Analyzer 7.1
Administrator's Guide

Notes, Cautions, and Warnings

NOTE: A NOTE indicates important information that helps you make better use of your system.

CAUTION: A CAUTION indicates potential damage to hardware or loss of data if instructions are not followed.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

2013 – 04 P/N 232-001454-00 Rev. B

Table of Contents

CHAPTER 1

Introduction to Analyzer

This chapter provides an overview of the Dell SonicWALL Analyzer and information about the user interface. See the following sections:

Overview

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

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

- Displays bandwidth use by IP address and service
- Identifies inappropriate Web use
- Provides detailed reports of attacks
- Collects and aggregates system and network errors
- Shows VPN events and problems
- Presents visitor traffic to your Web site
- Provides detailed daily logs to analyze specific events.

Deployment Requirements

The Dell SonicWALL Analyzer comes with a base license to manage either 5, 10, or 25 nodes. You can purchase additional licenses on MySonicWALL. For more information on licensing additional nodes, visit:
http://www.sonicwall.com/us/Products_Solutions.html

Note Global Management System is not supported on laptops or tablets.

Before installing, review the requirements in the following sections:

Operating System Requirements

The Dell SonicWALL Analyzer supports the following operating systems:

- Windows Server 2008 SBS R2 64-bit
- Windows Server 2008 R2 Standard 64 bit
- Windows Server 2008 SP2 64-bit
- Windows Server 2003 64-bit (SP2)
- Windows 7 SP1 64-bit

Tip In all instances, Dell SonicWALL Analyzer is running as a 32-bit application. Bundled databases run in 64-bit mode on 64-bit Windows operating systems. All listed operating systems are supported in both virtualized and non-virtualized (VMware ESXi 4.1) environments.

Hardware for Windows Server

The Dell SonicWALL Analyzer requires the following hardware:

- x86 Environment: minimum 3 GHz processor dual-core CPU Intel processor
- 4GB RAM minimum
- 300 GB disk space

A Windows 64-bit operating system with a minimum RAM of 8-GB is highly recommended for better performance of reporting modules. Please read the Capacity Planning and Performance Tuning appendix in the *GMS 7.1 Administrator's Guide.*

MySQL Requirements

Dell SonicWALL Analyzer automatically installs MySQL as part of the base installation package. Separately installed instances of MySQL are not supported with Analyzer 7.1 Software.

Java Requirements

Download and install the latest version of the Java 7 plug-in on any system that accesses the GMS 7.1 UI. This can be downloaded from www.java.com or http://www.oracle.com/technetwork/java/javase/downloads/index.html

Browser Requirements

- Microsoft Internet Explorer 8.0 or higher (Do not use Compatibility Mode)

Note Internet Explorer version 10.0 in Metro interfaces of Windows 8 is currently not supported.

- Mozilla Firefox 16.0 or higher
- Google Chrome 18.0 or higher (recommended browser for dashboard real-time graphics display)

Network Requirements

To complete the Global Management System deployment process documented in this *Getting Started Guide*, the following network requirements must be met:

- The Dell SonicWALL Analyzer server must have access to the Internet
- The Dell SonicWALL Analyzer server must have a static IP address
- The Dell SonicWALL Analyzer server's network connection must be able to accommodate at least 1 KB/s for each device under management. For example, if Global Management System is monitoring 100 SonicWALL appliances, the connection must support at least 100 KB/s.

Caution Depending on the configuration of Dell SonicWALL log settings and the amount of traffic handled by each device, the network traffic can vary dramatically. The 1 KB/s for each device is a general recommendation. Your installation requirements may vary.

Dell SonicWALL Appliance and Firmware Support

Dell SonicWALL Platforms	Dell SonicWALL Firmware Version
Firewall / VPN	
SuperMassive 10000 Series	SonicOS 6.0 or newer:
SuperMassive 9000 Series	SonicOS 6.1 or newer
NSA Series	SonicOS 5.0 or newer
TZ Series	SonicOS Enhanced 3.2 or newer SonicOS Standard 3.1 or newer
PRO Series	SonicOS Enhanced 3.2 or newer
CSM Series	SonicOS CF 2.0 or newer
Secure Remote Access	
SMB SRA Series	SonicOS SSL-VPN 2.0 or newer (management) SonicOS SSL-VPN 2.1 or newer (reporting)
E-Class SRA Series	SRA 9.0 or newer
Backup and Recovery	
CDP Series	CDP 2.3 or newer (management) CDP 5.1 or newer (reporting)

Dell SonicWALL Analyzer Installation

Analyzer can be installed as a fresh install or as an upgrade to SonicWALL ViewPoint 6.0 and above. Beginning in SonicWALL ViewPoint 5.1, all software components related to Dell SonicWALL Analyzer and SonicWALL Global Management System (GMS), including the MySQL database, executable binary files for all services, and other necessary files, are installed using the Universal Management Suite (UMS) single-binary installer. All SonicWALL Analyzer and SonicWALL GMS files are installed as part of the Universal Management Suite, but no distinction is made between SonicWALL Analyzer and SonicWALL GMS during the installation. The initial installation phase takes just a few minutes for any type of installation, such as a SonicWALL Analyzer server, a SonicWALL GMS server, a database server, or any other role.

To install the Universal Management Suite from the single binary installer, refer to the *Dell SonicWALL Analyzer Getting Started Guide*.

License and Registration Requirements

SonicWALL Analyzer is registered and licensed from the Windows server on which it is installed. Dell SonicWALL Analyzer registration is performed using the SonicWALL Universal Management Host system interface.

Refer to the *Dell SonicWALL Analyzer Getting Started Guide* for detailed instructions on registering and licensing Analyzer on your system.

On Dell SonicWALL appliances that send reporting data to the Analyzer, Analyzer is licensed and activated separately from the Dell SonicWALL appliances. MySonicWALL provides a way to associate Dell SonicWALL appliances with the Analyzer instance installed on the Windows system. Licensing your Analyzer application on a Dell SonicWALL appliance requires:

- **A MySonicWALL account**. A MySonicWALL account allows you to manage your SonicWALL products and purchase licenses for various services. Creating a MySonicWALL account is fast, simple, and free. Simply complete an online registration form directly from your SonicWALL security appliance management interface. Your MySonicWALL account is also accessible at <https://www.mysonicwall.com> from any Internet connection with a Web browser. Once you have an account, you can purchase SonicWALL Analyzer and other licenses for your registered SonicWALL security appliances.
- **A registered SonicWALL security appliance with active Internet connection**. You need to register your SonicWALL security appliance to activate SonicWALL Analyzer. Registering your SonicWALL security appliance is a simple procedure done directly from the management interface. Once your SonicWALL security appliance is registered, you can activate SonicWALL Analyzer by using an activation key or by synchronizing with mysonicwall.com.

Accessing the Correct Management Interface

Dell SonicWALL Analyzer includes two separate management interfaces:

- **SonicWALL Universal Management Host (UMH) System Management Interface** – Used for system management of the Dell SonicWALL Analyzer instance, including registration and licensing, setting the admin password, creating backups, restarting the system, configuring network settings, selecting the deployment role, and configuring other system settings.
  Access the system management interface with the URL:

  http://<*IP_address*>:<*port_number*>/appliance/

  If you are using the standard HTTP port, 80, it is not necessary to append the port number to the IP address. If you are accessing the interface from the same system on which it is installed, use the following URL:

  http://localhost/appliance/

- **Dell SonicWALL Analyzer Management Interface** – Used to access the Dell SonicWALL Analyzer application that runs on the system. This interface is used to configure and view Dell SonicWALL Analyzer reporting on SonicWALL appliances and for configuring Dell SonicWALL Analyzer administrative settings. Access the Dell SonicWALL Analyzer management interface with one of the following URLs:

  http://<*IPaddress*>:<*port_number*>/sgms/
  http://localhost/sgms/

Switching Between Management Interfaces

You can easily switch between the SonicWALL UMH system management interface and the Dell SonicWALL Analyzer application management interface.

One method is to change the URL by adding **/sgms** for the Analyzer application interface or adding **/appliance** for the UMH interface.

A second method involves clicking the **Switch** icon. While logged into either interface, you can switch to the login page of the other interface by clicking the **Switch** button in the top right corner of the page.

Login to Analyzer

After registering your SonicWALL Analyzer product, to login into the SonicWALL Analyzer management interface, either double-click on the SonicWALL Analyzer icon on your desktop, or from a remote system, access the following URL from a web browser:

http://<*IP_address*>:<*port_number*>

The Dell SonicWALL Analyzer login page appears by default in English. To change the language setting, click your language of choice at the bottom of the login page. The available language choices for SonicWALL Analyzer include English, Japanese, Simplified Chinese, and Tradition Chinese.

1. Enter the SonicWALL user ID (default: admin) and password (default: password). Select 'Local Domain' as the domain (default).
2. Click **Submit**. The Dell SonicWALL Analyzer management interface displays.

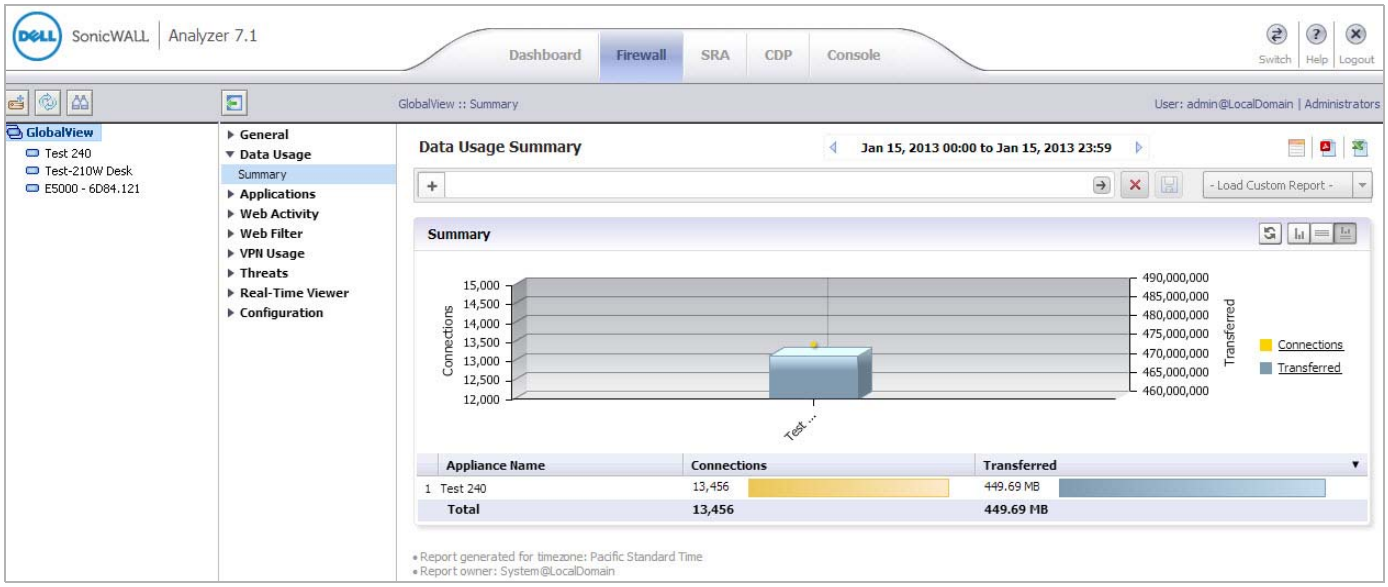
Note For more information on installation, login procedures, and registration of your SonicWALL Analyzer installation, please refer to the appropriate *Getting Started Guide*, available at: <http://www.sonicwall.com/us/support.html>

Navigating the Analyzer User Interface

This section describes the Firewall, SRA, and Console panels in the SonicWALL Analyzer user interface. For information about the Dashboard panel, see the “Using the Universal Scheduled Reports Application” section on page 60.

Firewall Panel

The Firewall Panel is an essential component of network security that is used to view and schedule reports about critical network events and activity, such as security threats, inappropriate Web use, and bandwidth levels. To open the Firewall Panel, click the **Firewall** tab at the top of the Analyzer user interface.



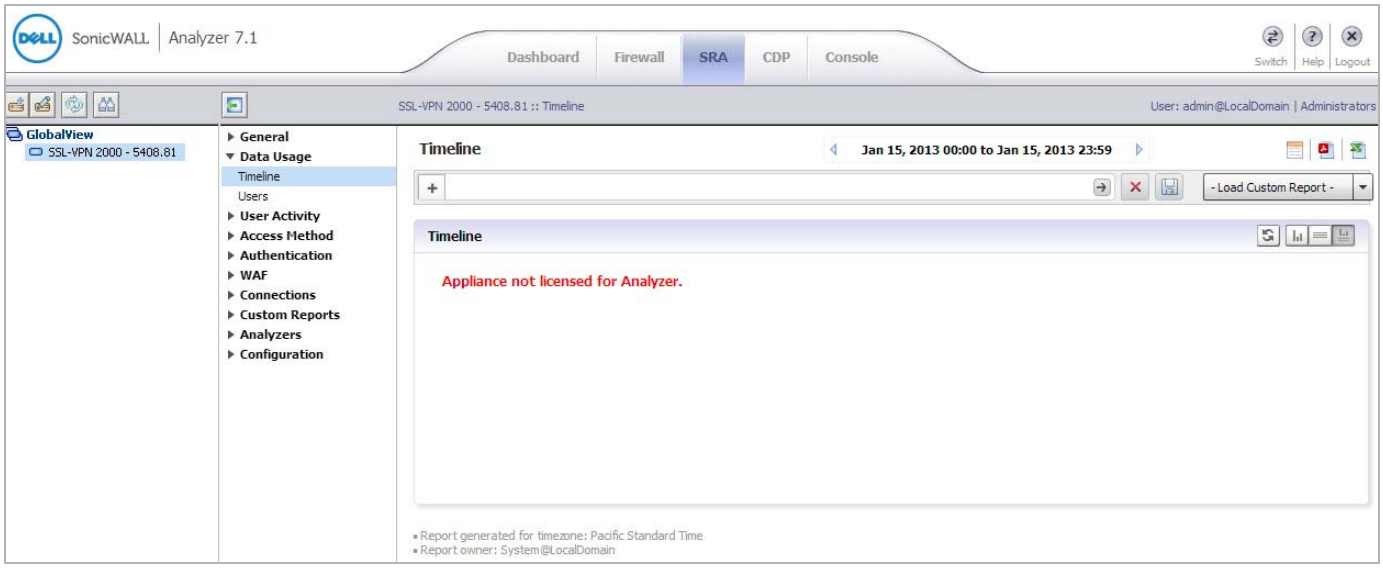
From the Firewall Panel, you can view the following for connected SonicWALL appliances:

- View general unit status, license status, and syslog settings.
- View the SonicWALL security dashboard. Dashboard reports display an overview of bandwidth, uptime, intrusions and attacks, and alerts for connected SonicWALL firewall appliances. The Security Dashboard report provides data about worldwide security threats that can affect your network. The Dashboard also displays data about threats blocked by the SonicWALL security appliance.
- View custom reports of Internet activity or Website filtering at the unit level. Custom reports filter raw syslog data and you can specify start and end dates or a date range such as “Week to date”. You can filter by user, domain, protocol, traffic, and full URL categories, depending on the type of custom report. The search template can be saved for use again later with the same appliance.
- View general bandwidth usage. These reports include a daily bandwidth summary report, a top users of bandwidth report, and over-time summary and top users reports.
- View a services report. This report includes information about events and usage of protocols and megabytes.

