region of the Template Section, specify the time period that the report will cover. For detailed information and instructions, see [“Configuring the Date and Time for Custom Reports” on page 311](#).
3. In the **Report Layout** region of the Template Section, specify the contents and appearance of the report. For detailed information and instructions, see [“Configuring the Report Layout and Generating the Report” on page 314](#).
4. Click **Generate Report** to create the report using the specified configuration.

Viewing a Custom Report

After you click Generate Report, the Report Section is displayed in Split Mode in the lower half of the main window, even if you previously were in Full Mode for the Template Section.

Pagination controls are displayed at the upper right of the report, just below the Save Template button and the printer, PDF, and Excel icons. Navigation buttons are provided to take you to the first page, next page, previous page, and last page, or you can specify an exact page number in the field.



In a Detailed Report, the selected report fields are displayed as column headings. You can click on any column heading to sort that page by the values in the column that you click. Click again to toggle between ascending and descending order on that page. When you navigate away from that page and

then come back using the pagination controls, the page reverts to the original sorting order as specified in the **Sort by** field of the Template Section before generating the report.

Report Section <Split Mode>					
Resource Activity Save Template					
Page 1 / 4					
	Date/Time	Destination IP	Source IP	Protocol	User
1	2009-12-09 15:50:13	192.168.151.126	10.195.11.82	N/A	{p}@local
2	2009-12-09 16:00:23	192.168.151.126	10.195.11.82	N/A	{UNKNOWN}@Null Auth ...
3	2009-12-09 16:35:41	192.168.151.126	10.195.11.82	N/A	{UNKNOWN}@Null Auth ...
4	2009-12-09 16:35:41	127.0.0.1	10.195.11.82	Translation-NoAgent	{UNKNOWN}@Null Auth ...
5	2009-12-09 16:35:41	127.0.0.1	10.195.11.82	Translation-NoAgent	{UNKNOWN}@Null Auth ...
6	2009-12-09 16:35:51	192.168.151.126	10.195.11.82	N/A	{manu}@local
7	2009-12-09 16:35:51	127.0.0.1	10.195.11.82	Translation-NoAgent	{manu}@local
8	2009-12-09 16:35:51	127.0.0.1	10.195.11.82	Translation-NoAgent	{manu}@local

In a Summary Report, the Report Section displays the event count as horizontal bar charts. This lets you see the information at a glance, such as who had the most resource activity and which protocols they used the most.

Report Section <Split Mode>			
Resource Activity Save Template			
Page 1 / 1			
	User	Protocol	Event Count
1	{manu}@local	N/A	31
2		Translation-NoAgent	23
3		EWPCA	5
4		N/A	2
5		-	1
6	{onnm}@local	N/A	30
7		Translation-NoAgent	27
8		N/A	2
9		-	1
10	{p}@local	N/A	19
11		EWPCA	15
12		N/A	4
13	{UNKNOWN}@Null Auth ...	N/A	12
14		N/A	6
15		Translation-NoAgent	6

You can click on a bar in the chart to pop up detailed information, just like the detailed report with all of the columns for all fields. The report lists details about this Summary Group field only. For example, if the Summary Group contains the User field and you click on a bar for one of the top users, the report displays the date and time of all resource activity for the user, and

includes data for every field available for detailed reports. A scroll bar is provided along the bottom of the Detailed Information window to allow viewing of all four fields plus the date and time column.

The Detailed Information window is shown below.

The screenshot shows a window titled 'Resource Activity' with a 'Detailed Information' sub-window. The sub-window displays a table with 5 columns: Date/Time, User, Destination IP, and Protocol. The table contains 22 rows of data, all showing the same user and destination IP, with varying timestamps. A scroll bar is visible at the bottom of the table.

	Date/Time	User	Destination IP	Protocol
1	2009-12-09 16:35:51	(manju)@local	127.0.0.1	Translation-NoAgent
2	2009-12-09 16:35:51	(manju)@local	127.0.0.1	Translation-NoAgent
3	2009-12-09 16:36:19	(manju)@local	127.0.0.1	Translation-NoAgent
4	2009-12-09 16:36:19	(manju)@local	127.0.0.1	Translation-NoAgent
5	2009-12-09 16:36:19	(manju)@local	127.0.0.1	Translation-NoAgent
6	2009-12-09 16:36:19	(manju)@local	127.0.0.1	Translation-NoAgent
7	2009-12-09 16:36:19	(manju)@local	127.0.0.1	Translation-NoAgent
8	2009-12-09 16:36:19	(manju)@local	127.0.0.1	Translation-NoAgent
9	2009-12-09 16:36:19	(manju)@local	127.0.0.1	Translation-NoAgent
10	2009-12-09 16:36:19	(manju)@local	127.0.0.1	Translation-NoAgent
11	2009-12-09 16:36:19	(manju)@local	127.0.0.1	Translation-NoAgent
12	2009-12-09 16:36:19	(manju)@local	127.0.0.1	Translation-NoAgent
13	2009-12-09 16:36:19	(manju)@local	127.0.0.1	Translation-NoAgent
14	2009-12-09 16:36:19	(manju)@local	127.0.0.1	Translation-NoAgent
15	2009-12-09 16:36:19	(manju)@local	127.0.0.1	Translation-NoAgent
16	2009-12-09 16:36:19	(manju)@local	127.0.0.1	Translation-NoAgent
17	2009-12-09 16:36:19	(manju)@local	127.0.0.1	Translation-NoAgent
18	2009-12-09 16:36:19	(manju)@local	127.0.0.1	Translation-NoAgent
19	2009-12-09 16:36:19	(manju)@local	127.0.0.1	Translation-NoAgent
20	2009-12-09 16:36:19	(manju)@local	127.0.0.1	Translation-NoAgent
21	2009-12-09 16:36:19	(manju)@local	127.0.0.1	Translation-NoAgent
22	2009-12-09 16:36:19	(manju)@local	127.0.0.1	Translation-NoAgent

Printing a Page or Exporting the Report as a PDF or CSV File

To print the current page of the report, click the printer icon  at the top of the Report Section. Your normal print dialog box pops up. This prints only the page that is currently displayed.

To export the entire report in PDF format, click the PDF icon  at the top of the Report Section. A PDF file is generated showing the report results in table format.

To export the entire report in Microsoft Excel Comma Separated Value (CSV) format, click the Excel icon  at the top of the Report Section. A CSV file is generated showing the report results in spreadsheet format.

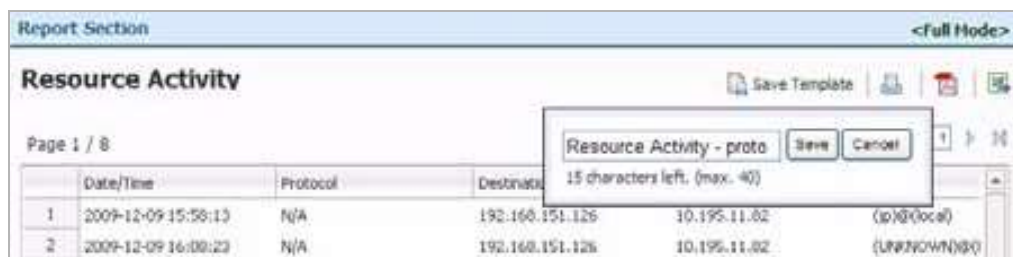
The PDF can contain a maximum of 10,000 records. If your report contains more than 10,000 records, you can use the Static Date Range fields to adjust the dates and regenerate the report to shorten its length. You can save the PDF or CSV file using any filename and location.

Saving the Report Template

After generating the report, you can save the settings for this report as a template for reuse. You can select the saved template from the Template Section at a later time, and use it to generate a report using the same settings. The template is saved for the currently selected appliance and for the specific user. The saved template will not be available for other appliances or for other users.

To save the report template:

1. In the Report Section in the upper right corner, click the **Save Template** button.



2. In the popup dialog box, type in a descriptive name for the template, up to 40 characters. The number of remaining characters allowed in the name is displayed below the input field and changes as you type.
3. Click **Save**. If you are in a Full Mode display of the Report Section, you can verify that the template has been saved by changing back to Split Mode and viewing the contents of the **Template** drop-down list.

Viewing SSL-VPN Resources Reports

Resources reports provide information on the amount of data transmitted through the selected SSL-VPN appliance by each service or protocol.

Resources reports are useful for revealing inappropriate usage of bandwidth and can help determine network policies. For example, if there is a large spike of bandwidth usage, you can determine whether this is caused by regular Web access, someone using FTP to transfer large files, an attempted Denial of Service (DoS) attack, or another service.



Note All reports appear in the appliance's time zone.

The procedures for viewing the Resources Reports are described in the following sections:

- [“Viewing SSL-VPN Resources Summary Reports” on page 325](#)
- [“Viewing SSL-VPN Resources Top Users Reports” on page 327](#)



Note You cannot view resources reports from the global view.

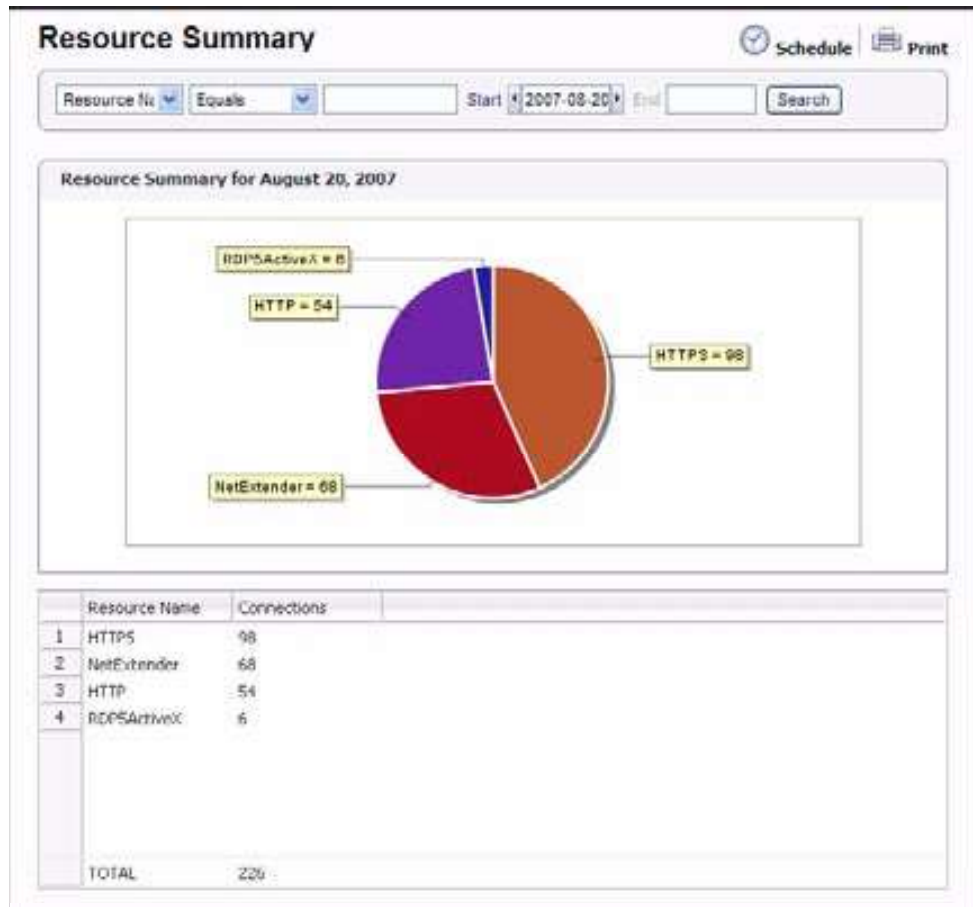
Viewing SSL-VPN Resources Summary Reports

The Resources Summary report displays the number of connections handled by each service or protocol during the specified day.

To view the Resources Summary report, perform the following steps:

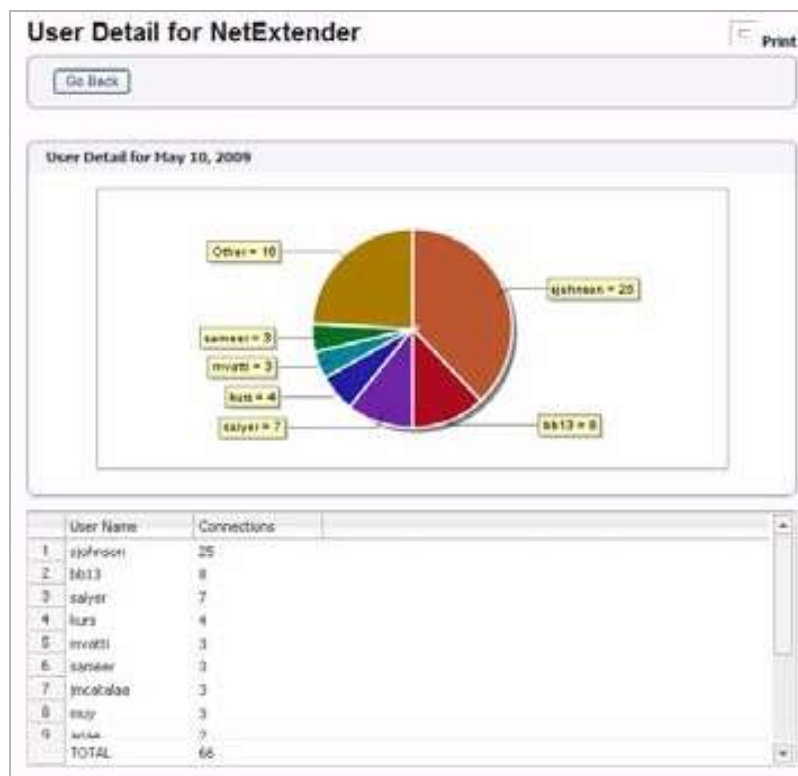
1. Click the **SSL-VPN** tab.
2. Select a SSL-VPN appliance.

- Expand the **Resources** tree and click **Summary**. The Resources Summary page displays.



- The graph displays the number of connections used by each service or protocol during the day.
- The table contains the following information:

- **Resource name**—the service or protocol
 - **Connections**—number of connection events or “hits”
6. To view the user detail for a particular resource, click the resource slice in the pie chart or the resource name in the table to drill down for this information.



7. To return to the Resources > Summary page, click the **Go Back** button.
8. To change the date of the report, use the Search Bar and click the **Start** field to access the drop-down calendar.
9. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date.