- View Web bandwidth usage. These reports include a daily bandwidth summary report, a top visited sites report, a top users of Web bandwidth report, a report that contains the top sites of each user, and a weekly summary report.
- View the number of attempts that users made to access blocked websites. These reports include a daily summary report, a top blocked sites report, a top users report, a report that contains the top blocked sites of each user, and a weekly summary report.
- View file transfer protocol (FTP) bandwidth usage. These reports include a daily FTP bandwidth summary report, a top users of FTP bandwidth report, and a weekly summary report.
- View mail bandwidth usage. These reports include a daily mail summary report, a top users of mail report, and a weekly summary report.
- View VPN usage. These reports include a daily VPN summary report, a top users of VPN bandwidth report, and a weekly summary report.
- View reports on attempted attacks and errors. The attack reports include a daily attack summary report, an attack by category report, a top sources of attacks report, and a weekly attack summary report. The error reports include a daily error summary report and a weekly error summary report.
- View reports on attempted virus attacks. Virus attacks reports are available for appliances that are licensed for SonicWALL Gateway Anti-Virus. These reports include the most frequent virus attack attempts, virus attacks by top destinations, virus attacks over time, virus attacks over a period of time, and virus attacks by top destinations over time.
- View reports on attempted spyware attacks. Anti-spyware reports are available for appliances that are licensed for SonicWALL Anti-Spyware. These reports include spyware attacks by category, spyware attacks over time, and spyware attacks by category over time.
- View reports on attempted intrusion attacks. Intrusion prevention reports are available for appliances that are licensed for SonicWALL Intrusion Prevention Service. These reports include intrusion attacks by source IP address, intrusion attacks by category, intrusion attacks over time, and intrusion attacks by category over time.
- View reports on traffic triggering Application Firewall policies. Application Firewall reports are available for SonicWALL firewall appliances that are licensed for SonicWALL Application Firewall. These reports include summary, over time, top applications, top users, and top policies.
- View successful and unsuccessful user and administrator authentication attempts. These reports include a user authentication report, an administrator authentication report, and a failed authentication report.
- View detailed logging information. The detailed logging information contains each transaction that occurred on the SonicWALL appliance.
- View current alerts and access alert settings.

SRA Panel

The SRA panel provides access to SSL VPN appliances and is similar to the Firewall panel. It is used to view and schedule reports about critical network events and activity, such as security threats, inappropriate Web use, and bandwidth levels. To open the SRA Panel, click the **SRA** tab at the top of the Analyzer user interface.

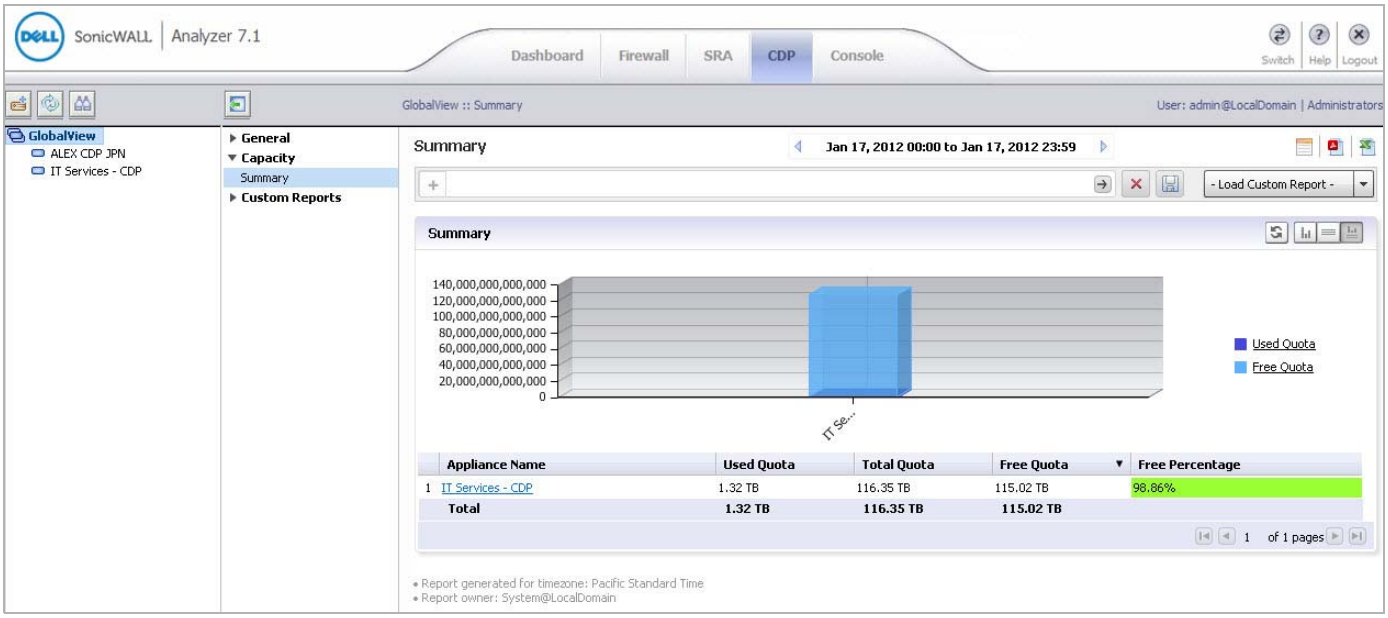


From the SRA Panel, you can view the following for connected SonicWALL SSL VPN appliances:

- View general unit status, license status, and syslog settings.
- View general bandwidth usage. These reports include a daily bandwidth summary report, a top users of bandwidth report, and over-time summary and top users reports.
- View custom reports of custom reports of resource activity at the unit level. Custom reports filter raw syslog data and you can specify start and end dates or a date range such as “Week to date”. You can filter by user, protocol, destination IP, and source IP categories. The search template can be saved for use again later with the same appliance.
- View a resources report. This report includes information about connections and the resource used to connect, such as HTTPS or NetExtender.
- View successful and unsuccessful user authentication attempts. These reports include a user authentication report and a failed authentication report.
- View detailed logging information. The detailed logging information contains each transaction that occurred on the SonicWALL appliance.

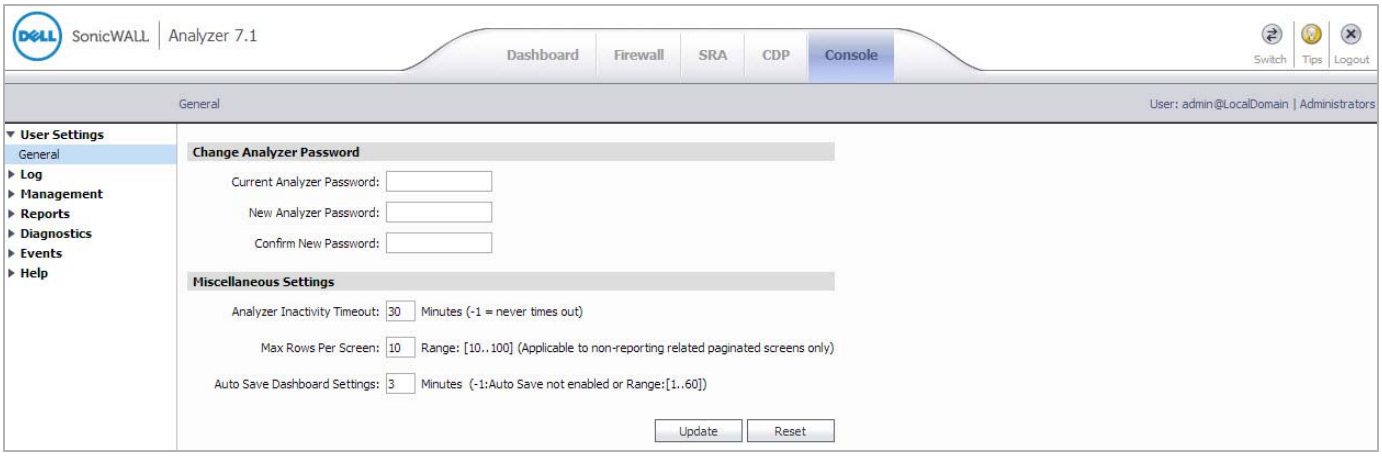
CDP Panel

The CDP panel provides access to CDP appliances and is similar to the SRA panel. It is used to view and schedule reports about storage capacity, used quota, and free quota. To open the CDP Panel, click the **CDP** tab at the top of the Analyzer user interface.



Console Panel

The Console Panel is used to configure Dell SonicWALL Analyzer settings, view pending tasks, view the log, manage licenses, and configure alerts. To open the Console Panel, click the **Console** tab at the top of the Dell SonicWALL Analyzer user interface.



From the Console Panel, you can do the following:

- Change the Dell SonicWALL Analyzer password, adjust the amount of inactive time before the user is automatically logged out of Analyzer, and set the maximum number of rows displayed on paginated screens.

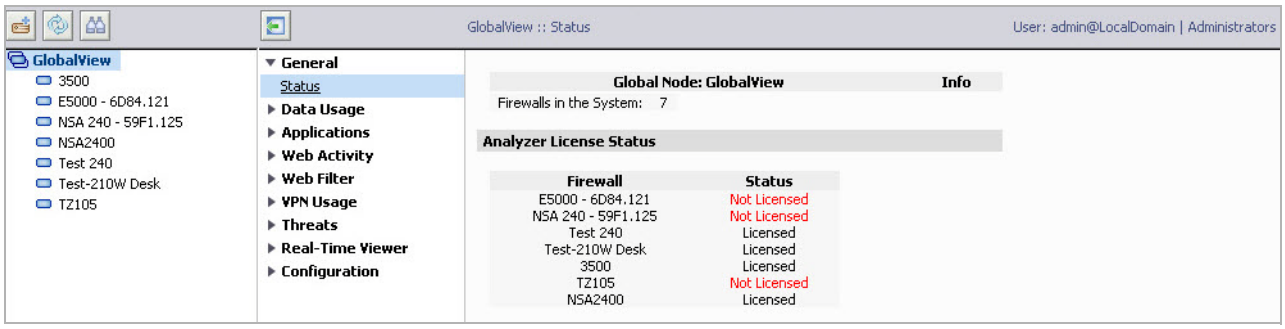
- Configure Web sites and Web users that will be excluded from Web usage reports.
- View the Dell SonicWALL Analyzer log and delete old log messages. The Dell SonicWALL Analyzer log contains information on alert notifications, failed Dell SonicWALL Analyzer login attempts, and other events that apply to Dell SonicWALL Analyzer.
- Manage SMTP settings, system email addresses, archive report settings, debug level for logs, and password security settings. You can set the schedule and server settings, and the email alert recipient schedule and preferred format.
- Manage login sessions. You can view the status of user sessions and, if necessary, end them.
- Configure report settings for sort options and maximum units with Log Viewer enabled. Enabling Log Viewer allows custom reports for the system, but is resource intensive.
- Control summarizer settings, syslog and summarized data deletion schedules, and host name resolution settings.
- Configure email archive settings and search settings for scheduled reports, and manage data archiving.
- View summarizer diagnostics, useful for capacity planning.
- Configure granular event management report settings, including threshold, schedule, and alert settings.
- Configure Web services deployment settings and view Web services status.
- View the version number, serial number, and database information for SonicWALL Analyzer, and access links to all available tips and video tutorials.

Analyzer Views and Status

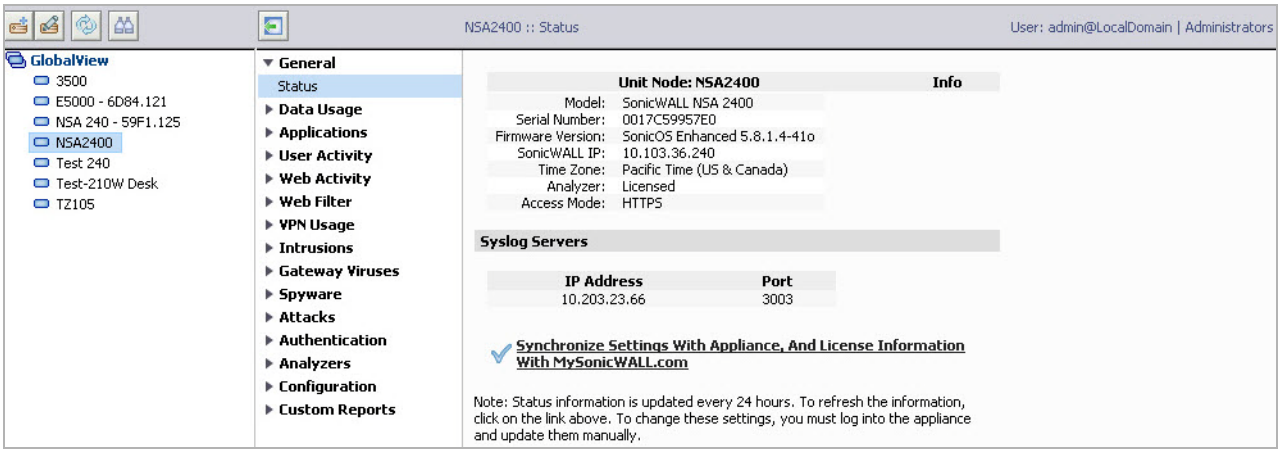
SonicWALL Analyzer allows you to view status and reports for all appliances at once using **GlobalView**, or for a single unit at a time with the **Unit** view. Analyzer provides status information on the General > Status page of the Firewall, SRA, or CDP panel.

GlobalView is a grouping of all the appliances you are monitoring with Analyzer. From the GlobalView of the Firewall, SRA, or CDP panel, Summary and Over Time reports are available for all SonicWALL appliances monitored by SonicWALL Analyzer.

To open the My Reports view, click the **GlobalView** icon at the top of the left pane. To display the global status page, navigate to **General > Status**.



From the Unit view, reports contain detailed data for the selected SonicWALL appliance. To specify the unit view, click any unit in the left pane. To display the unit status page, navigate to **General > Status** on the **Firewall**, **SRA**, or **CDP** panel.



Understanding Analyzer Icons

This section describes the meaning of icons that appear next to managed appliances listed in the left pane of the Analyzer management interface.

Appliance Status	Description
	One blue box indicates that the appliance is operating normally. The appliance is accessible from the Analyzer Software, and no tasks are pending or scheduled.
	Three blue boxes indicate that all appliances in the global group of this type (Firewall/SRA/CDP) are operating normally.

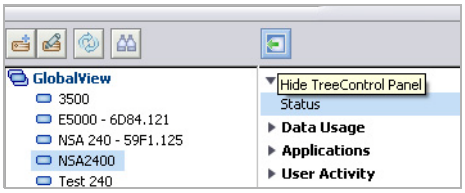
Using the Analyzer TreeControl Menu

This section describes the content of the TreeControl menu within the Dell SonicWALL Analyzer user interface.