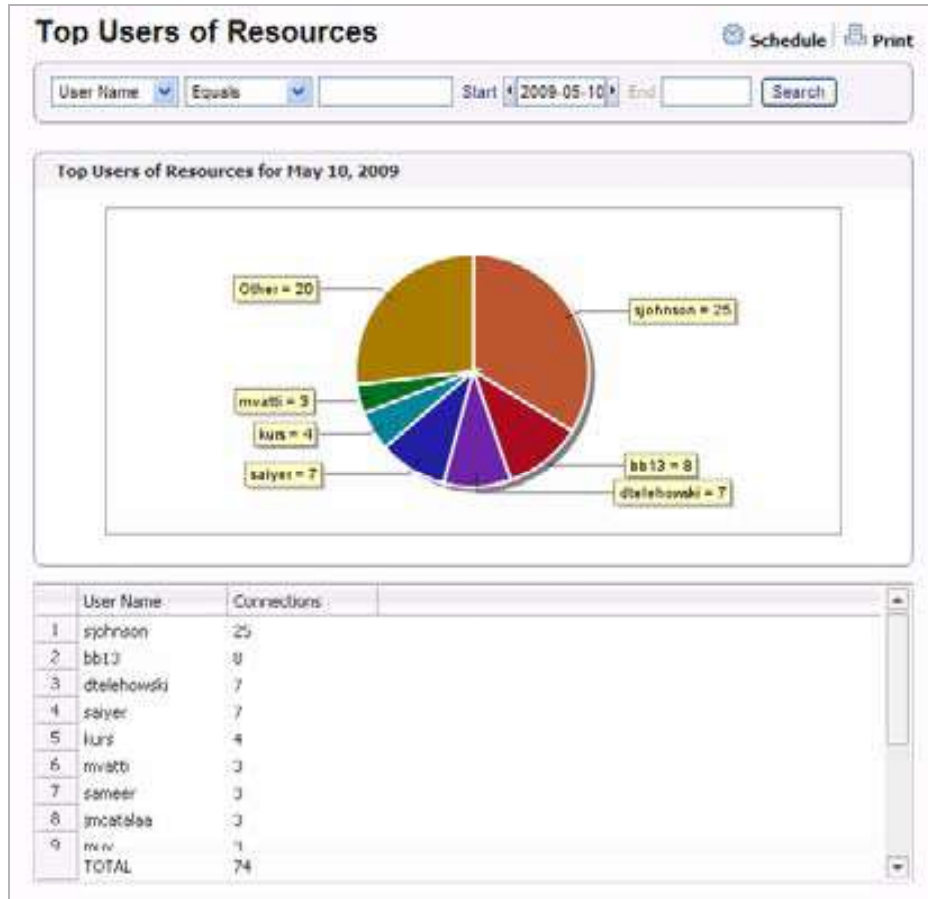
Note This date setting will stay in effect for all similar reports during your active login session.

Viewing SSL-VPN Resources Top Users Reports

The Resources Top Users report displays the users who used the most connections on the specified date.

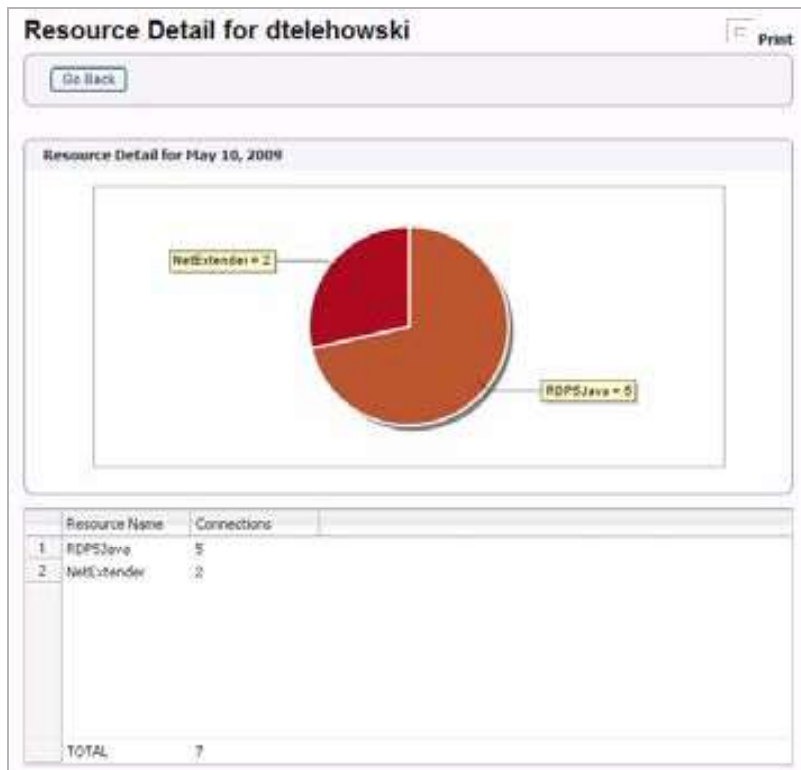
To view the Resources Top Users report, perform the following steps:

1. Click the **SSL-VPN** tab.
2. Select a SSL-VPN appliance.
3. Expand the **Resources** tree and click **Top Users**. The Top Users page displays.



4. The pie chart displays the percentage of connections used by each user.
5. The table contains the following information for all users:
 - **Users**—the user name
 - **Connections**—number of connection events or “hits”

6. To view the resources by service or protocol used by a particular user, click the user slice in the pie chart or the user name in the table to drill down for this information.



7. To return to the Resources > Top Users page, click the **Go Back** button.
8. By default, the ViewPoint Reporting Module shows yesterday's report, a pie chart for the top six users, and a table for all users. To change the date of the report, click the **Start** field to access the drop-down calendar.
9. To display a limited number of users, use the Search Bar fields.



Note The search bar fields use pattern matching with operators such as "contains". For example, "john" will match john_smith, john42, or big_john.

10. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected day.



Note The date setting will stay in effect for all similar reports during your active login session.

Viewing SSL-VPN Authentication Reports

The Authentication reports show user logins and failed login attempts. Authentication reports are available at the unit level.



Note All reports appear in the appliance's time zone.

Select from the following:

- [“Viewing SSL-VPN User Login Reports” on page 330](#)
- [“Viewing SSL-VPN Failed Login Reports” on page 331](#)

Viewing SSL-VPN User Login Reports

The user login report shows the user name, source host IP address, and time of login for users that logged on to the SSL-VPN appliance during the specified day.

To view the User Login report, perform the following steps:

1. Click the **SSL-VPN** tab.
2. Select a SSL-VPN appliance.
3. Expand the **Authentication** tree and click **User Login**. The User Login page displays.

The screenshot shows the 'User Logins' report interface. At the top, there are filters for 'User Name' (set to 'Equals'), 'Start' (2007-08-20), and 'End' (empty), with a 'Search' button. To the right are 'Schedule' and 'Print' icons. Below the filters is a table with the following data:

	Type	User Name	Source Host	Time	Duration
1	User Login	jgmueender	203.69.98.130	00:35:36	N/A
2	User Login	zchen	68.122.40.95	01:42:32	N/A
3	User Login	srishnamurthy	71.198.213.38	01:57:04	N/A
4	User Login	bb3	76.205.31.249	02:10:35	N/A
5	User Login	lwatanabe	210.138.204.194	02:26:19	N/A
6	User Login	bb1	207.190.245.55	02:34:46	N/A
7	User Login	hchen	24.6.223.81	02:40:06	N/A
8	User Login	hchen	24.6.223.81	02:49:41	N/A
9	User Login	dayrapetov	71.133.55.254	02:52:38	N/A
10	User Login	bb6	64.62.20.14	02:56:57	N/A

4. The table contains the following information:
 - **Type**—equal to User Login
 - **User Name**—the user name

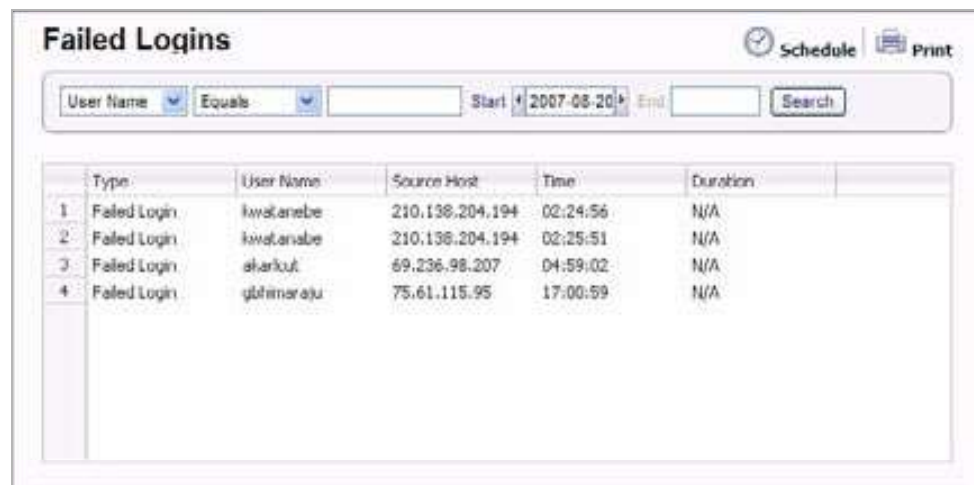
- **Source Host**—the IP address of the user's computer
 - **Time**—the time that the user logged in
 - **Duration**—the duration of the user login session
5. The ViewPoint Reporting Module shows yesterday's report. To change the date of the report, use the Search Bar and click the **Start** field to access the drop-down calendar.
 6. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date.

Viewing SSL-VPN Failed Login Reports

The failed login report shows failed login attempts for users who attempted to log into the SSL-VPN appliance during the specified day. This report is useful for identifying unauthorized access attempts and potentially malicious activity.

To view the Failed Login report, perform the following steps:

1. Click the **SSL-VPN** tab.
2. Select a SSL-VPN appliance.
3. Expand the **Authentication** tree and click **Failed Login**. The Failed Logins page displays.



	Type	User Name	Source Host	Time	Duration
1	Failed Login	kwakanebe	210.138.204.194	02:24:56	N/A
2	Failed Login	kwakanebe	210.138.204.194	02:25:51	N/A
3	Failed Login	sharkul	69.236.98.207	04:59:02	N/A
4	Failed Login	gblhmaraju	75.61.115.95	17:00:59	N/A

4. The table contains the following information:
 - **Type**—equal to Failed Login
 - **User Name**—the user name
 - **Source Host**—the IP address of the user's computer
 - **Time**—the time that the user attempted to log in

- **Duration**—not applicable
- 5. The ViewPoint Reporting Module shows yesterday's report. To change the date of the report, use the Search Bar and click the **Start** field to access the drop-down calendar.
- 6. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date.

Viewing the SSL-VPN Log

The Log Viewer contains detailed information on each transaction that occurred on the SSL-VPN appliance. This information is stored for the time that you specified in the configuration settings.

**Note**

The Log Viewer displays raw log information for every connection. Depending on the amount of traffic, this can quickly consume a large amount of space in the database. It is highly recommended to be careful when choosing the number of days of information that will be stored. For more information, see [“Scheduling and Configuring Reports”](#) on page 133.

Viewing the Log for a SSL-VPN Appliance

To view the Log, perform the following steps:

1. Click the **SSL-VPN** tab.
2. Select a SSL-VPN appliance.

- Expand the **Log Viewer** tree and click **Search**. The Search page displays.



Log Viewer Settings

☒ Enable Log Viewer **UPDATE**

Select Search Criteria

Start Date: 8/21/2007 Start Time: 00:00:00

End Date: 8/21/2007 End Time: 23:59:59

Source IP: All User:

Destination IP/Hostname: All

Message Category: Connections

Message Text: (blank for all)

Results Per Page: 500

Note: Specifying date, time, IP address, and Message Category will result in faster report generation.

☒ Generate Report

- Select **Enable Log Viewer** and then click **Update** to turn on collection of raw data in the database and enable viewing of that log data. This can consume a large amount of space in your database. Review your database space constraints before enabling the log viewer.
- Under Select Search Criteria, select the date range to view data from in the **Start Date** and **End Date** fields.
- Enter the starting time of events to view in the **Start Time** field.
- Enter the ending time of events to view in the **End Time** field.
- To limit the report to data originating from specific IP addresses, enter the source IP address in the **Source IP** field. To view all IP addresses, enter **All**.
- To view log entries for data originating from a particular user, enter the user name in the **User** field.
- To limit the report to data going to specific IP addresses or hosts, enter the destination IP address or host name in the **Destination IP/Hostname** field. To view data for all IP addresses, enter **All**.
- Select the type of events to view from the **Message Category** list box. You can select from the following:
 - All Categories
 - Connections
 - Rejected Connections

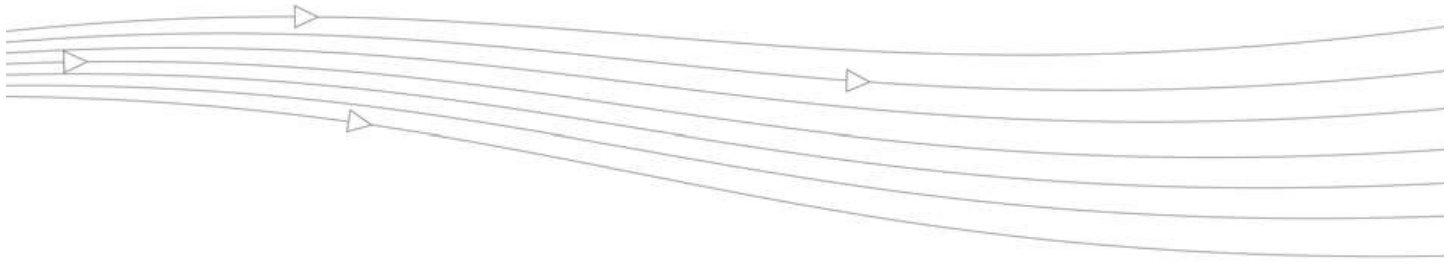
- User Events
 - Unrecognized Events
12. To limit the report to messages containing a specific text string, enter the text in the **Message Text** field. Leave the field blank to view all messages.
 13. Select the number of entries to display per page from the **Results Per Page** field.
 14. Click **Generate Report**. The Log Search Results page displays.

Log Search Results for August 23, 2007, 00:00:00 to August 23, 2007, 23:59:59, as of 08/23/2007 18:45:11 UTC
 Message Category: Connections

Displaying records 1-500 of 1015 [Next 500](#)

Time	Source	Destination	User	Resource	Message
08/23/2007 23:58:17	71.142.77.166	204.110.31.44	alvarez	NetExtender	NetExtender
08/23/2007 23:57:32	71.142.77.166	204.110.31.44	alvarez	NetExtender	NetExtender
08/23/2007 23:56:24	71.142.77.166	10.50.14.117	alvarez	RDPActiveX	Terminal Services
08/23/2007 23:56:05	71.142.77.166	204.110.31.44	alvarez	NetExtender	NetExtender
08/23/2007 23:55:23	71.142.77.166	204.110.31.44	alvarez	NetExtender	NetExtender
08/23/2007 23:54:06	71.142.77.166	204.110.31.44	alvarez	NetExtender	NetExtender
08/23/2007 23:53:33	75.24.111.94	10.50.128.206	cye	HTTPS	HTTPS Connection
08/23/2007 23:53:33	75.24.111.94	10.50.128.206	cye	HTTPS	HTTPS Connection
08/23/2007 23:53:33	75.24.111.94	10.50.128.206	cye	HTTPS	HTTPS Connection

15. To view the next page of entries, click **Next**.
16. To generate another report, click **Search** again in the **Log Viewer** tree.



Appendix A

Installing SonicWALL ViewPoint

This appendix is designed to help you install SonicWALL ViewPoint. If you have not used SonicWALL ViewPoint before, you might want to familiarize yourself with SonicWALL ViewPoint concepts and features. This appendix contains the following sections:

- [“About Installing and Upgrading SonicWALL ViewPoint” section on page 336](#)
- [“Activating SonicWALL ViewPoint on Your Appliances” section on page 340](#)
- [“Installing Universal Management Suite” section on page 342](#)
- [“Upgrading SonicWALL ViewPoint 5.1 to 6.0” section on page 349](#)
- [“Registering SonicWALL ViewPoint” section on page 351](#)
- [“Configuring Deployment Settings” section on page 354](#)
- [“Upgrading from ViewPoint to GMS” section on page 356](#)
- [“Miscellaneous Procedures and Troubleshooting Tips” section on page 368](#)

About Installing and Upgrading SonicWALL ViewPoint

You can either perform a fresh installation of SonicWALL ViewPoint using the installer or upgrade a previous installation of SonicWALL ViewPoint, patched or unpatched.

The upgrade installer checks with the SonicWALL backend to see if the SonicWALL ViewPoint deployment has valid support. If it does not, then the upgrade discontinues. When the SonicWALL ViewPoint installer detects that the SonicWALL backend site is not accessible, it prompts the user to enter an Upgrade Key.



If the key is valid, it allows the upgrade to continue. If the key is invalid, the installation fails.



Note The upgrade key can be obtained by contacting SonicWALL Technical Support.

Installing SonicWALL ViewPoint

This chapter describes how to install or upgrade SonicWALL ViewPoint.

To install or upgrade SonicWALL ViewPoint, complete the following procedures:

- Review the installation requirements. See [“Installation Overview”](#) on page 336.
- To install SonicWALL ViewPoint, see [“Installing Universal Management Suite”](#) on page 342.

Installation Overview

The SonicWALL ViewPoint Installation program is an HTML-launched installer that automatically detects whether you are installing on Windows Server 2000/2003/2008. After the installation program detects the operating system, the installation procedure is identical.

System Requirements

**Note**

SonicWALL does not support installations of ViewPoint running on any virtualization software, such as VMware.

Before installing SonicWALL ViewPoint, review the requirements in the following sections:

- [Operating System Requirements, page 337](#)
- [Database Requirements, page 337](#)
- [Java Requirements, page 338](#)
- [Browser Requirements, page 338](#)
- [Hardware Requirements, page 339](#)
- [SonicWALL Appliance and Firmware Support, page 339](#)
- [Network Requirements, page 339](#)
- [MySonicWALL Account Requirements, page 340](#)

Operating System Requirements

In order to install and run SonicWALL ViewPoint, you must be logged in as the administrator. SonicWALL ViewPoint is supported on the following operating systems:

- Windows Server 2008 SBS, 64-bit
- Windows Server 2008 Standard (SP1), 32-bit and 64-bit
- Windows Server 2003 (SP2), 32-bit and 64-bit
- Windows Server 2000 (SP4)
- Windows 7, 32-bit and 64-bit
- Windows Vista (SP1), 32-bit and 64-bit
- Windows XP Professional (SP3), 32-bit

In all instances, SonicWALL ViewPoint runs as a 32-bit application.

Database Requirements

For fresh installations or after upgrading from 5.1, SonicWALL ViewPoint 6.0 supports the following database:

- MySQL 32-bit version 5.0.83 for Windows, bundled with SonicWALL ViewPoint 5.1 and above

The MySQL 5.0 separate installer that was provided with SonicWALL ViewPoint 5.0 is still supported.

The requirements for the MySQL server are as follows:

- Windows 2000 (SP4) and newer Windows operating systems
- Minimum 300 GB hard disk space
- Minimum 2 GB RAM
- NTFS file system
- Not a Virtual Machine (VM)

After upgrading from 5.1, SonicWALL ViewPoint 6.0 supports the following databases only when the database was already in use prior to upgrading:

- Microsoft SQL Server 2005 (SP2), 32-bit and 64-bit, as follows:
 - SQL Server 2005 Workgroup
 - SQL Server 2005 Standard
 - SQL Server 2005 Enterprise
 - SonicWALL ViewPoint does not support Microsoft SQL 2005 Express
- Microsoft SQL Server 2000 (SP4)
- Microsoft Desktop Engine (MSDE) bundled with ViewPoint

Java Requirements

Java Plug-in version 1.6 or higher is required on client machines when accessing the SonicWALL ViewPoint application interface. SonicWALL Universal Management Suite (UMS) automatically downloads the latest Java Plug-in. SonicWALL UMS services use JRE 1.6. For the Web server, SonicWALL UMS uses Tomcat 6.0.20.

Browser Requirements

- Microsoft Internet Explorer 6.0 or higher
- Mozilla Firefox 2.0 or higher
- Pop-up blocker disabled

SonicWALL ViewPoint supports SSL 3.0 / TLS 1.0 for HTTPS direct login to SonicWALL appliances from SonicWALL ViewPoint. For enhanced security across a SonicWALL ViewPoint network for installations that must comply with stringent regulatory compliance and account management controls as found in such standards as PCI, SOX, or HIPAA, the following browsers have SSL 3.0/TLS 1.0 as standard encryption protocols:

- Microsoft Internet Explorer 7.0 or higher

- Mozilla Firefox 2.0 or higher

Hardware Requirements

The hardware platform where SonicWALL ViewPoint is installed must meet the following requirements:

- x86 environment
- 3 GHz or faster single-CPU Intel processor
- Minimum 2 GB RAM
- At least 100 GB of free disk space



Note

Ensure that the drive where SonicWALL ViewPoint is installed has ample space to store the SonicWALL ViewPoint log files.

SonicWALL ViewPoint requires large amounts of disk space for database storage. In early versions, the maximum raw syslog database size was 2 GB. SonicWALL 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.

SonicWALL Appliance and Firmware Support

You can use SonicWALL ViewPoint reporting for the following SonicWALL security appliances:

- SonicWALL firewalls running SonicOS 1.0 or higher, or SonicWALL firmware 6.1.2.0 or higher
- SonicWALL SSL-VPN 200 / 2000 / 4000 running SonicOS SSL VPN 2.1 or higher
- SonicWALL SRA 4200 running SonicOS SSL VPN 3.5.0.11 or higher
- SonicWALL Aventail E-Class SRA EX-Series appliances running version 9.0 or higher
- SonicWALL CSM Series running SonicOS CF 1.0 or higher

Network Requirements

To complete the SonicWALL ViewPoint deployment process, the following network requirements must be met:

Syslog and SNMP Port Settings

You should either disable your personal firewall, or enable ports for syslog, syslog forwarding, and SNMP traps. The default syslog port is UDP 514 and the default SNMP port is UDP 162.

If the SonicWALL ViewPoint system is behind a gateway or firewall, you may need to open up these ports on that device.

Static IP / DHCP

If accessed from the WAN interface, the SonicWALL appliance must have a static IP address. Otherwise, it may have either a static or dynamic IP address.

HTTP / HTTPS

HTTP and HTTPS access for adding a SonicWALL appliance to ViewPoint is supported as follows:

- HTTP for access to a LAN IP address only
- HTTPS for access to a LAN IP or WAN IP address

MySonicWALL Account Requirements

A MySonicWALL account is required to complete the SonicWALL UMS installation and registration process. If you do not already have a MySonicWALL account, open a Web browser and navigate to the following website:

<http://www.mysonicwall.com>

Follow the on-screen prompts to create a user account.

Activating SonicWALL ViewPoint on Your Appliances

To use SonicWALL ViewPoint, you must license it on each SonicWALL security appliance for which you want reports. The SonicWALL appliance must be registered on MySonicWALL before you can purchase and activate the SonicWALL ViewPoint license for it. You must also enable the SonicWALL ViewPoint license on the appliance itself.

See the following sections:

- [“Registering Your SonicWALL Appliance” on page 341](#)
- [“Activating the ViewPoint Software on Your Appliance” on page 341](#)
- [“Enabling the ViewPoint License on Your Appliance” on page 342](#)

Registering Your SonicWALL Appliance

To register the SonicWALL appliance that ViewPoint will monitor, perform the following steps:

1. Log on to MySonicWALL.
2. Click **My Products**. The **SonicWALL My Products** page displays.

3. Enter your SonicWALL serial number in the **Serial Number** field.
4. Enter a descriptive name for the SonicWALL appliance in the **Friendly Name** field.
5. Select the **Product Group** from the drop-down list.
6. Click **Register**. The MySonicWALL website registers the SonicWALL appliance.

Activating the ViewPoint Software on Your Appliance

To activate the SonicWALL ViewPoint software, perform the following steps:

1. Log on to mysonicwall.com.
2. Click the label of the newly registered SonicWALL appliance. The Service Management page displays.
3. Scroll down to locate the ViewPoint service and click **Enter Key**. The Activate Service page displays.
4. Enter the ViewPoint Activation Key in the **Activation Key** field. The ViewPoint Activation Key is printed on the ViewPoint Software License Certificate shipped with the ViewPoint package. If you purchased ViewPoint on mysonicwall.com, the key is emailed to you.

5. Click **Submit**. After the Activation Key is registered, a ViewPoint License Key will appear. Carefully write down the ViewPoint License Key in a safe place.

Enabling the ViewPoint License on Your Appliance

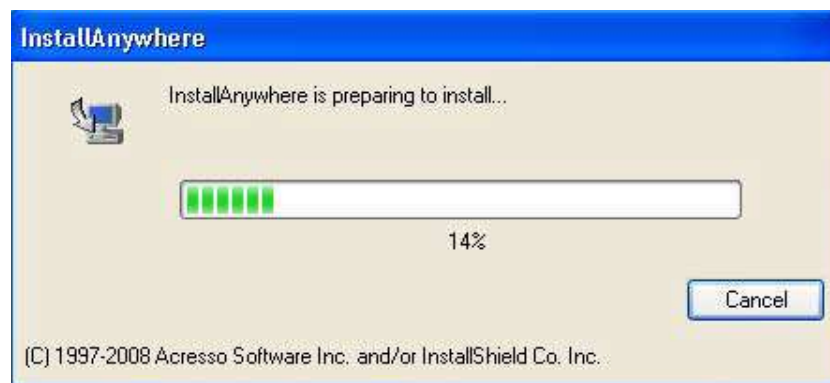
To enable the SonicWALL ViewPoint license, perform the following steps:

1. Log into the SonicWALL appliance.
2. Navigate to **Log > ViewPoint**. The **ViewPoint** page displays.
3. Enter the ViewPoint License Key provided by mysonicwall.com in the **Enter Upgrade Key** field.
4. Click **Apply**.
5. Restart the SonicWALL for the change to take effect.

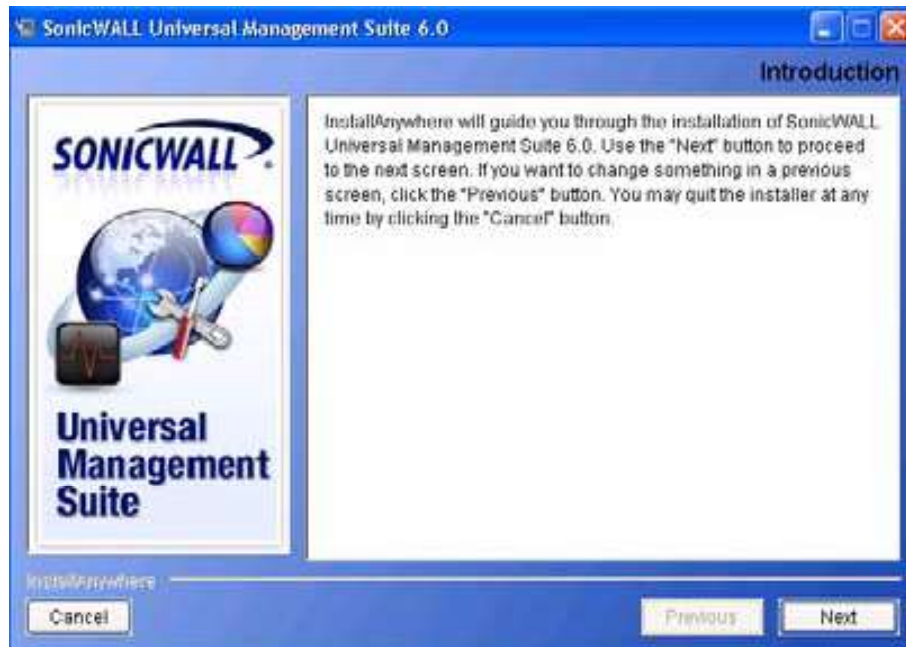
Installing Universal Management Suite

This section provides the procedures to install the SonicWALL Universal Management Suite (UMS) software. To install the SonicWALL UMS software, perform the following steps:

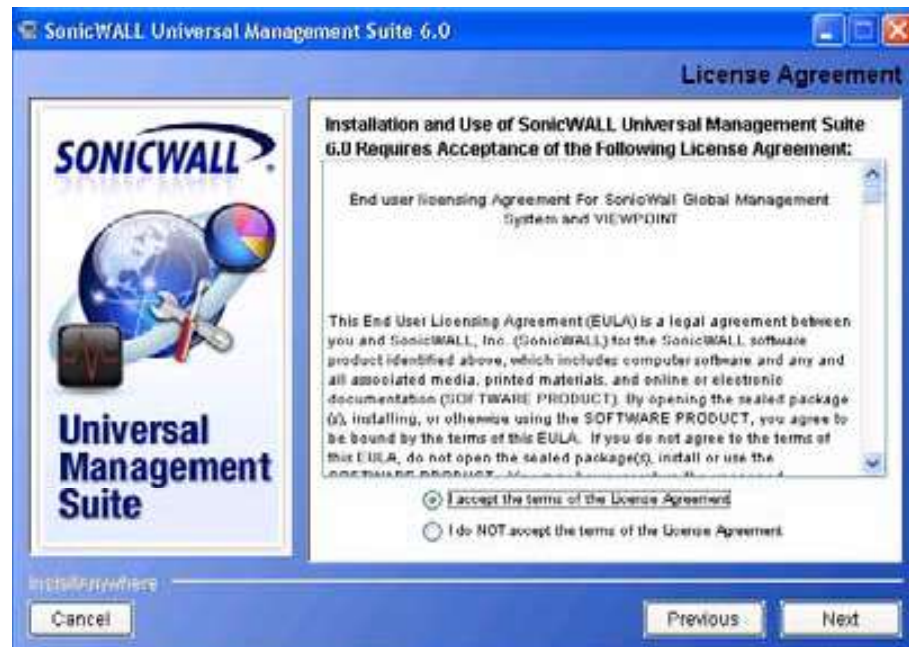
1. Log on to your SonicWALL ViewPoint management computer as **administrator** (Windows).
2. Run the SonicWALL ViewPoint installation file, **sw_gmsvp_win_eng_6.0.xxxx.xxxx.exe** (where “xxxx” represent the exact version numbers). It may take several seconds for the InstallAnywhere installer to initialize.