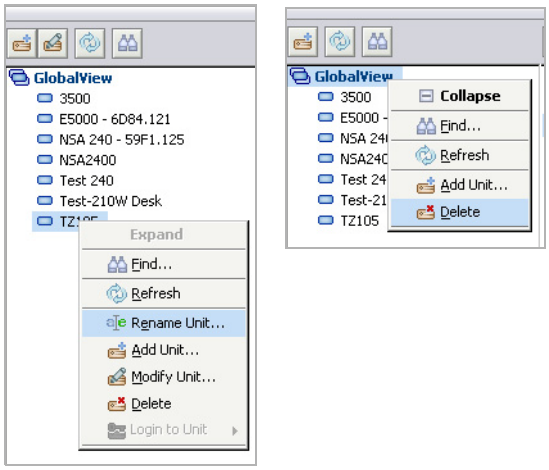
You can control the display of the TreeControl pane by selecting one of the appliance tabs at the top of the main window. For example, when you click the **Firewall** tab, the TreeControl pane displays all the connected SonicWALL firewall appliance units. The two appliance tabs can display the following appliance types when Analyzer is monitoring these device types:

- SonicWALL firewall appliances
- SRA and EX-Series SRA appliances

You can hide the entire TreeControl pane by clicking the sideways arrow icon, and redisplay the pane by clicking it again. This is helpful when viewing some reports or other extra-wide screens.



To open a TreeControl appliance menu, right-click GlobalView or a Unit icon.



The following options are available in the right-click menu:

- **Find** – Opens a Find dialog box that allows you to search for units.
- **Refresh** – Refreshes the Analyzer UI display.
- **Rename Unit** – (unit view only) Renames the selected SonicWALL appliance.
- **Add Unit** – Add a new unit to the Analyzer view. Requires unit IP and login information.
- **Modify Unit** – (unit view only) Change basic settings for the selected unit, including unit name, IP and login information, and serial number.
- **Delete** – Delete the selected unit
- **Login to Unit** – (unit view only) Login to the selected unit using HTTP or HTTPS protocols.

CHAPTER 2

Using the UMH System Interface

This chapter content describes the Universal Management Host system interface, one of the two management interfaces available for Dell SonicWALL Analyzer. The Dell SonicWALL Analyzer UMH system interface contains similar configuration settings for Microsoft Windows and Virtual Appliance deployments.

The Dell SonicWALL Analyzer Virtual Appliance UMH interface contains the following settings that are not applicable to Windows deployments:

- **System > Time**
- **System > File Manager**
- **System > Shutdown**
- **Network > Settings**
- **Network > Routes**

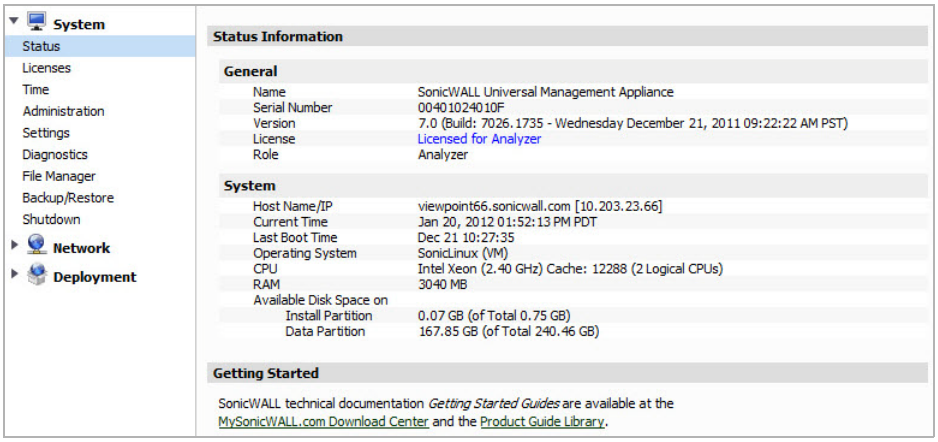
Note Microsoft Windows deployments can skip these settings as they only apply to Virtual Appliance deployments

This section includes the following subsections:

Overview of the UMH System Interface

The Dell SonicWALL Analyzer UMH system interface is used for system management of the Dell SonicWALL Analyzer instance, including registration and licensing, setting the administrator password, configuring network and database settings, selecting the deployment role, and configuring other system settings.

When installing SonicWALL Universal Management Suite on a host, a Web server is installed to provide the system management interface. The system interface is available by default at http://localhost/appliance/ after restarting the system.



Switching to the Application Interface

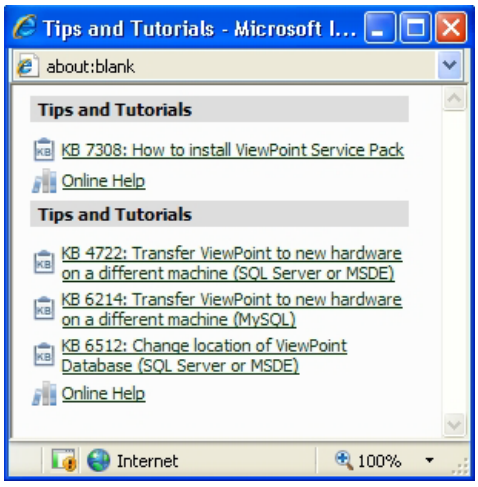
To switch between the System interface and the Dell SonicWALL Analyzer application interface, click the **Switch** button in the top right corner of the interface.

Viewing Online Help and Tips

To display context sensitive help for the current page, click the **Help** button in the top right corner of the interface.

The **Help** button can change to the **Tips** button if the current page has any context sensitive tips or video tutorials.

Clicking on the **Tips** button displays dynamic links for whitepapers, videos, knowledge base articles, other references, and online help.



Logging Out of the UMH System Interface

To log out of the Dell SonicWALL Analyzer UMH system interface, click the **Logout** button in the top right corner of the interface.

Configuring UMH System Settings

This section describes the tasks you can perform on the System pages of the Dell SonicWALL Analyzer UMH system interface. The Dell SonicWALL Analyzer UMH system interface contains similar configuration settings for Microsoft Windows and Virtual Appliance deployments. The Dell SonicWALL Analyzer Virtual Appliance UMH interface contain the following settings that are not applicable to Windows deployments. Microsoft Windows deployments can skip these settings as they only apply to Virtual Appliance deployments:

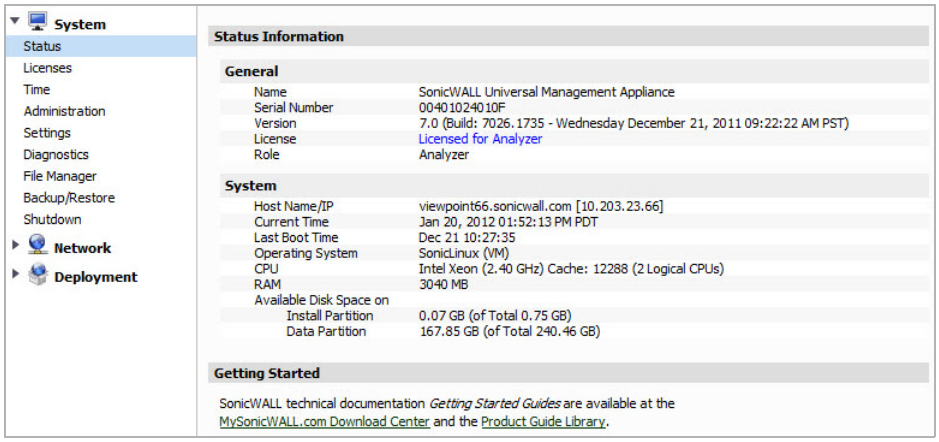
- **System > Time**
- **System > File Manager**
- **System > Shutdown**

See the following sections:

- "Viewing System Status" section on page 28
- "Managing System Licenses" section on page 29
- "Configuring System Time Settings (Virtual Appliance)" section on page 38
- "Configuring System Administration Settings" section on page 39
- "Managing System Settings" section on page 39
- "Using System Diagnostics" section on page 40
- "Using System File Manager (Virtual Appliance)" section on page 42
- "Using System Backup/Restore" section on page 42
- "Using System Shutdown (Virtual Appliance)" section on page 43

Viewing System Status

The **System > Status** page provides the general information about the installation, including the name which identifies the system as a SonicWALL Universal Management Host, the serial number of the Dell SonicWALL Analyzer instance, the software version, licensing status, and the system role. For Dell SonicWALL Analyzer, the role is always "Analyzer."



Under System, the host name of the computer is listed, along with the time and other information about the host computer.

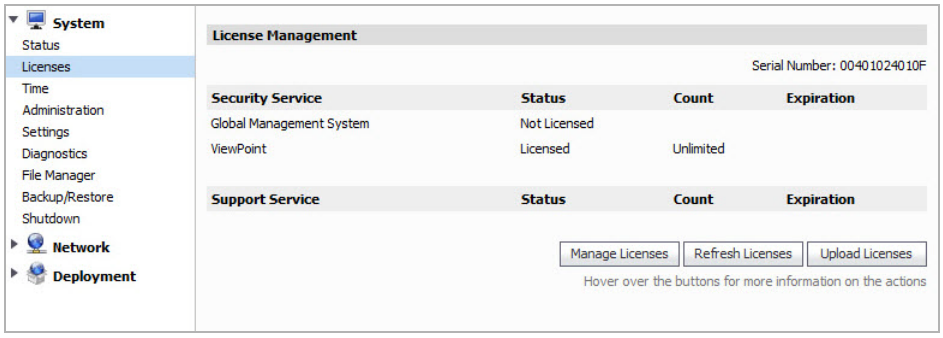
At the bottom of the page, a link is provided to access the *Getting Started Guide* which takes you to the online help table of contents.

Managing System Licenses

The **System > Licenses** page provides buttons for managing, refreshing, and uploading licenses. The page displays the status of Analyzer and Global Management System licenses. The Global Management System license status will show the status of your SonicWALL GMS Free Trial, if activated. If you choose to upgrade to SonicWALL GMS, this page will show Global Management System as fully licensed.

The value in the Count column indicates the number of appliances for which this SonicWALL Analyzer or SonicWALL GMS instance is licensed for reporting or management. For Dell SonicWALL Analyzer, this value is usually “unlimited”, but for SonicWALL GMS, the base license is either for 10 nodes or 25 nodes, and additional node licenses can be purchased in various increments.

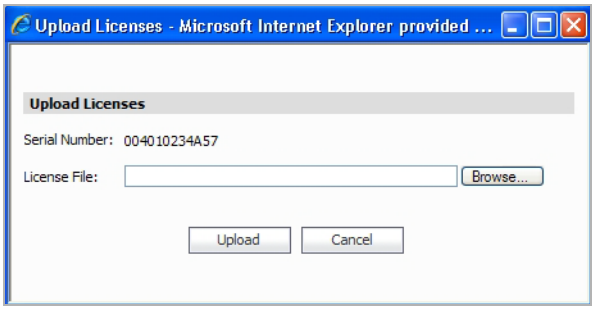
The Expiration column indicates the expiration date of the license. If no date is shown, the license is perpetual, and does not expire.



To display the MySonicWALL login page, click the **Manage Licenses** button. You can purchase licenses and obtain license keysets on MySonicWALL.

Click the **Refresh Licenses** button to refresh the license status on this page.

To upload a new license, click the **Upload Licenses** button and browse to a license file on your computer.

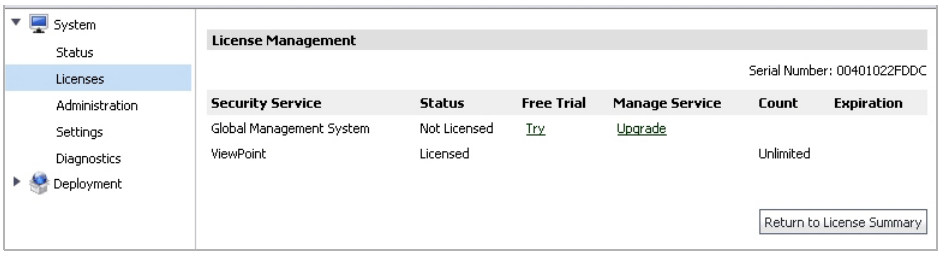


Upgrading from Analyzer to GMS

SonicWALL Analyzer 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 Analyzer 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 Analyzer reporting, the **Try GMS Free - 30 Days** button appears next to the tabs at the top of the SonicWALL Analyzer 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 Analyzer” section on page 30
- “Enabling the GMS Free Trial from the UMH Interface” section on page 32
- “Completing the Free Trial Upgrade” section on page 33
- “Configuring Appliances for GMS Management” section on page 35
- “Purchasing a SonicWALL GMS Upgrade” section on page 37

Enabling the GMS Free Trial from Analyzer

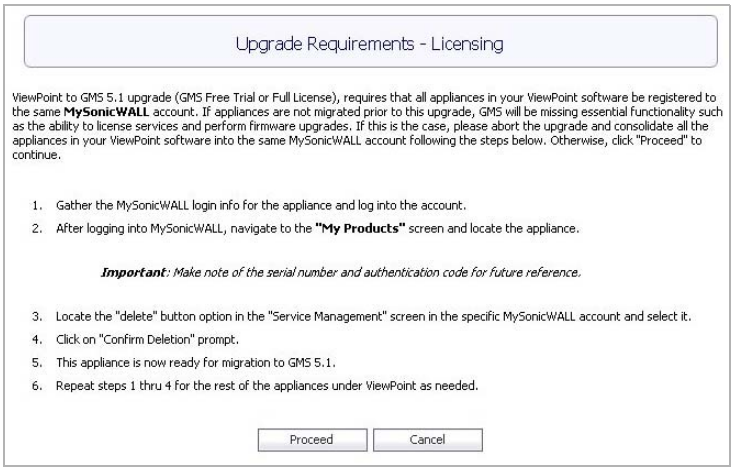
When five or more devices are connected to SonicWALL Analyzer reporting, the **Try GMS Free - 30 Days** button appears next to the tabs at the top of the SonicWALL Analyzer management interface.

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

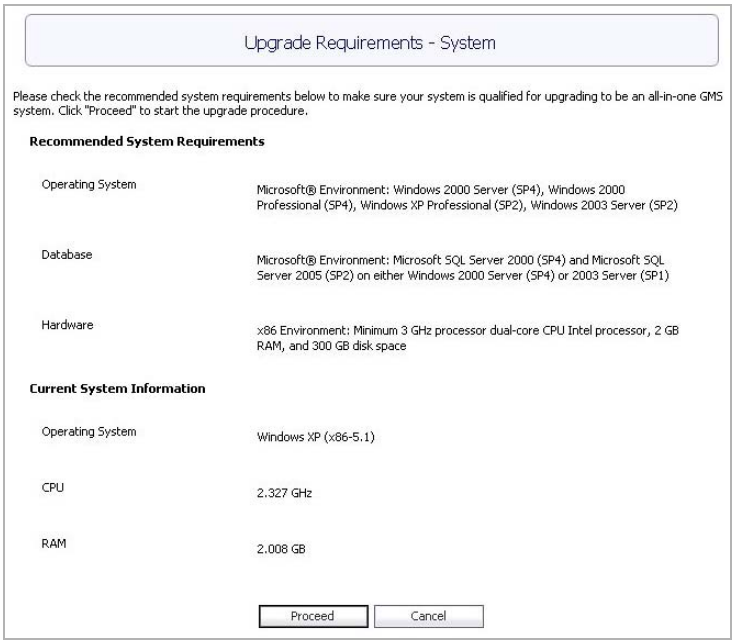
To enable the 30-day SonicWALL GMS Free Trial from the SonicWALL Analyzer management interface, perform the following steps:

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

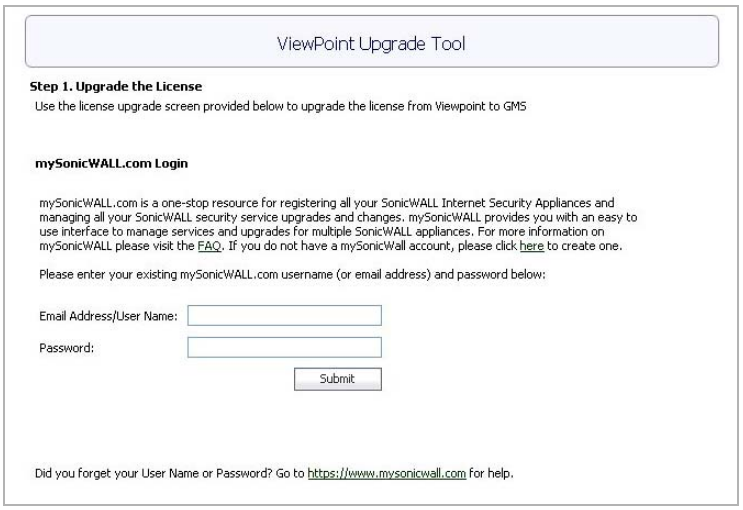
2. The Analyzer Upgrade Tool launches and guides you through the process of installing the Free Trial or Upgrade. The tool displays the **Upgrade Requirements – Licensing** screen. Before migrating to GMS, ensure that all appliances under Analyzer reporting are registered to the same MySonicWALL account.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



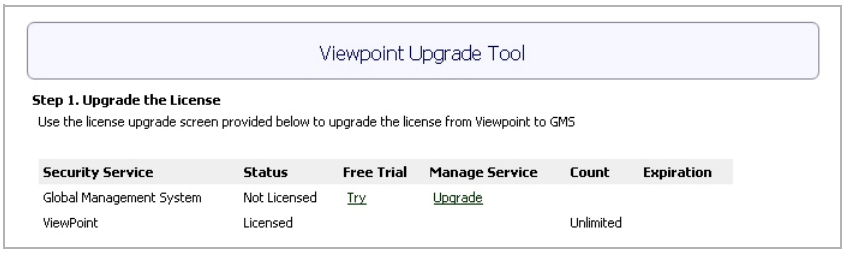
3. The **Upgrade Requirements – System** screen displays the recommended operating system, database, and hardware system requirements. Click **Proceed**.



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



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

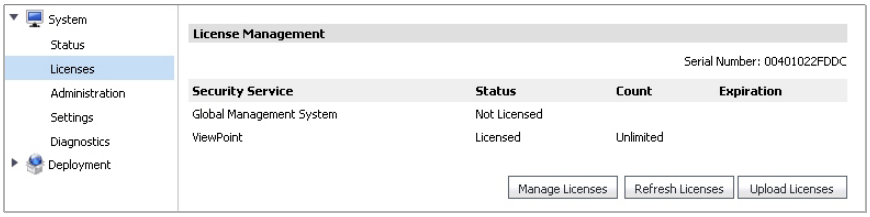


6. From this point, the upgrade process continues with the same steps for access from either the SonicWALL Analyzer interface or the Universal Management Host interface. To continue the procedure, perform the steps in the “Completing the Free Trial Upgrade” section on page 33.

Enabling the GMS Free Trial from the UMH Interface

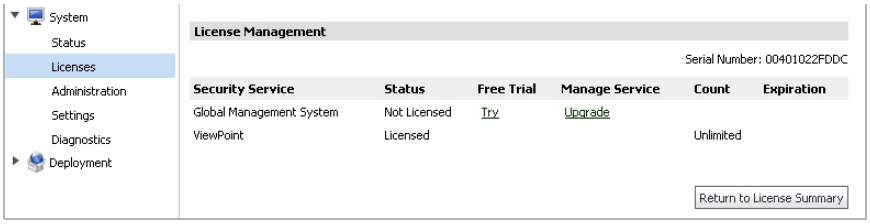
To enable the 30-day Free Trial of SonicWALL GMS from the Universal Management Host interface on your SonicWALL Analyzer system, perform the following steps:

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.

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



4. From this point, the upgrade process continues with the same steps for access from either the SonicWALL Analyzer interface or the Universal Management Host interface. To continue the procedure, perform the steps in the “Completing the Free Trial Upgrade” section on page 33.

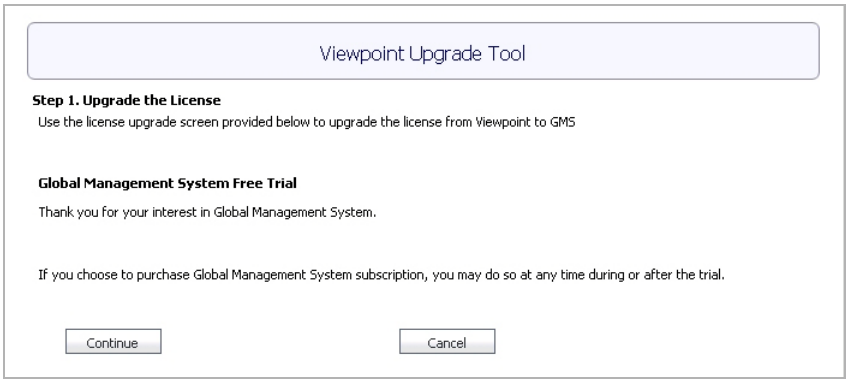
Completing the Free Trial Upgrade

This procedure provides the common upgrading steps for access from either the SonicWALL Analyzer 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:

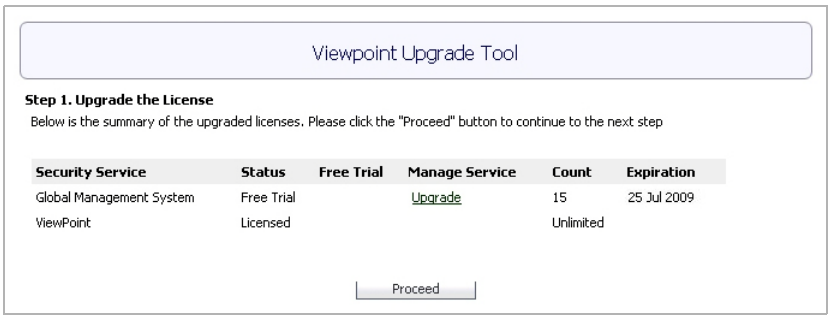
- “Enabling the GMS Free Trial from Analyzer” section on page 30
- “Enabling the GMS Free Trial from the UMH Interface” section on page 32

To continue the upgrade, perform the following steps:

1. In the Analyzer Upgrade Tool page, click the **Continue** button.



2. The next screen provides a summary of GMS and Analyzer 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**.

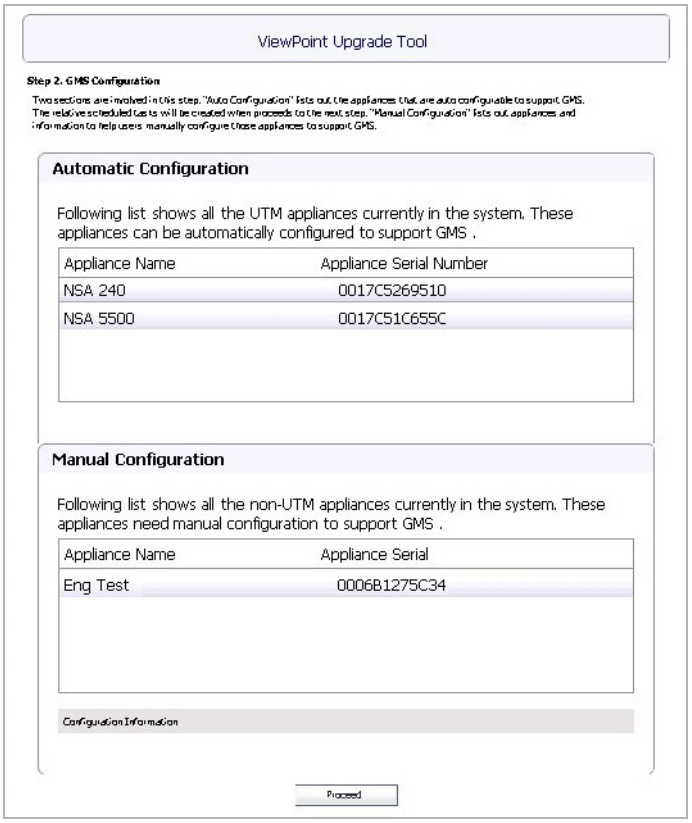


3. In the next Analyzer Upgrade Tool page, you begin the configuration for SonicWALL GMS instep 2 of the upgrade process. This page displays two sections:

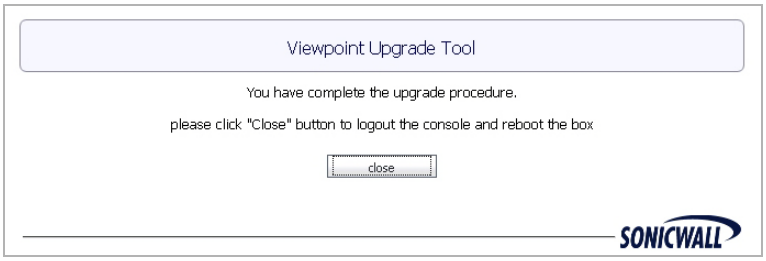
   Automatic Configuration – Contains a list of SonicWALL firewall or CSM appliances in your Analyzer installation. These appliances will be automatically configured for SonicWALL GMS management.

   Manual Configuration – Contains a list of SonicWALL Aventail, SSL-VPN, or CDP appliances in your Analyzer installation. You must manually configure these appliances for SonicWALL GMS management. See the “Configuring Appliances for GMS Management” section on page 35 for detailed instructions on enabling SonicWALL GMS management on these appliances.

   When ready, click **Proceed**.



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

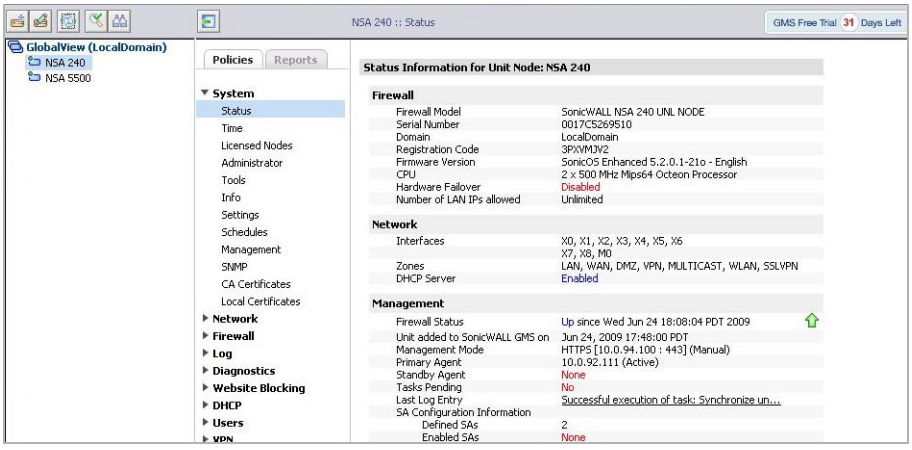


5. The GMS login page appears and requests that you reboot the system. Reboot the system. If a reboot is not performed, you may encounter problems with the correct IP Address appearing.

6. After rebooting, log in with your Analyzer 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.

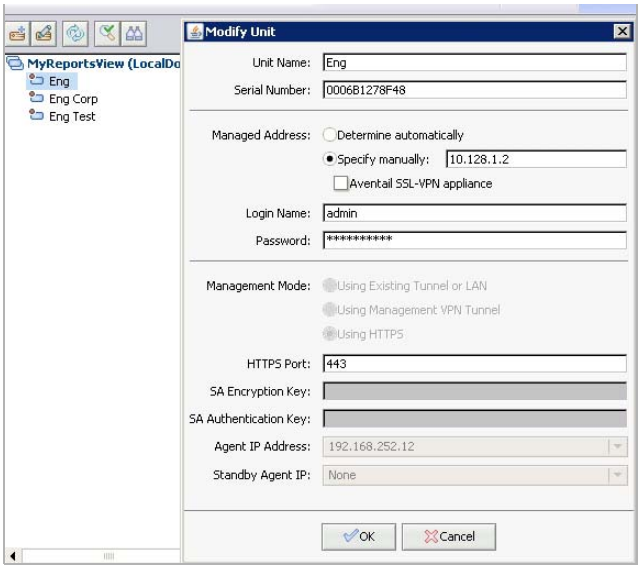


Configuring Appliances for GMS Management

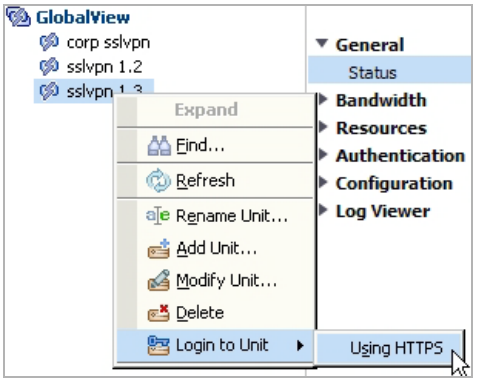
To manually configure the appliances listed in the Manual Configuration section of the Analyzer Upgrade Tool page (see Step 3. on page 34), perform the following steps for each appliance:

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**.

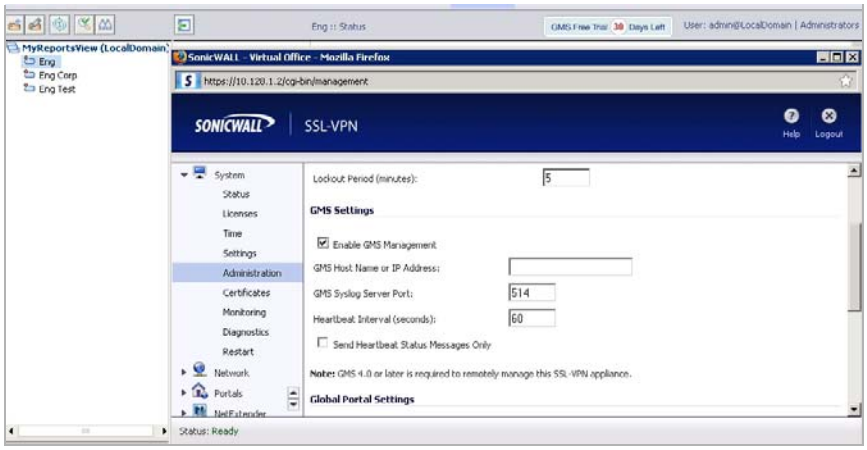
3. In the Modify Unit screen in the right pane, copy the appliance IP address in the **Managed Address** section to your clipboard, or make a note of it.