3. In the Introduction screen, click **Next**.



4. In the License Agreement screen, select the radio button next to **I accept the terms of the License Agreement**. Click **Next**.

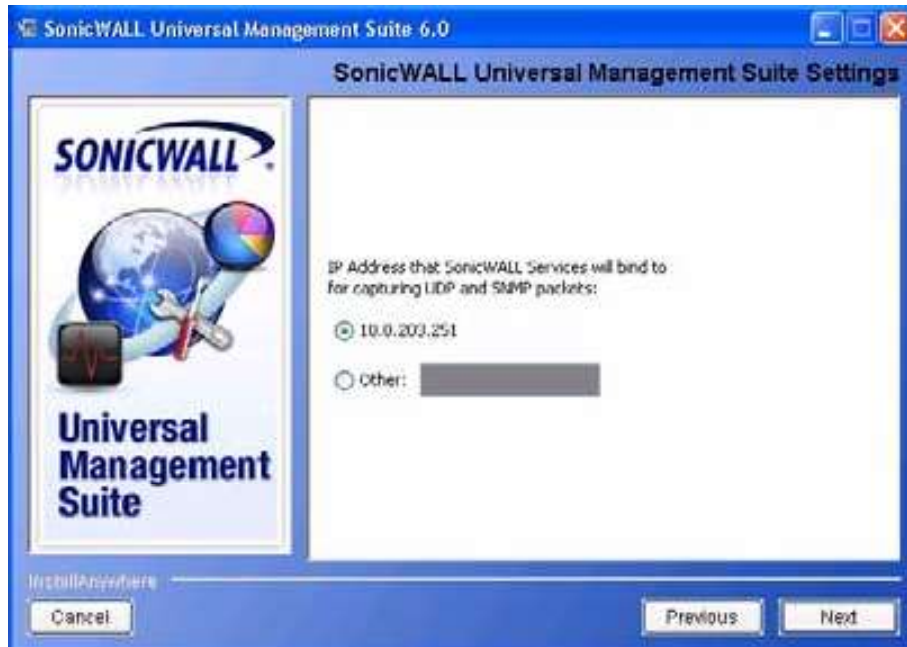


5. Select the path to the folder where you would like to install SonicWALL ViewPoint. You can accept the default path, **C:\GMSVP**, type in a new path, or click the **Choose** button to navigate to the selected folder. When you are finished, click **Next**.

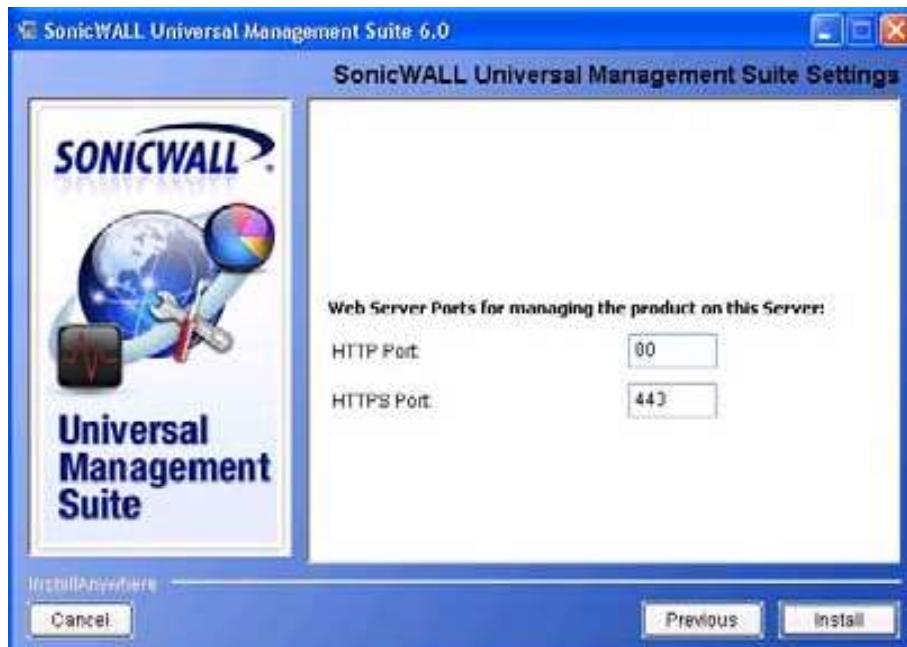
**Tip**

Do not include spaces in the SonicWALL ViewPoint installation path.

6. Select the IP address you want SonicWALL Services to bind to for capturing syslog and SNMP packets. The default is your management computer IP address. To provide a different IP address, select the radio button next to **Other** and enter the IP address. Click **Next**.



7. In the SonicWALL Universal Management Suite Settings window, enter the Web server ports for HTTP and HTTPS.



**Tip**

If you receive the message “Cannot bind to the port number specified. Please specify a different one,” the port you specified in **Web Server Port** is in use by another program, for example, Internet Information Services (IIS). Specify another unused Web server port, for example, 8080.

**Tip**

If you specify a custom port, you will need to modify the URLs you use to access SonicWALL ViewPoint by using the following format:
http://localhost:<port>/sgms/login (to login from the local host) or
http://<host_ipaddress>:<port>/sgms/login (to login from a remote location). For example, if you specified port 8080, the URL would be
http://localhost:8080/sgms/login for a local host login, or
http://10.0.93.20:8080/sgms/login for a remote login.

8. Click **Install**. You may see a Windows Firewall security alert. If you do, click **Unblock**.



9. The Installer displays the installation progress during the few minutes required. Upon completion, whether or not the system has Windows Firewall enabled, a dialog is displayed notifying you to either disable the firewall or manually open the syslog and SNMP ports, and to ensure that these ports are open on your network gateway or firewall. Click **OK**.



10. The Important Registration Information screen provides the URL and credentials to use to access the SonicWALL ViewPoint Universal Management Host system interface after restarting your system, as well as information about registration.

The default URL for accessing the interface from the local system is:

http://localhost:80/

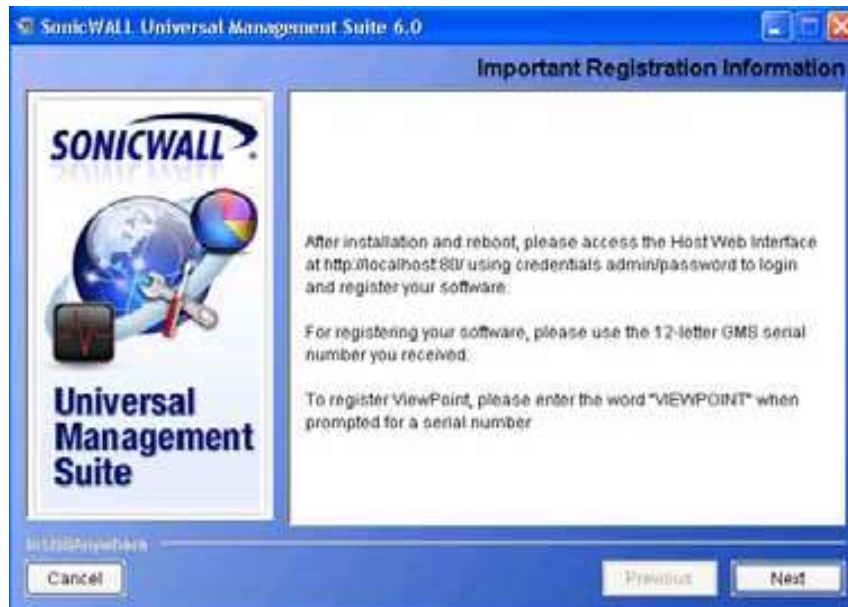
The default credentials are:

User name – **admin**

Password – **password**

To register for a SonicWALL ViewPoint installation, enter the word **VIEWPOINT** instead of a serial number when you register the product on MySonicWALL.

Click **Next**.

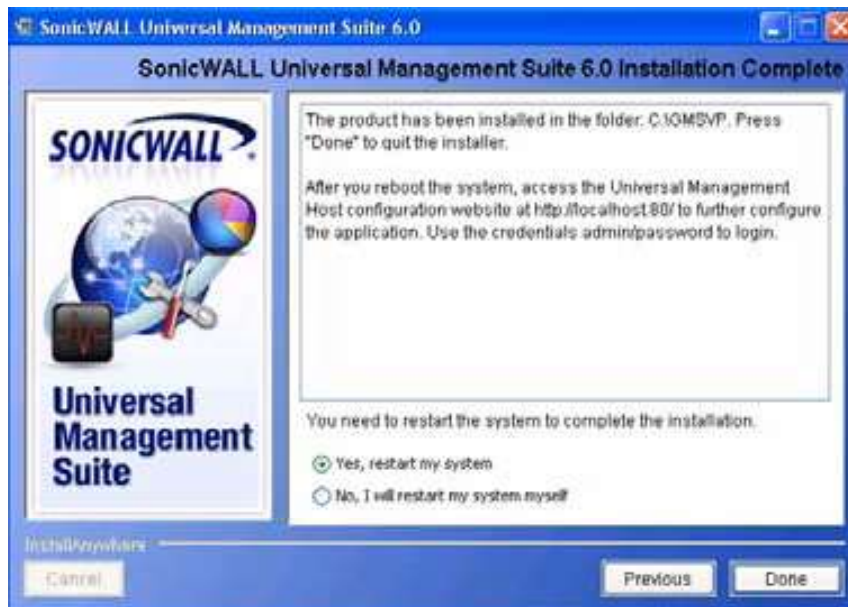


11. In the Installation Complete screen, select one of the following options for restarting your system to complete the installation, and then click **Done**:
- Yes, restart my system
 - No, I will restart my system myself



Note

Restarting after installation is required for full functionality.



12. After restarting your system, you can access the SonicWALL ViewPoint UMH system interface by either clicking on the new desktop shortcut for **SonicWALL Universal Management Suite 6.0** or by pointing your browser at **http://localhost:80/**.
13. Your default Web browser will launch **http://localhost:80/appliance/login**.
14. Login using the username **admin** and the password **password**.
15. You will be prompted to change your password.

**Note**

You are forced to change your password the first time you login.

Upgrading SonicWALL ViewPoint 5.1 to 6.0

To upgrade from SonicWALL ViewPoint 5.1 to 6.0 using the the Universal Management Suite 6.0 single binary installer, perform the following steps:

1. Log on to your SonicWALL ViewPoint management computer as **administrator** (Windows). Launch the SonicWALL Universal Management Suite 6.0 installer, by double-clicking the file **sw_gmsvp_win_eng_6.0.xxxx.xxxx.exe** (where “xxxx” represent the exact version numbers). It may take several seconds for the InstallAnywhere self-extractor to initialize.
2. In the Introduction screen, click **Next**.
3. In the License Agreement screen, select the radio button next to **I accept the terms of the License Agreement**. Click **Next**.
4. When the installer detects that SonicWALL ViewPoint 5.1 is currently installed on the system, a notification is displayed. Click **Install** to continue the upgrade.
5. The installer begins installing the files, using the existing installation folder, IP address to which SonicWALL Services bind for capturing syslog and SNMP packets, and Web port settings.

6. The Installer displays the installation progress during the few minutes required. Upon completion, whether or not the system has Windows Firewall enabled, a dialog is displayed notifying you to either disable the firewall or manually open the syslog and SNMP ports, and to ensure that these ports are open on your network gateway or firewall. Click **OK**.



7. The Important Registration Information screen provides the URL for access to the SonicWALL ViewPoint Universal Management Host system interface after upgrade completion, as well as information about registration.

The default URL for accessing the interface from the local system is:

http://localhost:80/

The default credentials are:

User name – **admin**

Password – **password**

To register for a SonicWALL ViewPoint installation, enter the word **VIEWPOINT** instead of a serial number when you register the product on MySonicWALL.

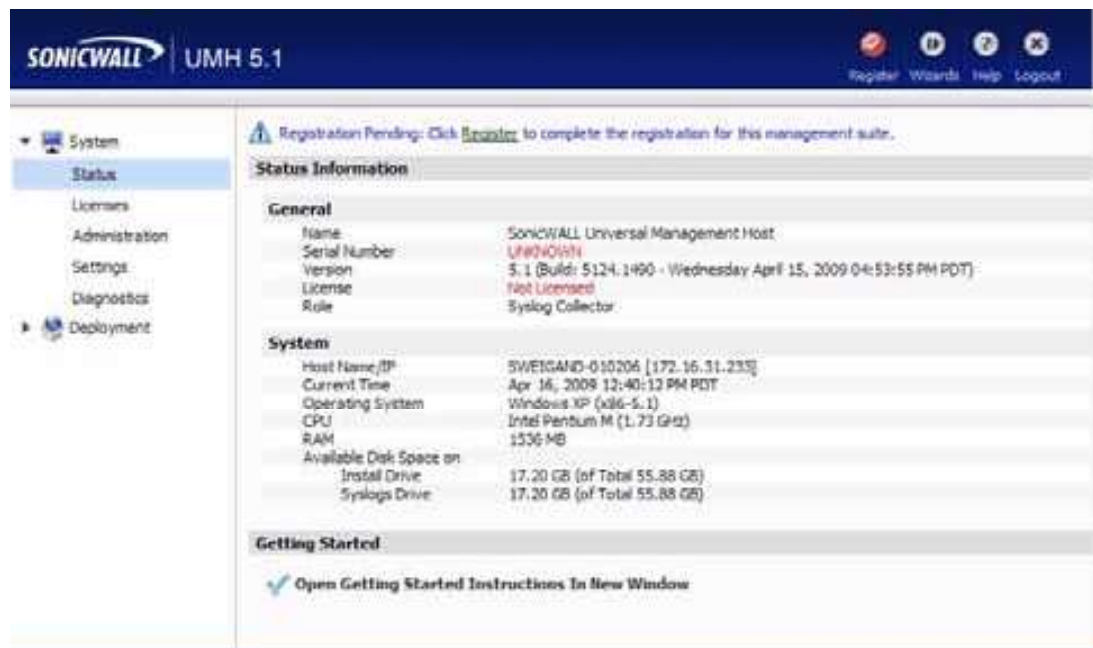
Click **Next**.