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 Analyzer Upgrade Tool page.

Purchasing a SonicWALL GMS Upgrade

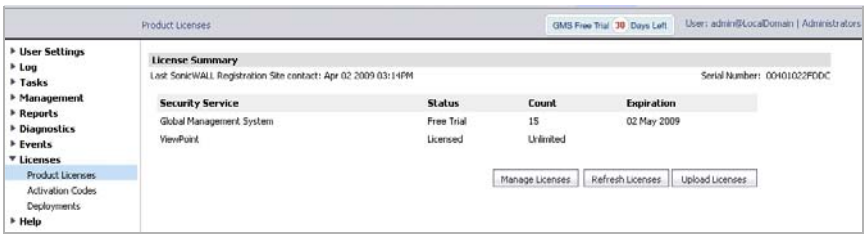
You can purchase an upgrade to SonicWALL GMS at any time during the 30-day Free Trial.

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.

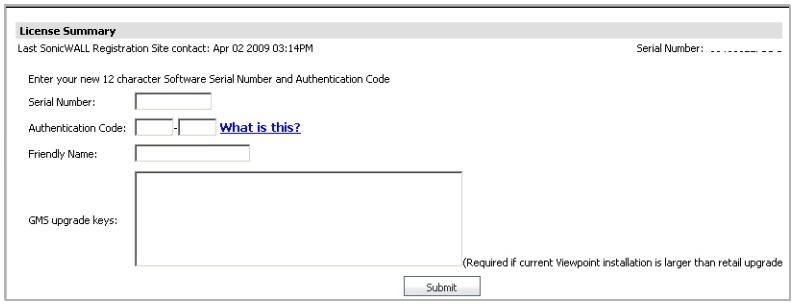
2. In the **Buy GMS** page, click **I want to upgrade to GMS now**.

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.

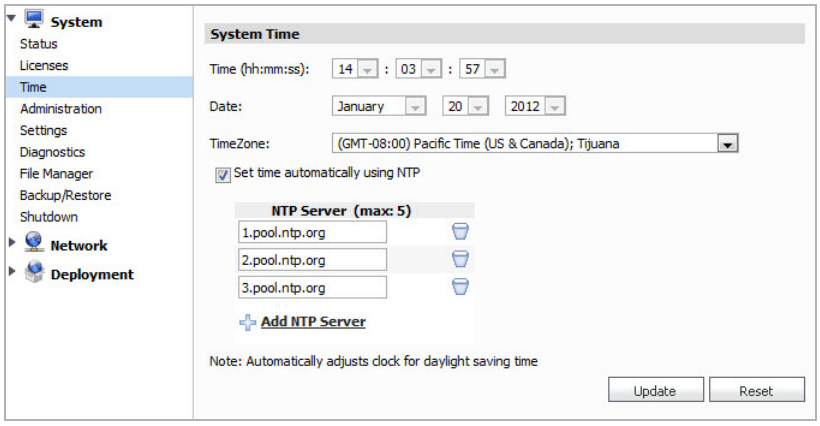
5. The next page has **Serial Number** and **Authentication Code** fields for SonicWALL GMS. You must contact your SonicWALL reseller to complete the purchase and obtain the 12-character serial number and authentication code. Type in the values to the **Serial Number** and **Authentication Code** fields.



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 Analyzer 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.

Configuring System Time Settings (Virtual Appliance)

The **System > Time** page allows you to automatically configure the date and time using NTP servers.

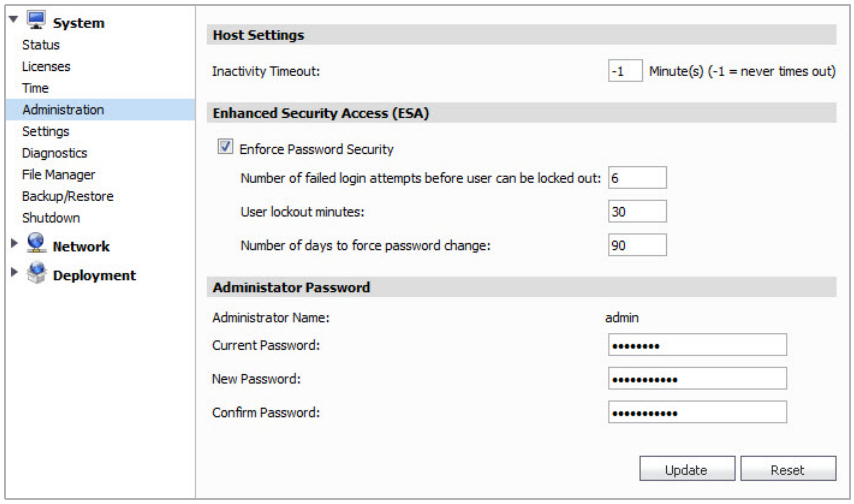


To manually select the time, under Systems Time select the time, date, and timezone.

To automatically set the time using an NTP server, select the Set time automatically using NTP checkbox. Next, select the Add NTP Server icon, and enter the IP address or domain name of the NTP server. Click the **Update** button to submit your system time configuration changes. Alternatively, click the **Reset** button to reset the system time to factory defaults.

Configuring System Administration Settings

The **System > Administration** page allows you to configure the system behavior for administrative login sessions.



Under Host Settings, enter the number of minutes of inactivity allowed before the session is logged out. A setting of **-1** allows an unlimited amount of inactivity without being logged out.

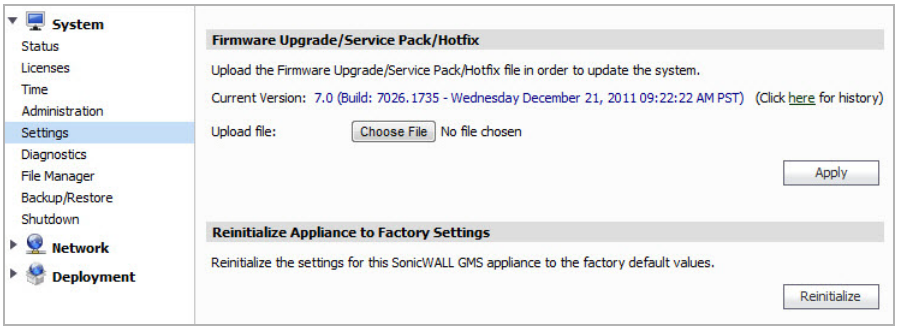
Under Enhanced Security Access, you can configure the number of failed login attempts before the admin account is locked out, and the number of minutes that the lockout lasts. You can also configure the number of days before the admin account password must be changed.

Under Administrator Password, you can change the administrator password for the Dell SonicWALL Analyzer application. Enter the current password for the system administrator (or root) account into the Current Password field, and then enter the new password into both the **New Password** and **Confirm Password** fields.

After making any changes on this page, click **Update**. To revert the fields on the page to their default settings, click **Reset**.

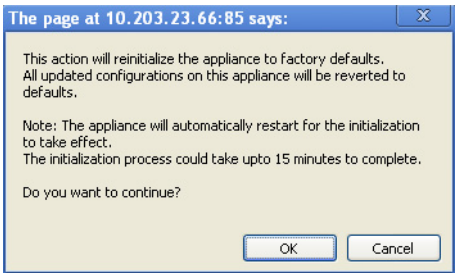
Managing System Settings

The **System > Settings** page provides a way to upload new Dell SonicWALL Analyzer software or service packs to the system. Click **Browse** to browse to the file you wish to upload, and then click **Apply**.



The page shows the current version of SonicWALL UMS, and provides a History link that displays the history of all hotfixes and firmware updates that were applied to the system.

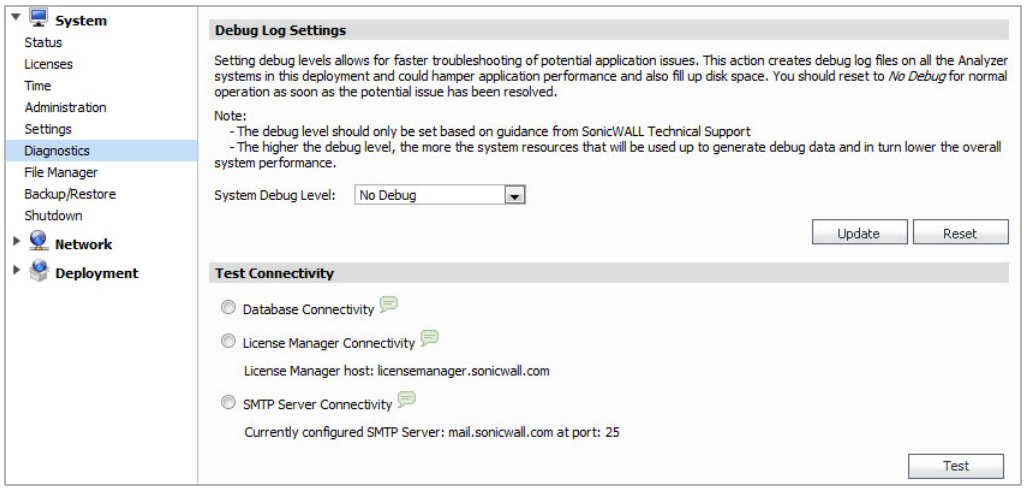
The Reinitialize Appliance to Factory Settings section allows the administrator to reset all UMH system settings to factory defaults. Click the **Reinitialize** button to reset to factory defaults. A pop-up warning message displays for the administrator to confirm this process.



Click the **OK** button, the system reboots and the reinitialization process takes 10-15 minutes to complete. Once the reinitialization process is complete, the administrator will need to login back to the management interface to confirm the system settings are now restored to factory defaults.

Using System Diagnostics

The **System > Diagnostics** page is used to set log levels, test connectivity to servers, generate Tech Support Reports, and to search and download system log files.



Under Debug Log Settings, select the log level from the **System Debug Level** drop-down list. Select from the following system debug verbosity levels:

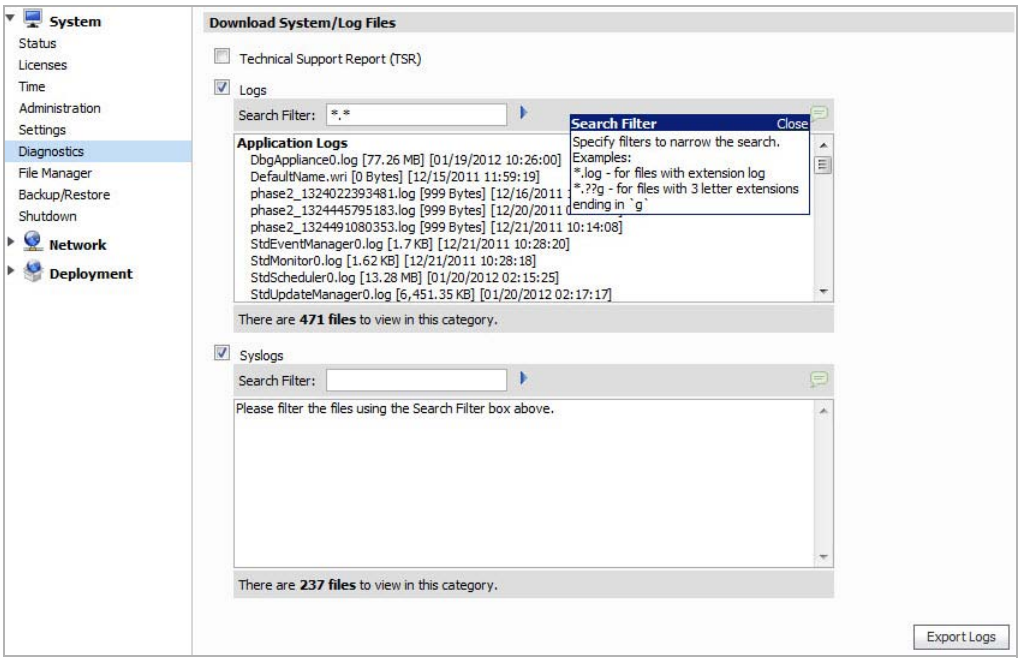
- No Debug
- Level 1 (Codepath)
- Level 2 (Simple)
- Level 3 (Logic)
- Level 4 (Detailed)
- Level 5 (Highly Detailed)

The No Debug level setting provides no debug information. And the Level 5 (Highly Detailed) setting provides the maximum debug information.

In the Test Connectivity section, select one of the following radio buttons and then click **Test** to verify connectivity to that server:

- **Database Connectivity** – Tests connectivity to the database server configured on the Deployment > Roles page.
- **License Manager Connectivity** – Type the host name or IP address into the License Manager Host field and click Test to test connectivity to that server.
- **SMTP Server Connectivity** – Tests connectivity to the SMTP server configured on the Deployment > Settings page.

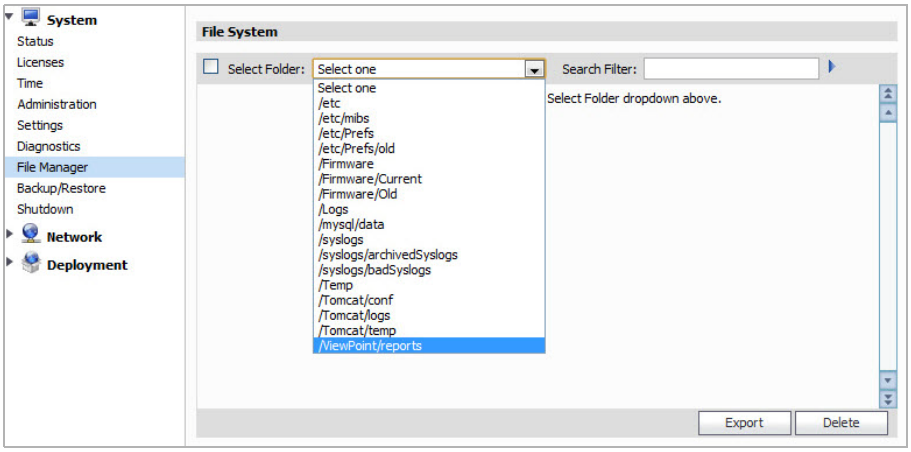
In the Download System/Log Files section, you can enter a filter, or search value, into either of the **Search Filter** fields, and then press **Enter**, to locate log entries of interest. Click the **Export Logs** button to save the log files to a file on your computer.



To generate a TSR (Technical Support Report), select the **Technical Support Report (TSR)** checkbox, and then click **Export Logs**.

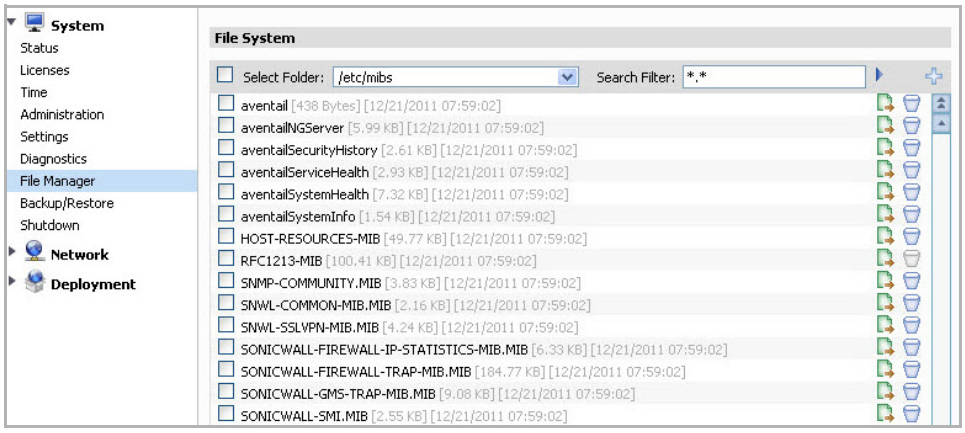
Using System File Manager (Virtual Appliance)

The **System > File Manager** page provides access to the file system. Copy files or export files to these folders. Administrators often use this page to export system settings preference files (etc/prefs) to another directory location for backup archiving.



To perform a file set export, select a folder from the pull-down menu. The page refreshes and displays the contents of the selected folder. Individual files can be exported or deleted. Click the Selected Folder checkbox to select all the files for this folder. For managing a batch of files, select multiple files from the list and click the **Export** button or **Delete** button.

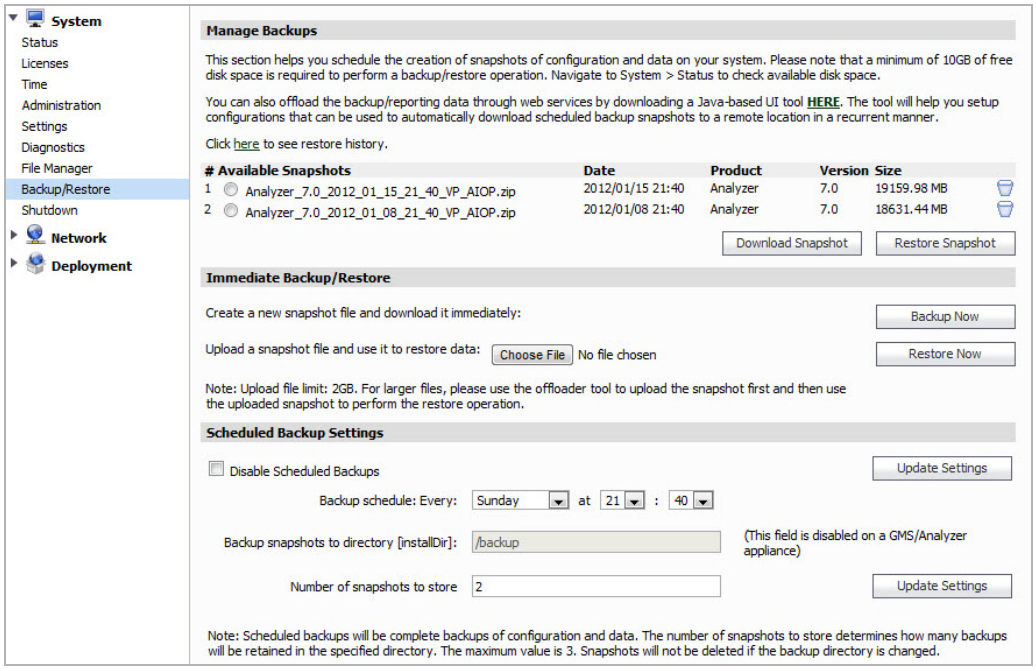
Administrators can also use the file manager to import files, such as, third-party MIB files to the directory folder for multiple-vendor solution interoperability. To import or to upload a file, select a folder from the pull-down menu. The page refreshes and displays the contents of the selected folder. In the top-right corner of the page, click the plus icon to upload a file. Next, click the **Choose File** button to open the file management dialog box. In the file management dialog box, navigate to the file you would like to upload and click the **Open** button. The selected file is now displayed next to the Choose File button. Click the **Upload** button to complete the file manager import.



Using System Backup/Restore

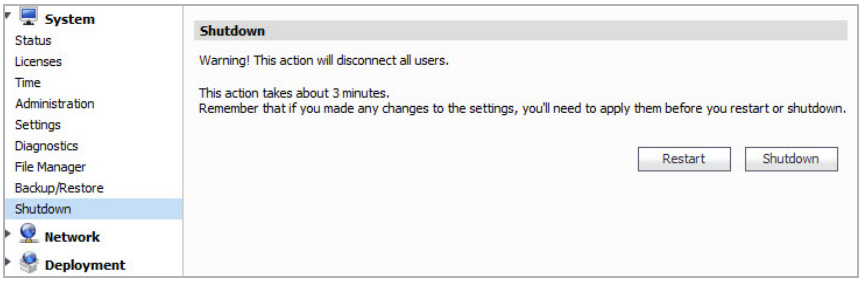
The **System > Backup/Restore** page helps you schedule and create immediate snapshots of configuration and data on your system. Note that a minimum of 10GB of free disk space is required to perform a backup/restore operation. Navigate to the **System > Status** page to verify available disk space.

You can also offload the backup/reporting data through web services by downloading a Java-based UI tool. This tool will help you setup configurations that can be used to automatically download backup snapshots to a remote location in a reoccurring schedule.



Using System Shutdown (Virtual Appliance)

The **System > Shutdown** page allows you to restart or shut down the appliance. Click the **Restart** button to reboot the system. To stop all the services and database processing, click the **Shutdown** button.



Configuring UMH Network Options (Virtual Appliance)

This section describes the tasks you can perform on the Network pages of the Dell SonicWALL Analyzer UMH system interface.

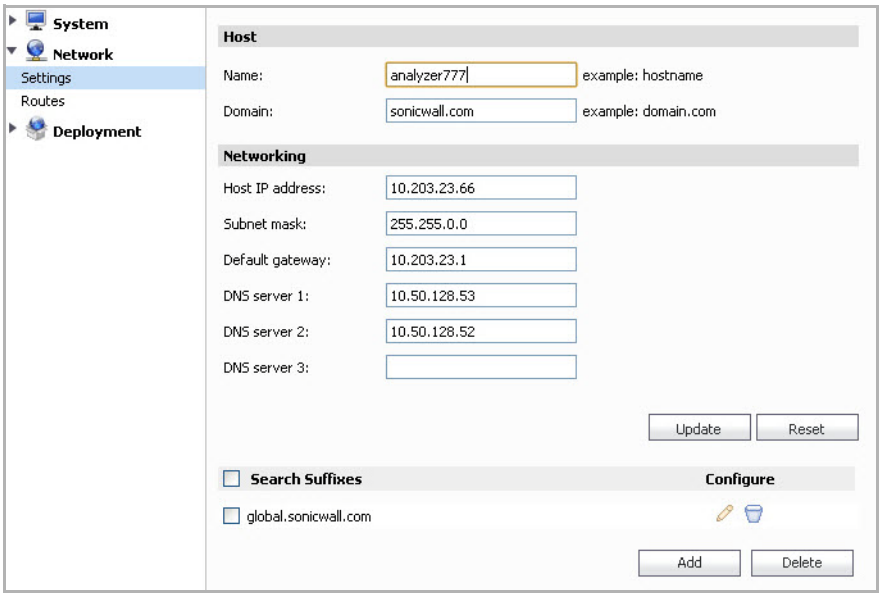
See the following sections:

- “Configuring Network Settings (Virtual Appliance)” section on page 44
- “Configuring Network Routes (Virtual Appliance)” section on page 44

Configuring Network Settings (Virtual Appliance)

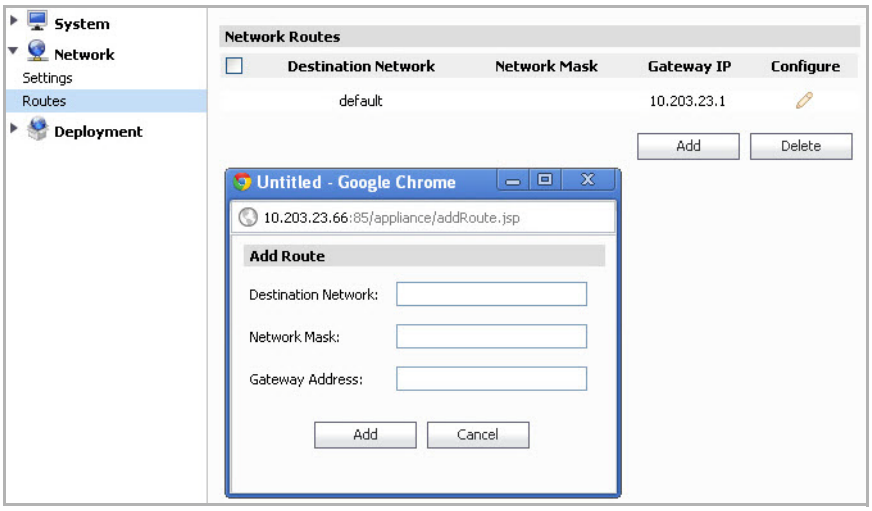
This section provides network settings configuration procedures for host, networking, and search suffixes. To configure host settings, enter host and domain name information. To configure networking settings, enter host IP address, subnet mask, default gateway, and optionally enter DNS server IP addresses. Click the **Update** button to apply the host and networking settings changes. Click the Reset button to restore these settings to factory defaults.

Search suffixes provide the ability to automatically append a DNS suffix. For example, when you ping “sonicwall” it automatically goes to “sonicwall.engineering.” To configure Search Suffixes, click the **Add** button to include multiple search suffixes. And to remove Search Suffixes, click the checkbox next to the Search Suffixes list, and click the **Delete** button.



Configuring Network Routes (Virtual Appliance)

This section provides configuration procedures to add network routes. To add a network route, enter a destination network IP address, network mask, and gateway, and click the **Add** button. To edit the default network route, click the configure icon. When multiple network routes are added to the list, selecting the checkbox at the top-left corner of the page selects all the added network routes. Click the **Delete** button to remove a network route from the list. **Note**: the default network route cannot be deleted.



Configuring UMH Deployment Options

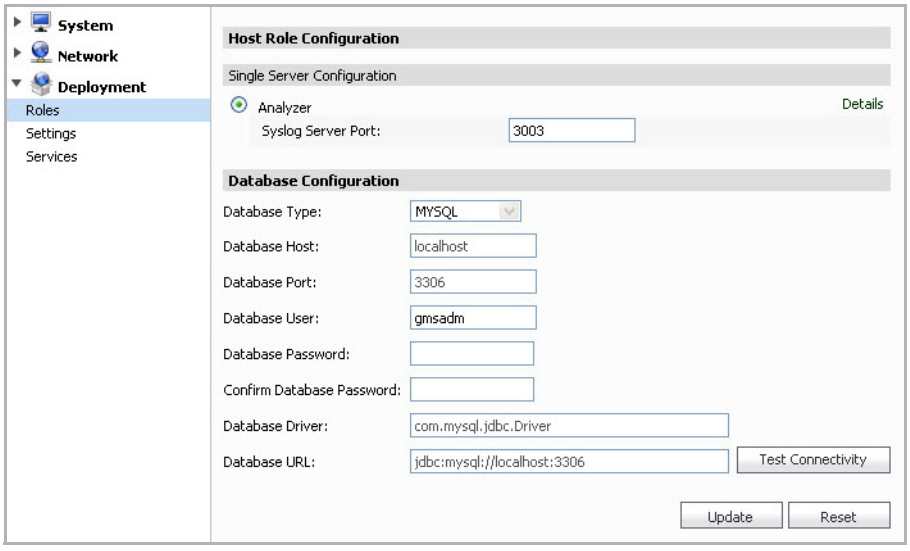
This section describes the tasks you can perform on the Deployment pages of the Dell SonicWALL Analyzer UMH system interface.

See the following sections:

- “Configuring the Deployment Role” section on page 45
- “Configuring Deployment Settings” section on page 47
- “Controlling Deployment Services” section on page 49

Configuring the Deployment Role

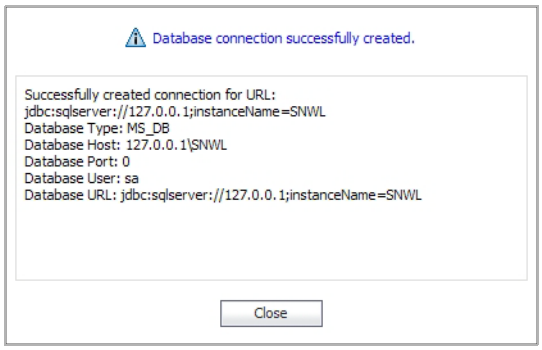
In a Dell SonicWALL Analyzer installation, the **Deployment > Roles** page provides a way to configure the syslog port and the database settings, and to test database connectivity.



To set the syslog port, enter the port number into the **Syslog Server Port** field.

Under Database Configuration, to provide credentials with which Dell SonicWALL Analyzer will access the database, enter the account user name into the **Database User** field, and enter the account password into both the **Database Password** and **Confirm Database Password** fields. Additionally, you can enter a **Database Driver** file name and the **Database URL** for an explicit directory path location.

To test connectivity to the database server, click the **Test Connectivity** button. A pop-up message displays the database connectivity status.