8. The final installer screen contains the path of the installation folder, and warns you that the Universal Management Suite Web page will be launched next. Click **Done**.

In the SonicWALL ViewPoint login page, enter the same credentials for **User** and **Password** that you had in your earlier version prior to the upgrade.

Registering SonicWALL ViewPoint

SonicWALL ViewPoint registration is performed using the Universal Management Host system management interface. The first time you log into the system interface, the System > Status page will display a **Registration Pending** notification at the top of the screen, and the **Register** button will be available in the top right corner of the interface.



SonicWALL ViewPoint must be registered before you can use it. To complete registration, SonicWALL ViewPoint must have access to the Internet. The SonicWALL ViewPoint registration process sends your registration information to the MySonicWALL registration site. When registration is completed, SonicWALL ViewPoint will be licensed on your system.



Note MySonicWALL registration information is not sold or shared with any other company.

To register SonicWALL ViewPoint, perform the following steps:

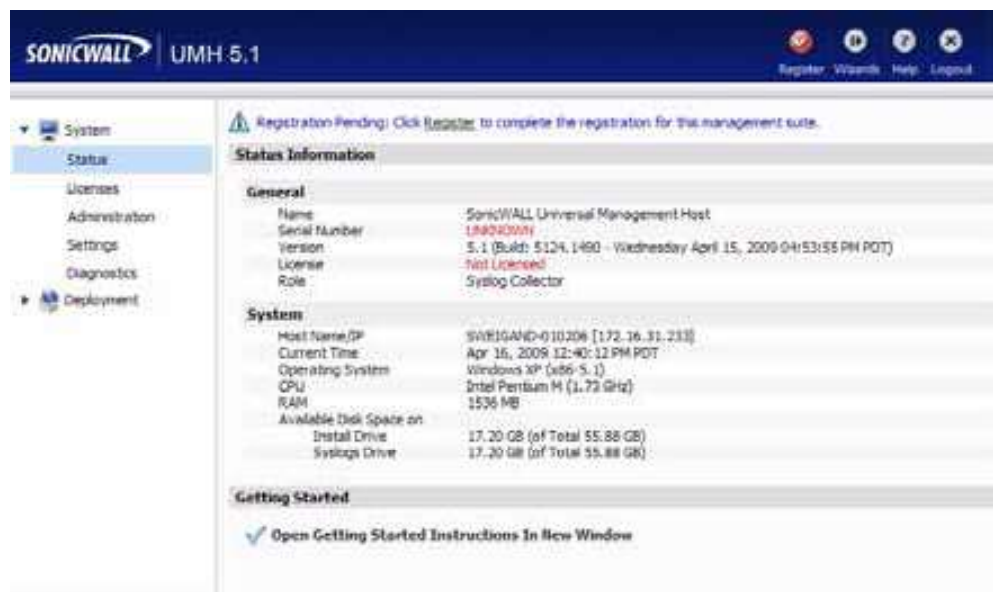
1. In a browser, log in to the system management interface (**<http://<host>:80/appliance/login>**). If this is the first time you have logged in after running the Installer and rebooting, you will be required to change the password for the admin account. Enter the new password in the appropriate fields and then click **Submit**.

2. If the software detects that the Windows Firewall is enabled on the system, a warning dialog box is displayed on top of the System > Status page. To receive syslog and SNMP packets, either disable the Windows Firewall or configure it to open these ports (default syslog port UDP 514 and default SNMP port UDP 162). When ready, click **OK**.

Optionally, you can select the **Perform this check after 30 days** checkbox if you do not plan to disable the Windows Firewall immediately, and do not wish to see this warning every time you login. The check for Windows Firewall cannot be disabled completely, and if you leave it running you will see this alert after the 30-day delay. You can repeat the delay as many times as needed.



3. In the System > Status page, click the **Register** button.



4. In the License Management page, type your MySonicWALL user name and password and then click **Submit**.

SONICWALL UMH 5.1

Register Wards Help Logout

License Management

Serial Number: None

mySonicWALL.com Login

mySonicWALL.com is a one-stop resource for registering all your SonicWALL Internet Security Appliances and managing all your SonicWALL security service upgrades and changes. mySonicWALL provides you with an easy to use interface to manage services and upgrades for multiple SonicWALL appliances. For more information on mySonicWALL, please visit the [FAQ](#). If you do not have a mySonicWALL account, please click [here](#) to create one.

Please enter your existing mySonicWALL.com username (or email address) and password below:

Email Address/User Name:

Password:

Did you forget your User Name or Password? Go to <https://www.mysonicwall.com> for help.

5. In the next License Management page, type **VIEWPOINT** (all capital letters) into the **Serial Number** field and leave the **Authentication Code** fields blank. Type a descriptive name for the system into the **Friendly Name** field and then click **Submit**.

License Management

Serial Number: None

Enter your 12 character Software Serial Number, Authentication Code and a Friendly Name
For ViewPoint: Enter VIEWPOINT as Serial Number and ignore Authentication Code

[Click here](#) if you have an 8 character Serial Number

Serial Number:

Authentication Code: [What is this?](#)

Friendly Name:



Note

The Friendly Name for this system will also be used as the name for the SonicWALL ViewPoint deployment. As you register SonicWALL appliances on MySonicWALL, you will have the option of adding them to this deployment for SonicWALL ViewPoint reporting.

6. In the next License Management page, click **Continue**. This completes the registration process.



When registration is complete, the **Deployment > Roles** page is displayed. Although there is only one possible role for a SonicWALL ViewPoint deployment, you must still configure certain fields on this page and then click **Update** to fully activate the application. For instructions on configuring these settings, see the [“Configuring the Deployment Role” section on page 32](#).

Configuring Deployment Settings

This section describes the settings available on the **Deployment > Settings** page of the UMH system management interface, available by default at:
<http://localhost/appliance>

Configuring Web Port Settings

To change the Web port settings, perform the following steps:

1. On the **Deployment > Settings** page under **Web Port Configuration**, to use a different port for HTTP access to the SonicWALL ViewPoint, type the port number into the **HTTP Port** field. The default port is 80.



2. To use a different port for HTTPS access to the SonicWALL ViewPoint, type the port number into the **HTTPS Port** field. The default port is 443.
3. Click **Update** to apply the Web port settings.



Note Changing the Web port settings will cause the system to restart.

4. After the appliance restarts, use the new port to access the “appliance” or SonicWALL ViewPoint management interface. For example:
 - If you changed the HTTP port to 8080, use the URL:
http://<IP Address>:8080/appliance/
 - If you changed the HTTPS port to 4430, use the URL:
http://<IP Address>:4430/appliance/

Configuring SMTP Settings

The SMTP settings are used for sending email alerts to the SonicWALL ViewPoint administrator. To configure the SMTP settings, perform the following steps:

1. On the **Deployment > Settings** page under **SMTP Configuration**, enter the IP address of the SMTP server into the **SMTP server** field.



2. In the **Sender address** field, enter the email address that will appear as the ‘From’ address when email alerts are sent to the administrator.
3. In the **Administrator address** field, enter a valid email address for the administrator who will receive email alerts.
4. Click **Update** to apply the SMTP settings.

Upgrading from ViewPoint to GMS

SonicWALL ViewPoint installations have the option of upgrading to SonicWALL GMS without reinstalling. You can start a 30-day Free Trial of SonicWALL GMS by clicking a button or link in either the ViewPoint or Universal Management Host interface and following a simple procedure. When you are ready to finalize the upgrade, your SonicWALL reseller can provide you with the license key for a seamless transition to SonicWALL GMS.

When five or more registered devices are connected to SonicWALL ViewPoint reporting, the **Try GMS Free - 30 Days** button appears next to the tabs at the top of the SonicWALL ViewPoint management interface.



You can also start the Free Trial by clicking **Manage Licenses** on the **System > Licenses** page of the Universal Management Host interface, and then clicking the **Try** link.



For details on enabling the SonicWALL GMS Free Trial and purchasing the SonicWALL GMS upgrade license, see the following sections:

- [“Enabling the GMS Free Trial from ViewPoint” section on page 357](#)
- [“Enabling the GMS Free Trial from the UMH Interface” section on page 359](#)
- [“Completing the Free Trial Upgrade” section on page 360](#)
- [“Configuring Appliances for GMS Management” section on page 364](#)
- [“Purchasing a SonicWALL GMS Upgrade” section on page 366](#)

Enabling the GMS Free Trial from ViewPoint

When five or more devices are connected to SonicWALL ViewPoint reporting, the **Try GMS Free - 30 Days** button appears next to the tabs at the top of the SonicWALL ViewPoint management interface.

To find out how many devices your SonicWALL ViewPoint installation is handling, log in to MySonicWALL and navigate to the **My Products** page. Click on the link for your SonicWALL ViewPoint installation to get to the **Service Management** page, and scroll to the bottom. You will see the list of appliances under **Associated Products**.

To enable the 30-day SonicWALL GMS Free Trial from the SonicWALL ViewPoint management interface, perform the following steps:

1. In the SonicWALL ViewPoint management interface, click the **Try GMS Free - 30 Days** button next to the tabs at the top of the page.



2. The Viewpoint Upgrade Tool launches and guides you through the process of installing the Free Trial or Upgrade. The tool displays the **Upgrade Requirements – Licensing** screen. Before migrating to GMS 5.1, ensure that all appliances under Viewpoint reporting are registered to the same MySonicWALL account. Follow the steps provided in the screen, and then click **Proceed**.



- The **Upgrade Requirements – System** screen displays the recommended operating system, database, and hardware system requirements. Click **Proceed**.

Upgrade Requirements - System

Please check the recommended system requirements below to make sure your system is qualified for upgrading to be an all-in-one GMS system. Click "Proceed" to start the upgrade procedure.

Recommended System Requirements

Operating System	Microsoft® Environment: Windows 2000 Server (SP4), Windows 2000 Professional (SP4), Windows XP Professional (SP2), Windows 2003 Server (SP2)
Database	Microsoft® Environment: Microsoft SQL Server 2000 (SP4) and Microsoft SQL Server 2005 (SP2) on either Windows 2000 Server (SP4) or 2003 Server (SP4)
Hardware	x86 Environment: Minimum 3 GHz processor dual-core CPU Intel processor, 2 GB RAM, and 300 GB disk space

Current System Information

Operating System	Windows XP (x86-6.1)
CPU	2.927 GHz
RAM	2,000 GB

- The ViewPoint Upgrade Tool displays the login screen for MySonicWALL. Enter your MySonicWALL credentials and click **Submit**.

ViewPoint Upgrade Tool

Step 1. Upgrade the License
Use the license upgrade screen provided below to upgrade the license from Viewpoint to GMS

mySonicWALL.com Login

mySonicWALL.com is a one-stop resource for registering all your SonicWALL Internet Security Appliances and managing all your SonicWALL security service upgrades and changes. mySonicWALL provides you with an easy to use interface to manage services and upgrades for multiple SonicWALL appliances. For more information on mySonicWALL please visit the [FAQ](#). If you do not have a mySonicWall account, please click [here](#) to create one.

Please enter your existing mySonicWALL.com username (or email address) and password below:

Email Address/User Name:

Password:

Did you forget your User Name or Password? Go to <https://www.mysonicwall.com> for help.

5. In the next ViewPoint Upgrade Tool page, click the **Try** link in the **Free Trial** column for Global Management System.



6. From this point, the upgrade process continues with the same steps for access from either the SonicWALL ViewPoint interface or the Universal Management Host interface. To continue the procedure, perform the steps in the [“Completing the Free Trial Upgrade”](#) section on page 360.

Enabling the GMS Free Trial from the UMH Interface

To enable the 30-day Free Trial of SonicWALL GMS from the Universal Management Host interface on your SonicWALL ViewPoint system, perform the following steps:

1. In the Universal Management Host interface, navigate to the System > Licenses page and click **Manage Licenses**.



2. If you are not already logged into MySonicWALL, the MySonicWALL login screen is displayed. Enter your MySonicWALL credentials in the appropriate fields and log in.

- On the next page, click the **Try** link in the **Free Trial** column for Global Management System.



- From this point, the upgrade process continues with the same steps for access from either the SonicWALL ViewPoint interface or the Universal Management Host interface. To continue the procedure, perform the steps in the [“Completing the Free Trial Upgrade”](#) section on page 360.

Completing the Free Trial Upgrade

This procedure provides the common upgrading steps for access from either the SonicWALL ViewPoint interface or the Universal Management Host interface. To get to this point in the process, follow the steps described in one of the two preceding sections:

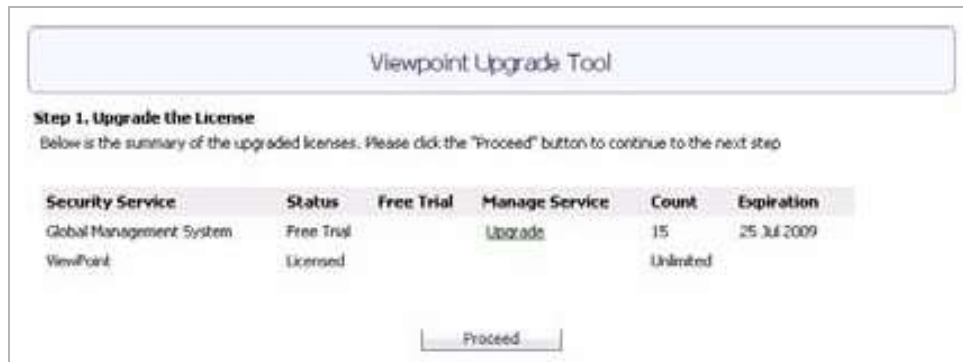
- “Enabling the GMS Free Trial from ViewPoint” section on page 357
- “Enabling the GMS Free Trial from the UMH Interface” section on page 359

To continue the upgrade, perform the following steps:

- In the ViewPoint Upgrade Tool page, click the **Continue** button.



2. The next screen provides a summary of GMS and ViewPoint status. Verify that the **Try** link for the Free Trial is gone and only the **Upgrade** link remains. The **Expiration** column displays the expiration date of your Free Trial. You can click the **Upgrade** link at any time during the Free Trial to purchase the SonicWALL GMS upgrade. Click **Proceed**.