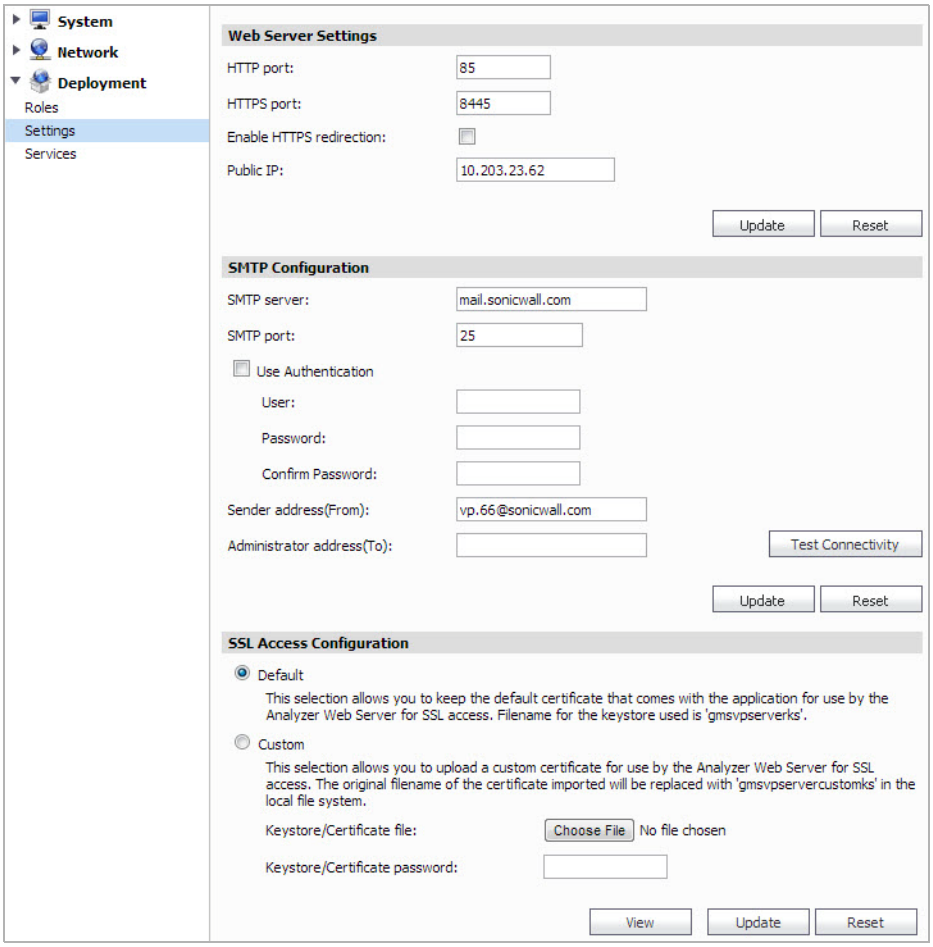


When finished, click **Update** to apply the changes. To revert the fields on the page to their default settings, click **Reset**.

Configuring Deployment Settings

This section describes the UMH/UMA **Deployment > Settings** page, used for Web port, SMTP, and SSL access configuration.

The Deployment > Settings page is identical in both the UMH and UMA management interfaces, except for the left navigation pane which shows the Network menu item on the UMA.



See the following sections:

- “Configuring Web Server Settings” section on page 47
- “Configuring SMTP Settings” section on page 48
- “Configuring SSL Access” section on page 48

Configuring Web Server Settings

Web Server Settings configuration is largely the same on any role:

1. Navigate to **Deployment > Settings > Web Server Settings** in the /appliance management interface.
2. To use a different port for HTTP access to the Dell SonicWALL Analyzer, type the port number into the **HTTP Port** field. The default port is 80.

If you enter another port in this field, the port number must be specified when accessing the appliance management interface or SonicWALL GMS management interface. For example, if port 8080 is entered here, the appliance management interface would be accessed with the URL: http://<*IP Address*>:8080/appliance/.

3. To use a different port for HTTPS access to the Dell SonicWALL Analyzer, type the port number into the **HTTPS Port** field. The default port is 443.

   If you enter another port in this field, the port number must be specified when accessing the appliance management interface or SonicWALL GMS management interface. For example, if port 4430 is entered here, the appliance management interface would be accessed with the URL: https://<*IP Address*>:4430/appliance/.

4. Click the **Enable HTTPS Redirection** checkbox to redirect HTTP to HTTPS when accessing the Analyzer management interface.
5. In the **Public IP** text-field, enter the public IP or FQDN of the outside web services.
6. When you are finished configuring the Web Server Settings, click the Update button.

Configuring SMTP Settings

The SMTP Configuration section allows you to configure an SMTP server name or IP address, a sender email address, and an administrator email address. You can test connectivity to the configured server.

To configure SMTP settings:

1. Navigate to the **Deployment > Settings** page under the **SMTP Configuration** section.
2. Type the FQDN or IP address of the SMTP server into the **SMTP server** field.
3. If the SMTP server in your deployment is set to use authentication, click the **Use Authentication** checkbox. This option is necessary for all outgoing Analyzer emails to properly send to the intended recipients. Enter the username in the **User** field, and enter/confirm the password in the **Password** and **Confirm Password** fields. This is the username/password that is used to authenticate against the SMTP server.
4. Type the email address from which mail will be sent into the **Sender address** field.
5. Type the email address of the system administrator into the **Administrator address** field.
6. To test connectivity to the SMTP server, click **Test Connectivity**.
7. To apply your changes, click **Update**.

Configuring SSL Access

The SSL Access Configuration section allows you to configure and upload a custom Keystore/Certificate file for SSL access to the GMS appliance, or select the default local keystore.

To configure SSL access:

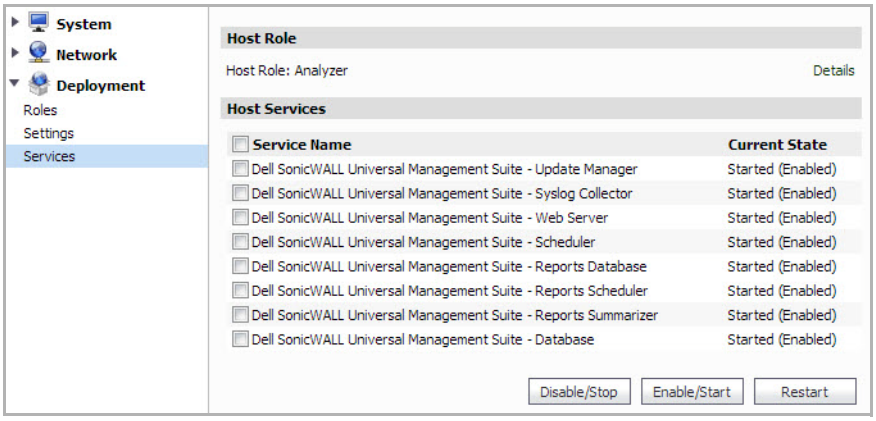
1. Navigate to the **Deployment > Settings** page under **SSL Access Configuration** section.
2. Select the **Default** radio button to keep, or revert to, the default settings, where the default GMS Web Server certificate with 'gmsvpserverks' keystore is used.
3. Select the **Custom** radio button to upload a custom keystore certificate for GMS SSL access.
4. In the **Keystore/Certificate file** field, click the **Browse** button to select your certificate file.

Note Your custom file is renamed to ‘gmsvpservercustomks’ after upload.

5. Type the password for the keystore certificate into the **Keystore/Certificate password** field.
6. Click the **View** button to display details about your keystore certificate.
7. Click the **Update** button to submit your changes.

Controlling Deployment Services

The **Deployment > Services** page provides a list of the services that are running on your system as part of Dell SonicWALL Analyzer. It also provides a way to stop or start any of the services.



To stop a service that is currently Enabled, select the checkbox for that service and then click **Disable/Stop**.

To start a service that is currently Disabled, select the checkbox for that service and then click **Enable/Start**.

To restart a service that is either Enabled or Disabled, select the checkbox for that service and then click **Restart**.

CHAPTER 3

Provisioning and Adding Dell SonicWALL Appliances

This chapter describes how to provision and add Dell SonicWALL appliances to the Dell SonicWALL Analyzer. All Dell SonicWALL appliances must be provisioned before adding them to the Dell SonicWALL Analyzer.

This chapter contains the following sections:

Provisioning Dell SonicWALL Appliances

This section describes how to configure Dell SonicWALL appliances to support Dell SonicWALL Analyzer.

Note Prior to adding a unit to Analyzer, the provisioned Dell SonicWALL appliance needs to be registered with License Manager. And during registration, make sure the provisioned Dell SonicWALL appliance has a valid Analyzer license—one Analyzer license for each Dell SonicWALL appliance.

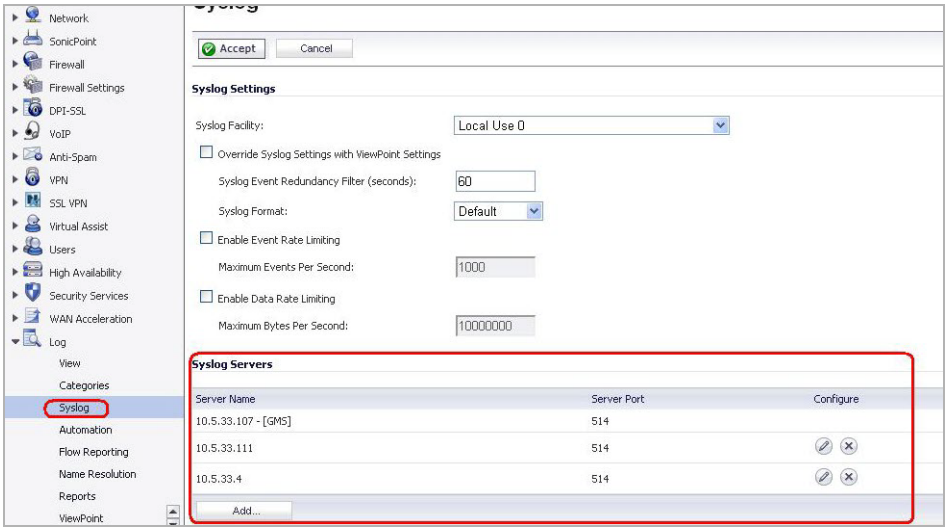
Provisioning a Dell SonicWALL Firewall Appliance

To provision a Dell SonicWALL firewall appliance for Dell SonicWALL Analyzer, perform the following:

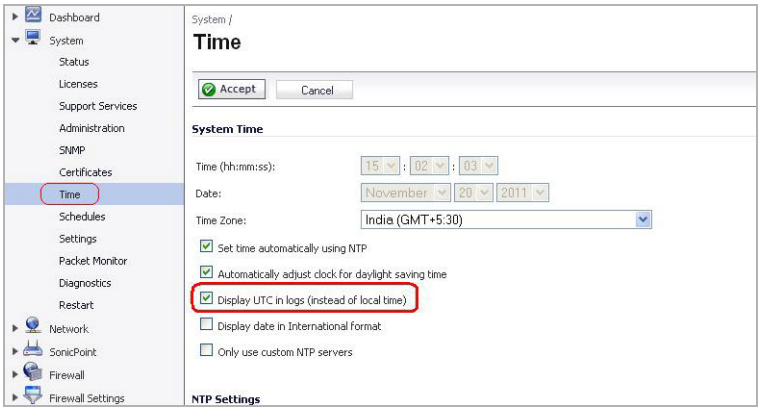
Step 1 Log in to the firewall appliance. Navigate to the **Log > Syslog** page.

Step 2 In Syslog Servers, click the **Add** button.

Step 3 Enter the Analyzer IP address to start sending syslogs. The Analyzer service should be activated. Set the log in UTC format and log category.



Step 4 Navigate to the **System > Time** page, and enable the **Display UTC in logs (instead of local time)** checkbox.



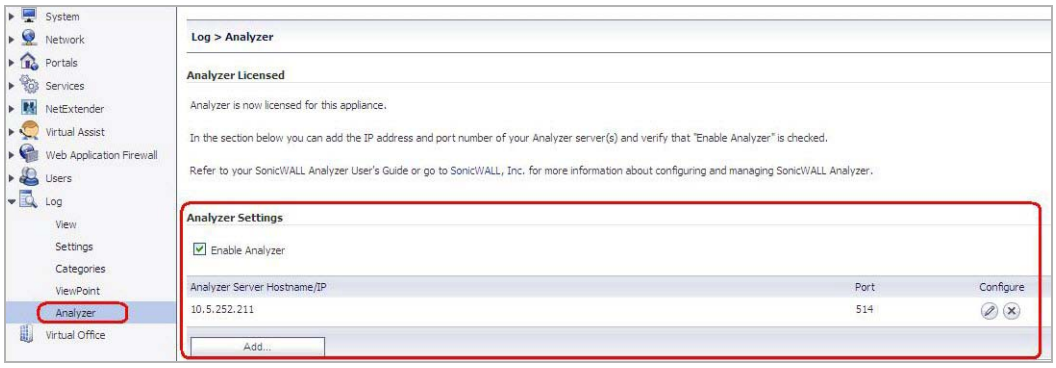
Provisioning a Dell SonicWALL SRA SMB Appliance

To provision a Dell SonicWALL SRA SMB appliance for Dell SonicWALL Analyzer, perform the following:

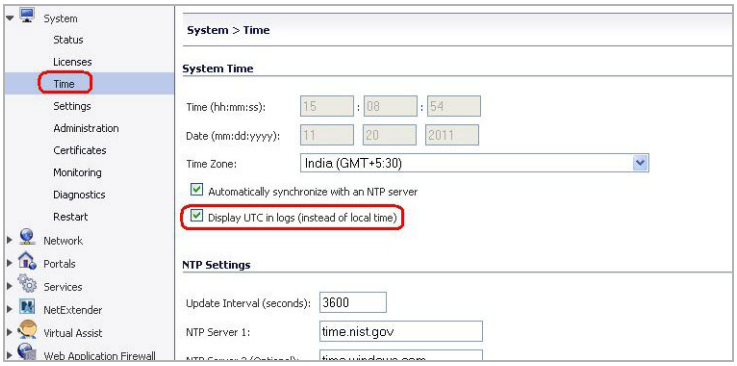
Step 1 Log in to the SRA SMB appliance. Navigate to the **Log > Analyzer** page.

Step 2 In Analyzer Settings, click the **Enable Analyzer** checkbox.

Step 3 Click the **Add** button to add the Analyzer IP address, this starts sending syslogs.

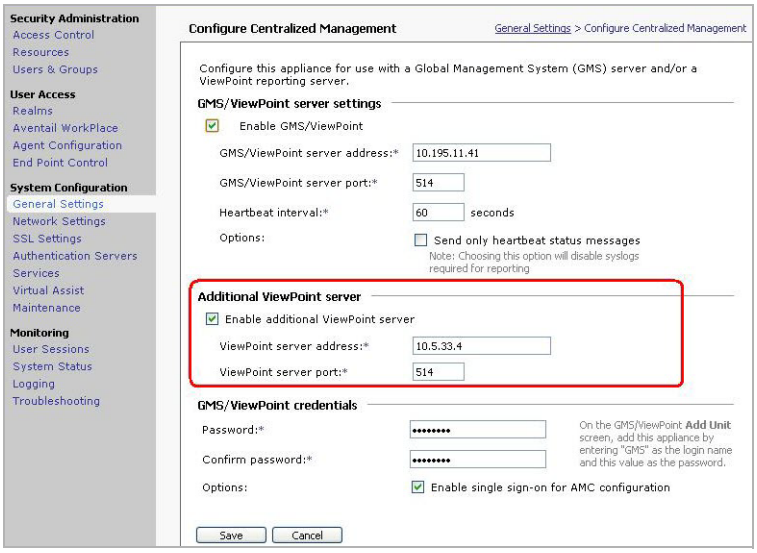


Step 4 Navigate to the **System > Time** page, and enable the **Display UTC in logs (instead of local time)** checkbox.



Provisioning a Dell SonicWALL E-Class SRA Series Appliance

Currently there is no Analyzer settings implementation in SonicWALL E-Class SRA series appliances. To add Analyzer reporting support, use the **Additional ViewPoint** settings in the **General Settings > Configure Centralized Management** screen. And enter the Analyzer IP address and port number to start sending syslog.