3. In the next ViewPoint Upgrade Tool page, you begin the configuration for SonicWALL GMS instep 2 of the upgrade process. This page displays two sections:
 - Automatic Configuration** – Contains a list of SonicWALL UTM or CSM appliances in your ViewPoint installation. These appliances will be automatically configured for SonicWALL GMS management.
 - Manual Configuration** – Contains a list of SonicWALL Aventail, SSL-VPN, or CDP appliances in your ViewPoint installation. You must manually configure these appliances for SonicWALL GMS management. See the [“Configuring Appliances for GMS Management”](#) section on page 364 for detailed instructions on enabling SonicWALL GMS management on these appliances.

When ready, click **Proceed**.

ViewPoint Upgrade Tool

Step 2: GMS Configuration

Two sections are involved in this step. "Auto Configuration" lists out the appliances that are auto-configurable to support GMS. The related scheduled tasks will be created when proceed to the next step. "Manual Configuration" lists out appliances and information to help users manually configure those appliances to support GMS.

Automatic Configuration

Following list shows all the UTM appliances currently in the system. These appliances can be automatically configured to support GMS.

Appliance Name	Appliance Serial Number
NSA 240	0017C5269510
NSA 5500	0017C51C655C

Manual Configuration

Following list shows all the non-UTM appliances currently in the system. These appliances need manual configuration to support GMS.

Appliance Name	Appliance Serial
Eng Test	0006B1275C34

Configuration Information

Proceed

- When the configuration finishes, the ViewPoint Upgrade Tool displays the completion dialog box. Click **Close** to log out of the console and restart the system.

Viewpoint Upgrade Tool

You have complete the upgrade procedure.
please click "Close" button to logout the console and reboot the box

close

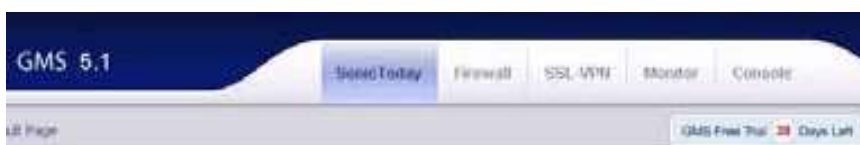
SONICWALL

5. The GMS login page appears and requests that you reboot the system. Reboot the system. If a reboot is not performed, you may encounter problems with the correct IP Address appearing.

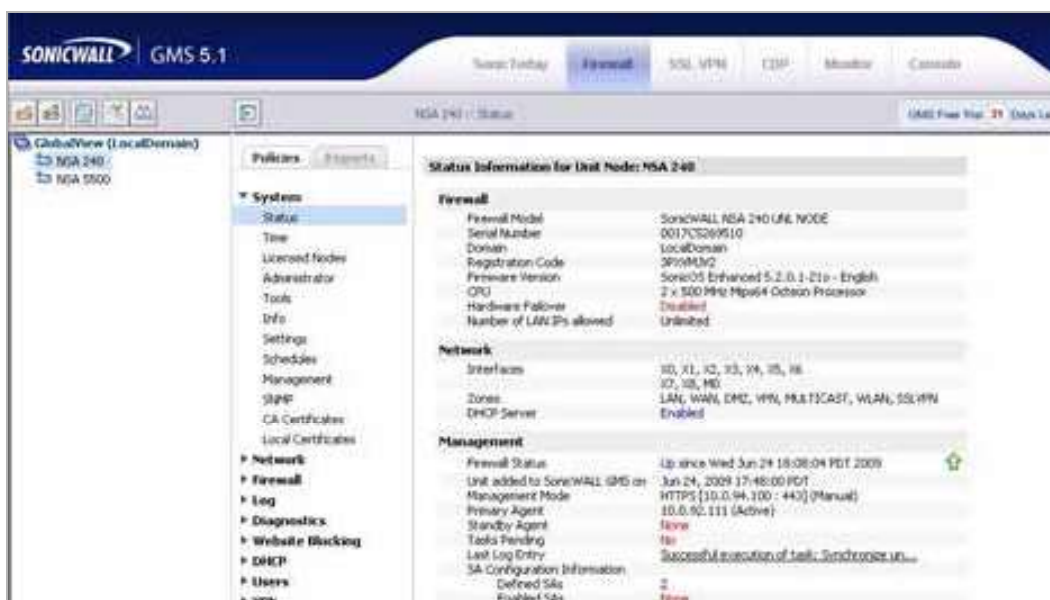


6. After rebooting, log in with your ViewPoint credentials.

When you log in, you will see a button displaying the number of days left in your Free Trial at the top of the page.



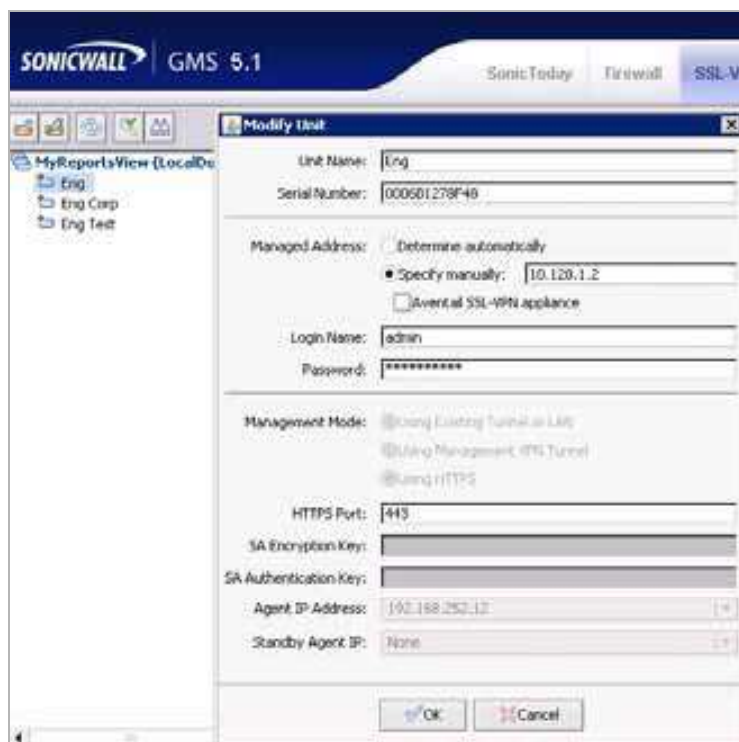
7. On the System > Status page for connected appliances, you can view the log entries for task synchronization and automatic addressing mode, related to the GMS configuration.



Configuring Appliances for GMS Management

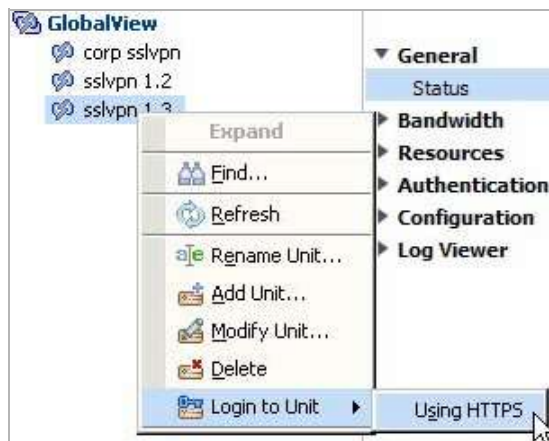
To manually configure the appliances listed in the Manual Configuration section of the ViewPoint Upgrade Tool page (see Step 3. on page 361), perform the following steps for each appliance:

1. In the SonicWALL GMS management interface, click the tab at the top of the page that corresponds to the type of appliance, such as **SSL-VPN** or **CDP**.
2. In the left pane, right-click one of the listed appliances and select **Modify Unit**.
3. In the Modify Unit screen in the right pane, copy the appliance IP address in the **Managed Address** section to your clipboard, or make a note of it.

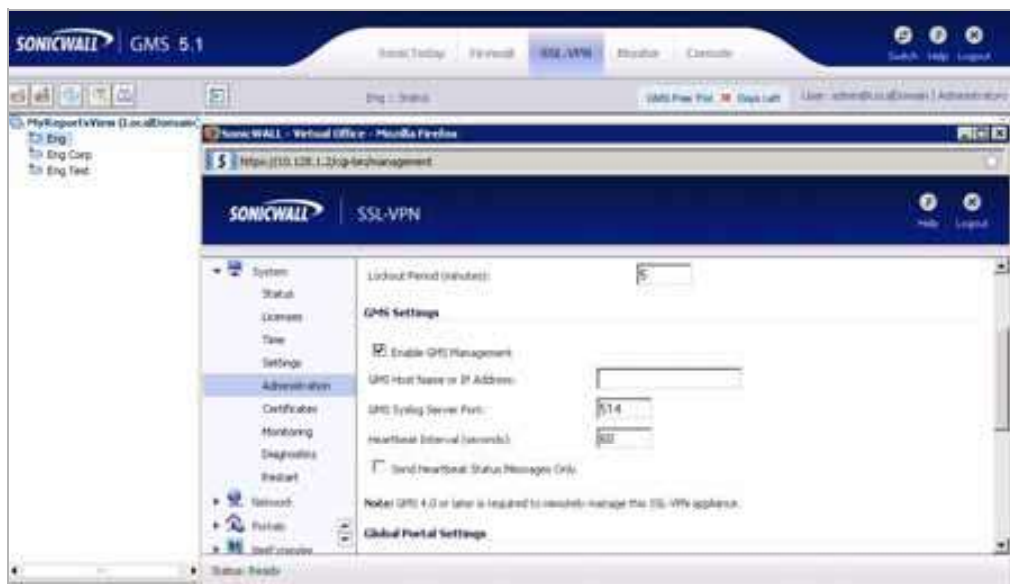


4. Click **Cancel**.

5. In the left pane, right-click the same appliance and select **Login to Unit > Using HTTPS**.



6. In the appliance management interface, navigate to the **System > Administration** page.



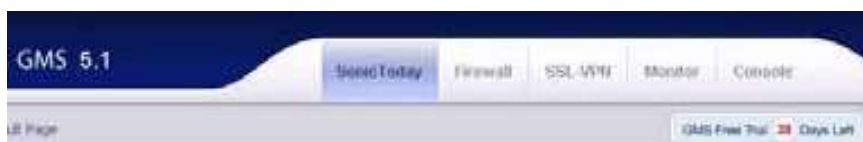
7. Under **GMS Settings**, select the **Enable GMS Management** checkbox, or verify that it is selected.
8. In the **GMS Host Name or IP Address** field, paste or type the appliance IP address that you obtained from the Modify Unit screen in Step 3.
9. Click the **Accept** button at the top of the appliance interface screen.
10. Click the **Logout** button in the top right corner of the appliance interface screen.
11. Repeat these steps for each appliance listed in the Manual Configuration section of the ViewPoint Upgrade Tool page.

Purchasing a SonicWALL GMS Upgrade

You can purchase an upgrade to SonicWALL GMS at any time during the 30-day Free Trial.

To purchase the SonicWALL GMS license, perform the following steps:

1. In the SonicWALL GMS interface, click the **GMS Free Trial X Days Left** button, where X is the number of days left in the Free Trial.



2. In the **Buy GMS** page, click **I want to upgrade to GMS now**.



3. The Console > Licenses > Product Licenses page is displayed. Click **Manage Licenses**.



4. In the next page, in the **Manage Service** column for Global Management System, click the **Upgrade** link.



5. The next page has **Serial Number** and **Authentication Code** fields for SonicWALL GMS. You must contact your SonicWALL reseller to complete the purchase and obtain the 12-character serial number and authentication code. Type in the values to the **Serial Number** and **Authentication Code** fields.

The screenshot shows the 'License Summary' page with input fields for 'Serial Number', 'Authentication Code', 'Friendly Name', and 'GMS upgrade keys'. A 'Submit' button is at the bottom right. A note indicates that GMS upgrade keys are required if the current ViewPoint installation is larger than a retail upgrade.

6. Enter a descriptive name for the SonicWALL GMS installation into the **Friendly Name** field. This name will appear in your MySonicWALL account.
7. If your SonicWALL ViewPoint installation currently handles more than 10 appliances, when you upgrade to SonicWALL GMS you will need to purchase additional SonicWALL GMS license(s) to manage the extra appliances. The standard “10-node” SonicWALL GMS license provided with the Free Trial supports up to 10 managed appliances. Enter the license keys for any additional SonicWALL GMS licenses into the **GMS upgrade keys** text box, one key per line.
8. Click **Submit**. The License page is displayed, showing that SonicWALL GMS is now licensed.

Miscellaneous Procedures and Troubleshooting Tips

This section contains miscellaneous SonicWALL ViewPoint procedures and troubleshooting tips.

Miscellaneous Procedures

This section contains information on procedures that you may need to perform. Select from the following:

- It is highly recommended that you regularly back up the SonicWALL ViewPoint data. For more information, see [“Backing up SonicWALL ViewPoint Data”](#) on page 368.
- SonicWALL ViewPoint requires Mixed Mode authentication when using SQL Server 2000. To change the authentication mode, see [“Changing the SQL Server Authentication Mode”](#) on page 369.
- If you are reinstalling SonicWALL ViewPoint, preserving the previous configuration settings can save a lot of time. To reinstall SonicWALL ViewPoint using an existing SonicWALL ViewPoint database, see [“Reinstalling SonicWALL ViewPoint Using an Existing Database”](#) on page 369.
- If you need to uninstall SonicWALL ViewPoint from a server, it is important to do it correctly. To uninstall SonicWALL ViewPoint, see [“Uninstalling SonicWALL Universal Management Suite and Its Database”](#) on page 369.

Backing up SonicWALL ViewPoint Data

SonicWALL ViewPoint stores its configuration data in the SGMSDB database. It is important to back up this database and the individual SonicWALL ViewPoint databases (sgmsvp_yyyy_mm_dd) on a regular basis.

The Console > Management > Database Maintenance page provides the necessary support for backing up and restoring the MySQL database that is bundled with SonicWALL UMS. For more information, see the [“Database Maintenance”](#) section on page 66.

If you are using SQL Server, this can be accomplished by backing up the entire SQL Server using the database backup tool. When using this tool, there is no need to stop the SonicWALL ViewPoint services for database backup. However, make sure that the backup occurs when SonicWALL ViewPoint activity is the lowest and that the backup operation schedule does not clash with the SonicWALL ViewPoint scheduler.

**Note**

It is also recommended to regularly back up the entire contents of the SonicWALL ViewPoint directory, the sgmsConfig.xml file.

Changing the SQL Server Authentication Mode

SonicWALL ViewPoint requires the Mixed Mode authentication mode. To change the authentication mode from Windows Mode to Mixed Mode, follow these steps:

1. Start the Microsoft SQL Server Enterprise Manager.
2. Right-click the appropriate SQL Server Group and select **Properties** from the pop-up menu.
3. Click the **Security** tab.
4. Change the Authentication mode from **Windows only** to **SQL Server and Windows**.
5. Click **OK**.

Reinstalling SonicWALL ViewPoint Using an Existing Database

If you need to reinstall SonicWALL ViewPoint, but want to preserve the settings in an existing SonicWALL ViewPoint database, follow these steps:

1. Install a new database, using the same username and password that you used for the existing SonicWALL ViewPoint database.
2. Install SonicWALL ViewPoint using this new database.
3. Stop all SonicWALL ViewPoint services.
4. Open the sgmsConfig.xml and web.xml files with a text editor. Change the values for the dbhost and dburl parameters to match the existing SonicWALL ViewPoint database.
5. Restart the SonicWALL ViewPoint services.
6. Uninstall the new database.

Uninstalling SonicWALL Universal Management Suite and Its Database

This section describes how to uninstall SonicWALL Universal Management Suite and its components. Select from the following:

- To uninstall SonicWALL Universal Management Suite on the Windows platform, see [“Windows”](#) on page 370.

- To uninstall SonicWALL Universal Management Suite databases from Microsoft SQL Server 2000, see [“MS SQL Server 2000”](#) on page 370.

Windows

To uninstall SonicWALL Universal Management Suite from a Windows system, follow these steps:

1. Click **Start**, point to **Settings**, and click **Control Panel**.
2. Double-click **Add/Remove Programs**. The Add/Remove Programs Properties window displays.
3. Select **SonicWALL Universal Management Suite** and click **Change/Remove**. The SonicWALL Universal Management Suite Uninstall program starts.
4. Follow the on-screen prompts.
5. Restart the system. SonicWALL Universal Management Suite is uninstalled.

MS SQL Server 2000

To uninstall or remove the SonicWALL Universal Management Suite databases in the MS SQL Server 2000, you can execute the following DOS command from any SonicWALL Universal Management Suite server:

```
osql -U username -P password -S dbHost_IP -q "drop database SGMSDB"  
osql -U username -P password -S dbHost_IP -q "drop database sgmsvp_yyyy_mm_dd"
```

Or you can use the MS SQL Server's Enterprise Manager and delete the SGMSDB and sgmsvp_ databases.

Troubleshooting Tips

This section contains SonicWALL ViewPoint troubleshooting tips.

Changing the Default Syslog Server Port Number

By default, the SonicWALL ViewPoint syslog server default port number is 514 on Windows systems. To change the port number, follow these steps:

1. Open the sgmsConfig.xml file with a text editor.
2. Add the following line to the end of the file before the `</Configuration>` section:
Parameter name="syslog.syslogServerPort" value="*port_number*"
where *port_number* is the new port number.
3. Save the file and exit.

Installing the Java Plug In

You need Java Plug-in 1.6 or later to access the SonicWALL ViewPoint management interface.



Tip

The Java Plug-in is automatically installed during the SonicWALL ViewPoint installation. However, you can manually install the Java Plug-in by following these steps.

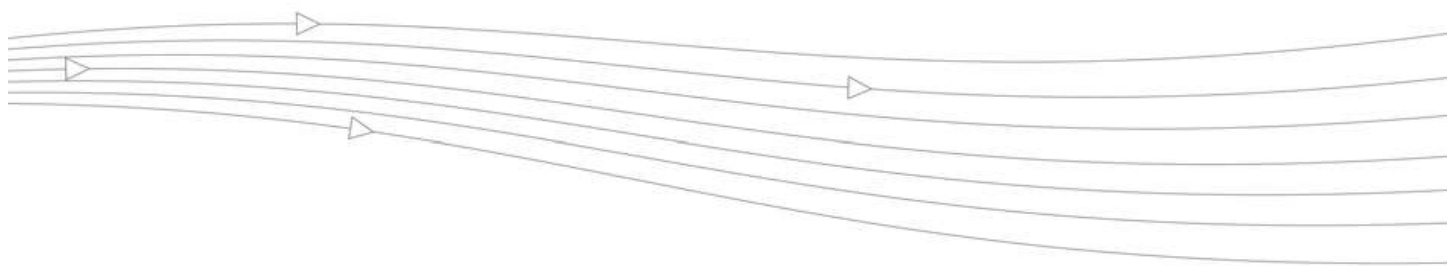
To manually install the Java Plug-in, perform the following steps:

1. Download the installer from the Internet at:

<http://java.sun.com/javase/downloads/index.jsp>



2. Execute the installer.
3. Select the radio button next to **Accept the Terms of the License Agreement**. Click **Next**.
4. Select the radio button next to **Typical** installation and click **Next**.
5. It may take several minutes for the Java Plug-in to install.
6. In the Installation Complete window, click **Finish**.
 - Restart your computer to complete the installation process.



Appendix B

Technical Tips

This chapter includes the following sections:

- [“Log Viewer” section on page 373](#)
- [“Real-time Syslog Viewer” section on page 375](#)
- [“Forwarding Syslog Data to Another Syslog Server” section on page 376](#)
- [“Posting ViewPoint Reporting to Another Web Server for End-User Access” section on page 377](#)

Log Viewer

The Log Viewer contains detailed information on each transaction that occurred on the SonicWALL appliance. This information is stored for the time that you specified in the configuration settings.



Note

The Log Viewer displays raw log information for every connection. Depending on the amount of traffic, this can quickly consume a large amount of space in the database. It is highly recommended to be careful when choosing the number of days of information that will be stored. For information about setting the number of days data is stored, see [“Enabling Report Table Sorting”](#) on page 72.

To configure Log Viewer settings for generating a report, perform the following steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **UTM** or **SSL-VPN** tab.

3. Select a SonicWALL appliance.
4. Expand the **Log Viewer** tree and click **Search**. The Search page displays. Log Viewer must be enabled for the appliance in order to display all the fields on the page.

5. Select **Enable Log Viewer** and then click **Update** to turn on collection of raw data in the database and enable viewing of that log data. This can consume a large amount of space in your database. Review your database space constraints before enabling the log viewer. The maximum number of appliances for which Log Viewer can be enabled is controlled on the Console > Reports > Settings page. See [“Controlling the Number of Appliances with Log Viewer Enabled” on page 72](#).



Note Custom Reports are available on appliances with Log Viewer enabled. See [“Using Custom Reports on UTM Appliances” on page 163](#).

6. Select the starting date to view from the **Start Date** list box.
7. Enter the starting time of events to view in the **Start Time** field.
8. Select the ending date of events to view in the **End Date** list box.
9. Enter the ending time of events to view in the **End Time** field.
10. Enter the source IP address to view in the **Source IP Address** field. To view all IP addresses, enter All.
11. Optionally enter the source port to view in the **Source Port** field.
12. Enter the destination IP address to view in the **Destination IP Address** field. To view all IP addresses, enter All.

13. Optionally enter the destination port to view in the **Destination Port** field.
14. Select the type of events to view from the **Message Category** list box.
15. To search for specific message text, type the text into the **Message Text** field.
16. Select the number of entries to display per page from the **Results Per Page** field.
17. Click **Generate Report**. The Log Viewer Results page displays.

Log Search Results for July 26, 2006 15:55:20 to July 26, 2006 21:55:15, 46 of 677262006 22:58:30 UTC
 Message Category: Connections

Displaying records 1-100 of 2606 Next 500 (1 2 3 4 5)

Time	Source/Port	Destination	Protocol	Src Port	Dest Port	Src Interface	Dest Interface	Tx Byte
07/26/2006 15:55:30.0.0.0	255.255.255.255	udp/0	68	0	WAN	LAN	0	
07/26/2006 15:55:30.0.0.0	255.255.255.255	udp/0	68	0	WAN	LAN	0	
07/26/2006 15:55:30.0.0.0	255.255.255.255	udp/0	68	0	WAN	LAN	0	
07/26/2006 15:55:20172.16.32.247	172.16.32.10	udp/0	2222	0	OPT	OPT	0	
07/26/2006 15:55:20172.16.32.247	172.16.32.10	udp/0	2223	0	OPT	OPT	0	
07/26/2006 15:55:16172.16.32.247	172.16.32.10	udp/0	2221	0	OPT	OPT	0	
07/26/2006 15:55:220.0.0.0	255.255.255.255	udp/0	68	0	WAN	LAN	0	
07/26/2006 15:55:210.0.0.0	255.255.255.255	udp/0	68	0	WAN	LAN	0	
07/26/2006 15:55:200.0.0.0	255.255.255.255	udp/0	68	0	WAN	LAN	0	
07/26/2006 15:57:54172.16.32.247	172.16.32.10	udp/0	2219	0	OPT	OPT	0	
07/26/2006 15:57:54172.16.32.247	172.16.32.10	udp/0	2220	0	OPT	OPT	0	
07/26/2006 15:57:4810.0.203.102	255.255.255.255	udp/0	68	0	WAN	LAN	0	
07/26/2006 15:57:46172.16.32.247	172.16.32.10	udp/0	2218	0	OPT	OPT	0	
07/26/2006 15:57:4510.0.203.102	255.255.255.255	udp/0	68	0	WAN	LAN	0	
07/26/2006 15:56:3710.0.203.102	255.255.255.255	udp/0	68	0	WAN	LAN	0	
07/26/2006 15:56:3410.0.203.102	255.255.255.255	udp/0	68	0	WAN	LAN	0	
07/26/2006 15:56:20172.16.32.247	172.16.32.10	udp/0	2216	0	OPT	OPT	0	
07/26/2006 15:56:20172.16.32.247	172.16.32.10	udp/0	2217	0	OPT	OPT	0	
07/26/2006 15:56:16172.16.32.247	172.16.32.10	udp/0	2216	0	OPT	OPT	0	
07/26/2006 15:55:290.0.0.0	255.255.255.255	udp/0	68	0	WAN	LAN	0	
07/26/2006 15:55:300.0.0.0	255.255.255.255	udp/0	68	0	WAN	LAN	0	
07/26/2006 15:55:370.0.0.0	255.255.255.255	udp/0	68	0	WAN	LAN	0	
07/26/2006 15:54:45172.16.32.247	172.16.32.10	udp/0	2212	0	OPT	OPT	0	
07/26/2006 15:54:45172.16.32.247	172.16.32.10	udp/0	2213	0	OPT	OPT	0	
07/26/2006 15:54:45172.16.32.247	172.16.32.10	udp/0	2214	0	OPT	OPT	0	
07/26/2006 15:53:11172.16.32.247	172.16.32.10	udp/0	2209	0	OPT	OPT	0	
07/26/2006 15:53:11172.16.32.247	172.16.32.10	udp/0	2210	0	OPT	OPT	0	
07/26/2006 15:53:11172.16.32.247	172.16.32.10	udp/0	2211	0	OPT	OPT	0	
07/26/2006 15:51:3010.0.203.147	255.255.255.255	udp/0	68	0	WAN	LAN	0	
07/26/2006 15:51:37172.16.32.247	172.16.32.10	udp/0	2206	0	OPT	OPT	0	
07/26/2006 15:51:37172.16.32.247	172.16.32.10	udp/0	2207	0	OPT	OPT	0	
07/26/2006 15:51:27172.16.32.247	172.16.32.10	udp/0	2206	0	OPT	OPT	0	

Real-time Syslog Viewer

The real-time syslog utility enables you to diagnose the system by viewing the syslog messages in real time.



Note Only use this utility when needed for diagnostic purposes.

To open the real-time syslog utility, perform the following steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **UTM** or **SSL-VPN** tab.
3. Expand **Real-Time Viewer** and click **Syslog**. The Real-Time Syslog page appears.
4. If syslog forwarding is not enabled, select **Enable Syslog Forwarding**, set the IP address and port used by the syslog reader, and then click **Update**.

5. If the Syslog Reader is not already running, click **Start Syslog Reader**.
6. Click **Start Button** at the bottom of the screen. The Syslog Viewer begins showing the latest syslog entries.



7. To change how many messages are displayed, select a number from the **Number of Messages** list box at the bottom of the screen.



8. To change how often the Syslog Viewer is refreshed, select the time from the **Refresh Time** list box at the bottom of the screen.
9. To stop the viewer, click the **Stop** button.
10. To search for text, use the browser's Find utility.
11. When you are finished, close the Syslog Viewer.

Forwarding Syslog Data to Another Syslog Server

To forward SonicWALL ViewPoint syslog data to another syslog server, perform the following steps:

1. Open the sgmsConfig.xml file with a text editor.
2. Locate the following line:
Parameter name =“syslog.forwardToHost” value=“”
3. Add the IP address or hostname of the destination syslog server to the value attribute.
4. Save the sgmsConfig.xml file and exit.

5. Ensure that at least firmware 6.3.1.0 is running on the SonicWALL appliances.

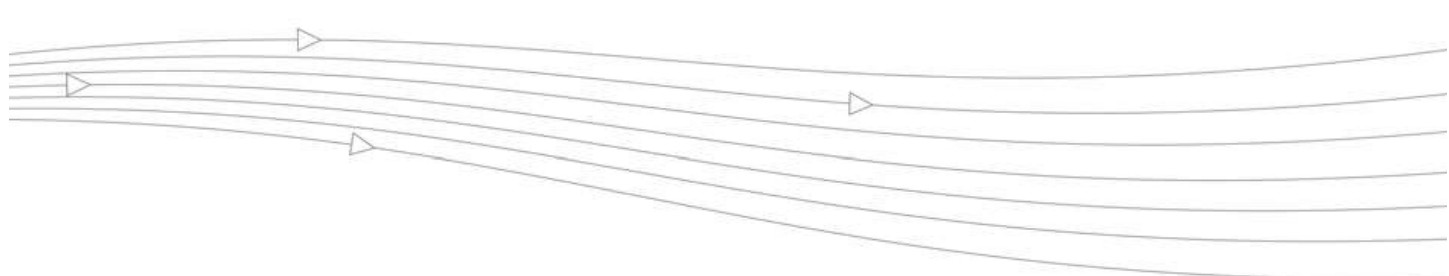


Note To configure SonicWALL ViewPoint to not store the syslog data after it has been forwarded, you must disable the ViewPoint Reporting Module. To do this, open the ViewPoint **Settings** page in the Console Panel, deselect the **Enable Reporting** check box, and click **Update**.

Posting ViewPoint Reporting to Another Web Server for End-User Access

To allow end user access to another web server for end-user access, install the SonicWALL ViewPoint Console in redundant mode.

You can then allow end user access to the redundant Console for viewing ViewPoint Reporting real-time and historical reports. End user access will be isolated from the main Console that is used for managing and configuring SonicWALL appliances.



Index

A

- activating
 - ViewPoint 341
- alert types 100
- alerting
 - using GEM 97
- anti-spyware
 - reports 266
- applets
 - signed 21
- Application Firewall reports 281
- archive
 - in Console>Reports 132
 - MDTA 87
 - on Console>Reports 81
 - report settings 81
 - scheduled report 135
 - summarizer data 87
- Attacks reports 250
- authentication code 353
- Authentication reports 287

B

- Bandwidth reports 180
- benefits
 - of compliance reports 144
 - of report data management 87
 - of SSL VPN reporting 294

browser

- requirements 338

C

- Compliance reports
 - configuration 152
 - overview 144
- compliance reports 144
- console
 - management settings 61
- cover page
 - customizing 147
- Custom Reports
 - Resource Activity 307
- customizing
 - detailed report 149
 - report cover page 147
 - summary report 148

D

- dashboard 159
 - Dashboard Summary report 159
- data
 - management 87
- database
 - backing up 368
 - reinstalling with existing db 369
 - requirements 337

- deployment
 - settings 354
- detailed report
 - customizing 149
- digital
 - signature in applet 21
- disabling
 - GEM thresholds 103
- domain names
 - in reports 130

E

- email
 - report settings 81
- enabling
 - GEM thresholds 103
 - report table sorting 71
- events
 - GEM overview 97
 - schedules 98
 - severities 97
 - thresholds 98

F

- File Transfer Protocol
 - See FTP
- free trial
 - for GMS 356
 - for GMS, configuring appliances 364
 - for GMS, enabling from UMH interface 359
 - for GMS, enabling from ViewPoint 357
- friendly name 353
- FTP reports 225

G

GEM

- alert types 100
- configuring 101
- default settings 99
- overview 97, 98
- schedules 98
- severities 97
- thresholds 98
- global view 117
- global views 120

GMS

- upgrading to from ViewPoint 356

Granular Event Management

See GEM

H

- hardware
 - requirements 339
- help
 - viewing online help 24
- host name resolution 79

I

- inheritance
 - report settings 138

installing

- appendix 335
- appliance, firmware support 339
- browser requirements 338
- database requirements 337
- deployment settings 354
- hardware requirements 339
- Java requirements 338
- network requirements 339
- on Windows 342
- overview 10
- system requirements 337
- task list 336
- Universal Management Suite 342

interfaces

- accessing both 11
- overview of ViewPoint application 13
- switching between 12, 24
- TreeControl 20
- UMH deployment options 31
- UMH deployment role 32
- UMH deployment services 36
- UMH HTTP(S) settings 34
- UMH SMTP settings 34
- UMH system administration 28
- UMH system diagnostics 30
- UMH system interface overview 24
- UMH system licenses 26
- UMH system settings 25
- UMH system software 29
- UMH system status 26

IPS

- reports 273

J

Java

- plugin 371
- requirements 338

java.policy file 21

L

licensing

- requirements 10
- SonicWALL appliances for use with ViewPoint 10
- ViewPoint on appliances 342

log

- viewing 58

Log Viewer 290, 332

log viewer

- for SSL VPN appliances 332

logging out 25

M

Mail Usage reports 231

MDTA 87

MySonicWALL

- creating an account 340

N

name resolution crawler 79

network

- requirements 339

P

pagination

- settings 51

password

- settings 51

PDF

- exporting reports to 144
- reports 152

port

- syslog 370

profiles

- existing 150
- scheduled report 149

R

registering

- procedure 351
- requirements 10
- SonicWALL appliances 341

reporting

- overview 115
- search bar 116, 118

reports

- adding scheduled 135
- Browse Time 128
- By Site to By User navigation 129
- compliance 144
- cover pages 147
- domains or IP addresses 130
- inheritance 138
- no data 156
- PDF format 144
- ROI 128
- searching by dates of 155
- settings 154
- SSL VPN 295
- SSL VPN authentication 330
- SSL VPN bandwidth 301
- SSL VPN custom resource activity 307
- SSL VPN overview 293
- SSL VPN resources 325
- SSL VPN scheduled reports 296
- SSL VPN summarization 297
- viewing Dashboard 159
- views 17
- Web usage, exclusions 53

requirements

- browser 338
- database 337
- hardware 339
- Java 338
- network 339
- system 337

reverse inheritance

- for reporting 139

role

- configuring 32

S

scheduled reports

- disabling/enabling 128

scheduler

- link to from report page 118

schedules 98

- resending 86

search bar 116, 118

- components of 123
- operators 125

Security Dashboard reports 159

serial number 353

- GMS 114

services

- enabling/disabling 36

Services reports 189

sessions

- managing 65

settings

- inactivity timeout 51
- pagination 51
- password 51
- website exclusion list 53

severities 97

signed applets 21

SMTP

- settings 34, 355

SNMP
 port 339

SQL
 authentication mode 369

status
 viewing 17

summarizer
 configuring reports to create 137
 instant summary reports 76
 using Summarize Now 76

summary report
 customizing 148

syslog
 port 339
 port number 370

system
 requirements 337

system interface
 deployment options 31
 deployment role 32
 deployment services 36
 HTTP(S) settings 34
 overview 24
 SMTP settings 34
 system administration 28
 system diagnostics 30
 system licenses 26
 system settings 25
 system software 29
 system status 26

T

thresholds 98

timeout
 inactivity settings 51

TreeControl
 collapsing/hiding the pane 20, 128
 menu 20

troubleshooting 368, 370
 reports, no data 156

U

UMH interface
 deployment options 31
 deployment role 32
 deployment services 36
 HTTP(S) settings 34
 overview 24
 SMTP settings 34
 system administration 28
 system diagnostics 30
 system licenses 26
 system settings 25
 system software 29
 system status 26

uninstalling 369

unit view 121

Universal Management Suite
 installing 342

upgrading
 purchasing GMS upgrade 366
 upgrade key 336
 ViewPoint to GMS 356

users
 managing sessions 65
 settings 51

V

views
 global 120
 unit 121

Virus Attacks Reports 260

VPN Usage reports 238

W

Web
 port configuration 354
 port settings 34

web event consolidation 141

Web Filter reports 209

Web usage

 exclusion list 53

Web Usage reports 191

Windows Firewall

 disabling 339, 352



SonicWALL, Inc.

2001 Logic Drive

San Jose CA 95124-3452

T +1 408.745.9600

F +1 408.745.9300

www.sonicwall.com



PN: 232-001802-00 Rev A 1/2010

©2010 SonicWALL, Inc. is a registered trademark of SonicWALL, Inc. Other product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. Specifications and descriptions subject to change without notice.

https://web.archive.org/web/20081207003303/http://www.sonicwall.com/downloads/EC_GMS_DS_US.pdf



SonicWALL® Global Management System

POLICY AND MANAGEMENT

Centralized Network Monitoring and Management Solution

- **Centralized security and network management**
- **Sophisticated VPN deployment and configuration**
- **Active device monitoring and alerting**
- **Centralized logging**
- **Intelligent reporting and activity visualization**
- **Offline management**
- **Streamlined license manager**
- **SNMP support**

The SonicWALL® Global Management System (GMS) provides organizations, distributed enterprises and service providers with a flexible, powerful and intuitive solution to centrally manage and rapidly deploy SonicWALL appliances and security policy configurations. SonicWALL GMS™ also provides centralized real-time monitoring, and comprehensive policy and compliance reporting.

SonicWALL GMS' intuitive Web-based user interface easily allows for complete life cycle control of thousands of SonicWALL appliances—from initial configuration to complex policy changes and remote updates. For enterprises, GMS simplifies the complexity of network management by offering a single management interface, thereby reducing administration time, complexity and the overall total cost of ownership (TCO). Service providers benefit from its multi-organizational management capabilities where it consolidates, groups and classifies thousands of individual customers' managed appliances and their respective security policies. Through an integrated reporting architecture, administrators can customize and schedule reports individually tailored to meet the needs of managed customers, executives and regulatory compliance audits for corporate departments.

Features and Benefits

Centralized security and network management is achieved using a flexible, powerful and intuitive tool to deploy, manage and monitor a distributed network environment and set policies from a central location. Administrators can now define, distribute, enforce and deploy a full range of service and security policies for thousands of SonicWALL appliances.

Sophisticated VPN deployment and configuration enables distributed enterprise networks to reduce the administration time, costs and complexity associated with establishing and maintaining corporate security policies, VPN connectivity and network configurations. For Service Providers, it consolidates and unifies all security policies for thousands of customers allowing for greater efficiencies in delivering an SLA.

Active device monitoring and alerting supplies real-time alerts with integrated monitoring capabilities allowing administrators to take preventative action and deliver immediate remediation.

Centralized logging provides a central location for consolidating security events and logs for thousands of appliances, thereby allowing for a single point to conduct network forensics.

Intelligent reporting and activity visualization presents comprehensive management and graphical reports for security devices and user activity yielding greater insight into usage trends and security events. It also enables the customization of these reports using corporate logos and colors, thereby delivering a cohesive branding message to users and customers.

Offline management enables scheduled configurations and/or firmware updates on managed appliances to occur offline to minimize service disruption to end users and customers.

Streamlined license manager displays a unified console for storing, applying, tracking and updating security license information for managed SonicWALL appliances, thereby simplifying the inventory for managing security and support license subscriptions.

SNMP support provides a powerful, real-time alerting mechanism for all TCP/IP and SNMP-enabled devices and applications, thus greatly enhancing the ability to pinpoint and respond to critical network events.



PROTECTION AT THE SPEED OF BUSINESS®

Keysight, EX-1030

Page 553

Specifications

**SonicWALL GMS Standard Edition**

SonicWALL GMS 10 Node Software License
01-SSC-3363

SonicWALL GMS 25 Node Software License
01-SSC-3311

SonicWALL GMS 24x7 Software Support
for 10 Nodes (1-year)*
01-SSC-6514

SonicWALL GMS 24x7 Software Support
for 25 Nodes (1-year)*
01-SSC-3334

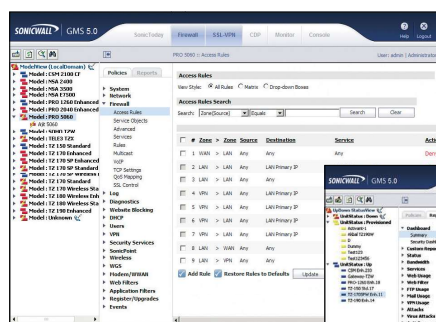
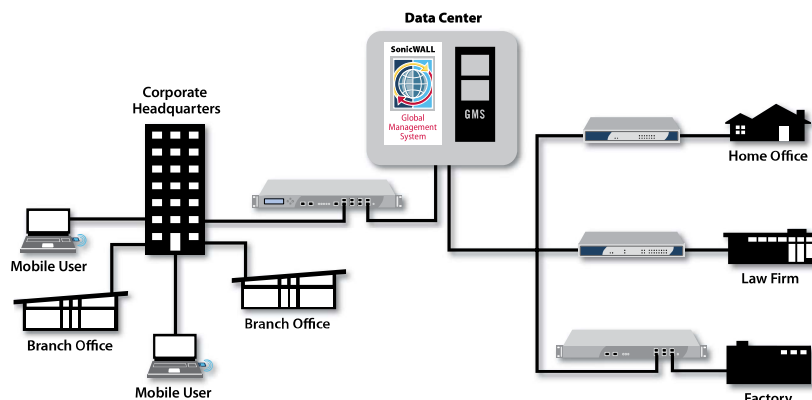
SonicWALL Comprehensive GMS 24x7
Support for 10 Nodes
01-SSC-3353

SonicWALL Comprehensive GMS 24x7
Support for 25 Nodes
01-SSC-3374

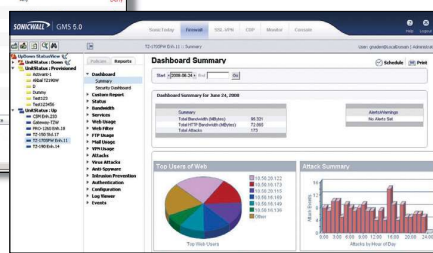
*Multi-year SKUs also available.

SonicWALL Global Management System

Providing a comprehensive security management solution for enterprises and service providers.



SonicWALL GMS allows administrators to easily create security policies for the SonicWALL Network Security appliances and enforce them at the global, group or unit level.



SonicWALL GMS allows administrators to generate a wide range of informative and historical reports to provide insight into usage trends, such as which Web sites have been accessed, by whom and security events of the managed SonicWALL Network Security appliances.

Minimum System Requirement

Below are the minimum requirements for SonicWALL GMS with respect to the operating systems, databases, drivers, hardware and SonicWALL supported appliances:

Operating System

Windows 2000 Server (SP4), Windows 2000 Professional (SP4), Windows XP Professional (SP2), Windows 2003 Server (SP2)

Hardware for Single Deployment

x86 Environment: Minimum 3 GHz processor Server dual-core CPU Intel processor, 2 GB RAM and 300 GB disk space

Hardware for Distributed Server Deployment

GMS Server x86 Environment: Minimum 3 GHz processor single-CPU Intel processor, 2 GB RAM and 300 GB disk space

Database Server x86 Environment: Minimum 3 GHz processor dual-core CPU Intel processor, 2 GB RAM and 300 GB disk space

GMS Gateway

SonicWALL PRO Series Network Security Appliance with minimum firmware, SonicOS Enhanced 3.2 and SonicWALL VPN-based Network Security appliances¹

Database

Microsoft® Environment: Microsoft SQL Server 2000 (SP4) and Microsoft SQL Server 2005 (SP2)² on either Windows 2000 Server (SP4) or 2003 Server (SP2)

Java

Java Plug-in version 1.5 or later

Supported SonicWALL Appliances Managed by GMS

SonicWALL Network Security appliances: E-Class NSA, NSA, PRO Series, TZ Series appliances

SonicWALL Continuous Data Protection appliances

SonicWALL CSM appliances, SonicWALL SSL-VPN appliances

All TCP/IP and SNMP-enabled devices and applications for active monitoring

Internet Browsers

Microsoft® Internet Explorer 6.0 or higher

Mozilla Firefox 2.0 or higher

Supported Firmware

SonicWALL Network Security appliances: E-Class NSA and NSA SonicOS Enhanced 5.0 or higher

SonicWALL PRO Series appliances: SonicOS Enhanced 3.2 or higher

SonicWALL TZ Series appliances: SonicOS Standard 3.1 or higher and SonicOS Enhanced 3.2 or higher

SonicWALL CDP appliances: SonicWALL CDP 2.3 or higher

SonicWALL CSM appliances: SonicWALL 2.0 or higher

SonicWALL SSL VPN appliances: SonicWALL SSL VPN SMB Firmware 2.0 or higher and SonicWALL Aventail E-Class SSL VPN Firmware 9.0 or higher

¹ The GMS Gateway should have at minimum a SonicWALL PRO 2040 Network Security appliance or higher.

² MySQL database is bundled with the GMS application.

SonicWALL, Inc.

1143 Borregas Avenue
Sunnyvale CA 94089-1306

T +1 408.745.9600
F +1 408.745.9300

www.sonicwall.com