Provisioning a Dell SonicWALL CDP Appliance

Currently there is no Analyzer settings implementation in Dell SonicWALL CDP appliances. To add Analyzer reporting support, use the **Analyzer** settings in the **Settings > SMB** screen. In Active Report, select the **Enable** checkbox. And enter the Analyzer IP address and port number to start sending CDP syslog.

Adding Dell SonicWALL Appliances to Dell SonicWALL Analyzer

Dell SonicWALL Analyzer checks with the Dell SonicWALL licensing server when you add an appliance, so it is important that Dell SonicWALL Analyzer has Internet access to the server.

Dell SonicWALL Analyzer can communicate with Dell SonicWALL appliances through HTTP or HTTPS.

Note

A SonicWALL appliance might already be registered to a different MySonicWALL account, in this case the “Register to MySonicWALL.com” task cannot be executed, and will remain in the scheduled tasks queue. To take full advantage of Analyzer managed appliances, it is important that either the managed appliance is not registered when it is added into Analyzer, or it is registered to the same MySonicWALL.com account as the Analyzer system that is managing the appliance.

For information on adding, modifying, and deleting units, refer the following sections:

- Adding Dell SonicWALL Appliances on page 55
- Modifying Dell SonicWALL Appliance Settings on page 56
- Deleting Dell SonicWALL Appliances from Analyzer on page 57

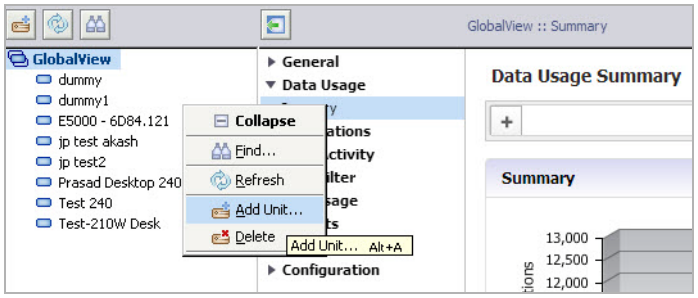
Adding Dell SonicWALL Appliances

To add a Dell SonicWALL appliance using the Dell SonicWALL Analyzer management interface, perform the following:

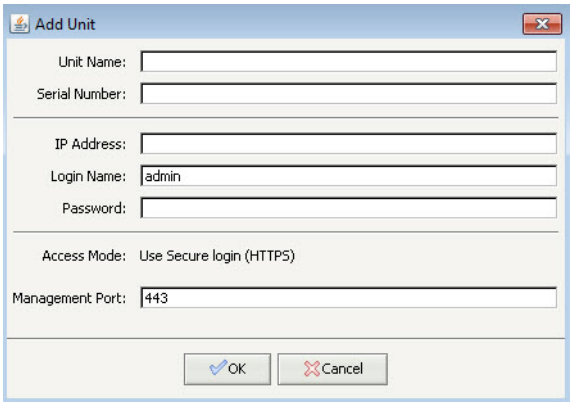
Step 1 Click the appliance tab that corresponds to the type of appliance that you want to add:

- **Firewall**
- **SRA**
- **CDP**

Step 2 Expand the Dell SonicWALL Analyzer tree and select the group to which you will add the Dell SonicWALL appliance. Then, right-click the group and select **Add Unit** from the pop-up menu. To not specify a group, right-click lRight-click an open area in the left pane (TreeControl pane) of the Dell SonicWALL Analyzer management interface and select **Add Unit** or click the **Add Unit i**con in the tool bar.



The Add Unit dialog box appears:



Step 3 Enter a descriptive name for the Dell SonicWALL appliance in the **Unit Name** field. Do not enter the single quote character (‘) in the **Unit Name** field.

Step 4 Enter the serial number of the Dell SonicWALL appliance in the **Serial Number** field.

Step 5 Enter the IP address of the Dell SonicWALL appliance in the **IP Address** field.

Step 6 Enter the administrator login name for the Dell SonicWALL appliance in the **Login Name** field.

Step 7 Enter the password used to access the Dell SonicWALL appliance in the **Password** field.

Step 8 For Access **Mode**, select from the following:

Step 9 The Dell SonicWALL appliance will be connected with HTTPS by default.

Step 10 Enter the port used to connect to the Dell SonicWALL appliance in the **Management Port** field (default port for is HTTPS: 443).

Step 11 Click **OK**. The new Dell SonicWALL appliance appears in the Analyzer management interface. It will have a yellow icon that indicates it has not yet been successfully acquired.

Step 12 Analyzer will then attempt to set up an HTTPS connection to access the appliance. Analyzer then reads the appliance configuration and acquires the SonicWALL appliance for reporting. This will take a few minutes.

After the Dell SonicWALL appliance is successfully acquired, its icon turns blue, its configuration settings are displayed at the unit level, and its settings are saved to the database.

Modifying Dell SonicWALL Appliance Settings

If you make a mistake or need to change the settings of an added Dell SonicWALL appliance, you can manually modify its settings or how it is managed.

To modify a Dell SonicWALL appliance, perform the following steps:

1. Right-click the appliance name in the left pane of the Analyzer UI and select **Modify Unit** from the pop-up menu. The Modify Unit dialog box appears.
2. The Modify Unit dialog box contains the same options as the Add Unit dialog box. For descriptions of the fields, see the“Adding Dell SonicWALL Appliances to Dell SonicWALL Analyzer” section on page 55.

When you have finished modifying options, click **OK**. The Dell SonicWALL appliance settings are modified.

Deleting Dell SonicWALL Appliances from Analyzer

To delete a Dell SonicWALL appliance from Dell SonicWALL Analyzer, perform the following steps:

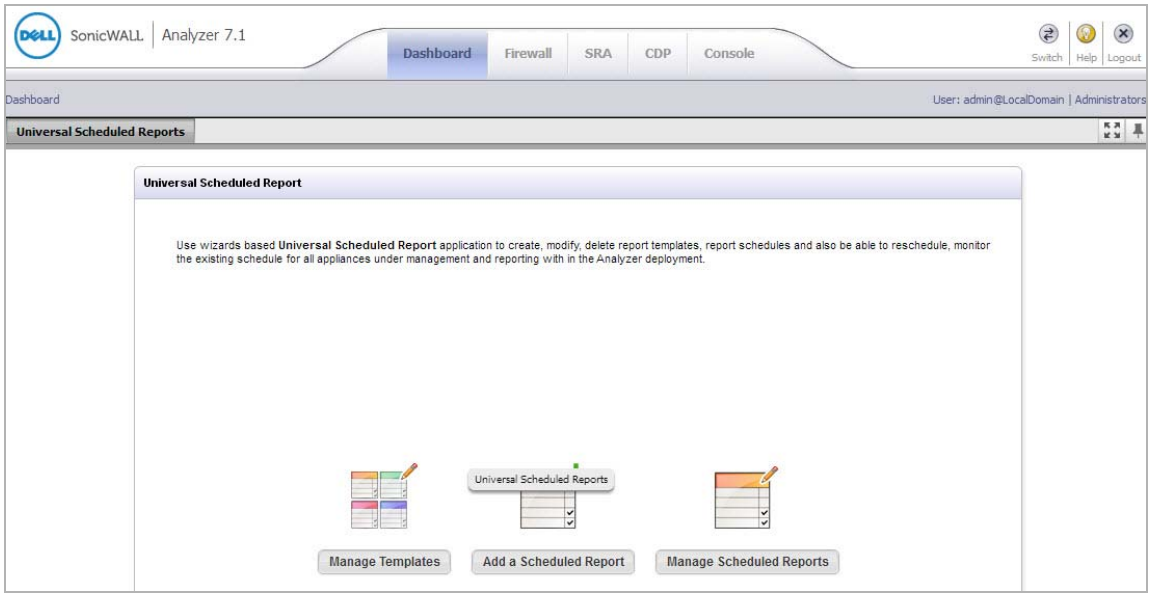
1. Right-click on a Dell SonicWALL appliance in the left pane and select **Delete** from the pop-up menu.
2. In the warning message that displays, click **Yes**. The SonicWALL appliance is deleted from SonicWALL Analyzer.

After the deleting the Dell SonicWALL appliance from Analyzer, unprovision the unit as a best practice. To unprovision the unit, log in to the Dell SonicWALL appliance and disable Analyzer management to avoid sending unnecessary syslogs to the Analyzer host.

CHAPTER 4

Using the Dashboard Panel

The Dashboard control bar provides top-of-the page menu items for customizing the settings of this page. When the Dashboard loads after SonicWALL Analyzer login, the control bar is displayed and then becomes hidden until you place your mouse cursor at the top of the page as shown below. You can lock the control bar by clicking on the “pin the control bar” icon.

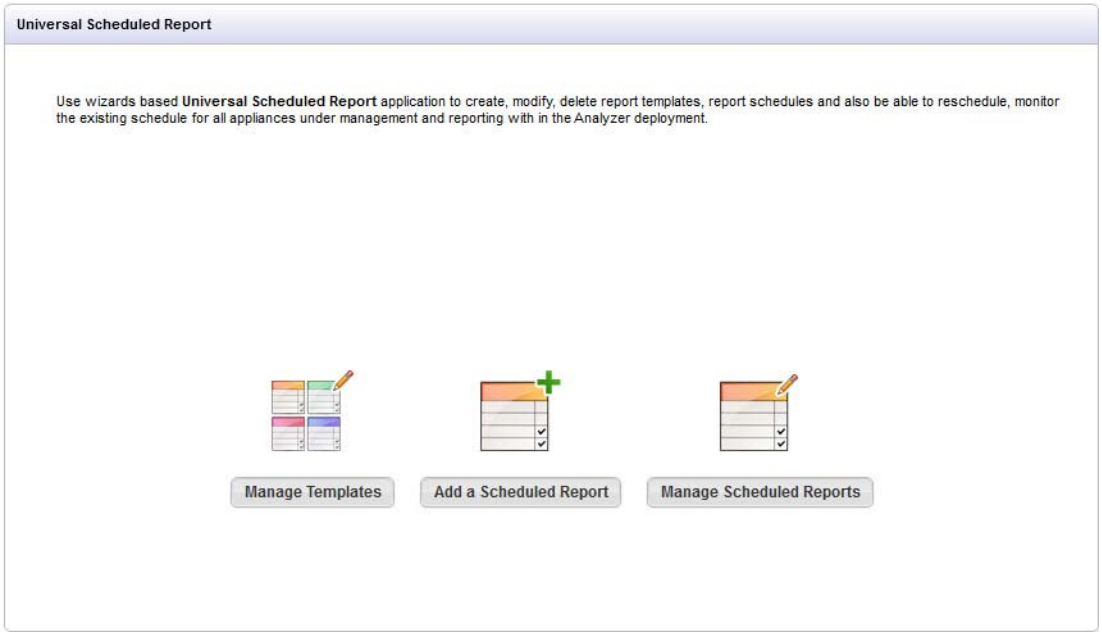


The Dashboard control bar provides the following components:

- **Universal Scheduled Reports**—Includes Universal Scheduled Reports Wizard to create report templates.
- **Switch to Full Screen**—The four arrows in four corners icon enables the page into full-screen mode.
- **Pin Control Bar**—The pin icon allows you to keep the Dashboard control bar always on.

Using the Universal Scheduled Reports Application

Scheduled Reporting has been an essential reporting component since the initial release of the Dell SonicWALL Analyzer product. It provides management interfaces to let the user setup schedules and configure reports to be exported in a periodic fashion and in various report formats. A typical scheduled report configuration is broken down by functionality and by nodes. Users need to navigate to separate tabs to configure scheduled reports for different nodes. The Universal Scheduled Reporting application streamlines the configuration processes to unify and enhance the existing functionality to the system-wide usage patterns. This allows the user to collect report data from multiple appliances and create a single global report.



To configure the Universal Scheduled Reports application, refer to the following sections:

- Using the Manage Templates Component, page 60
- Adding a Scheduled Report Component, page 66
- Managing the Scheduled Reports Component, page 79

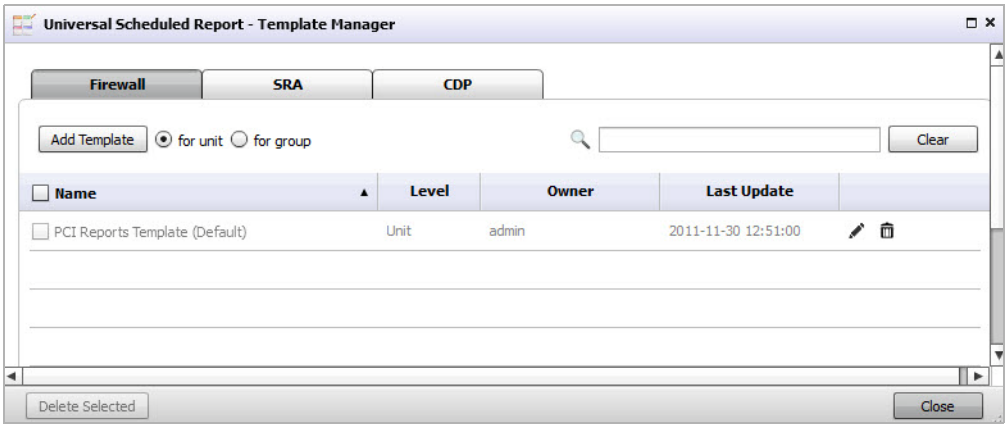
Using the Manage Templates Component

Manage Templates are used to create a template that makes up the list of reports at group level or unit level. The list of available reports for each of the product types are abstract, so all the available reports in system are presented here. The report list contains the appliance firmware and shows all the available reports in Dell SonicWALL Analyzer for the appliance. This decision on which report is applicable to a particular firmware version (for example, Application Intelligence is for SonicOS 5.8 and above) is made at run time when the scheduled report engine is ready to create the report. The schedule report creation and the template usage is detailed in this section.

Adding a Template

Preform the following steps to add a template using the Template Manager:

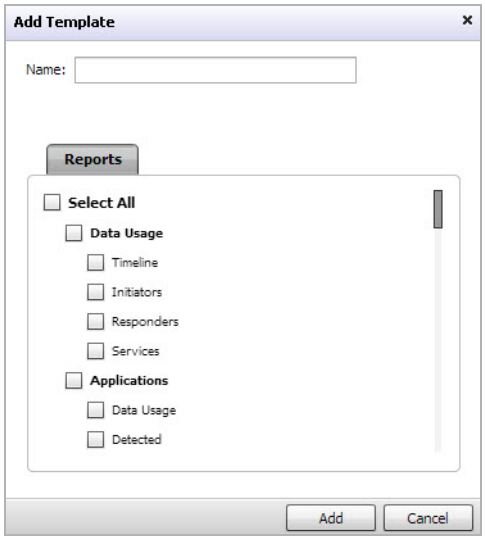
Step 1 Navigate to the **Universal Scheduled Report > Manage Templates** page.



Step 2 Choose the tab for the appliance you wish to add a template to.

Step 3 Select the option for either a **unit** or **group** template.

Step 4 Click the **Add Template** button.



Step 5 Enter a name for your template.

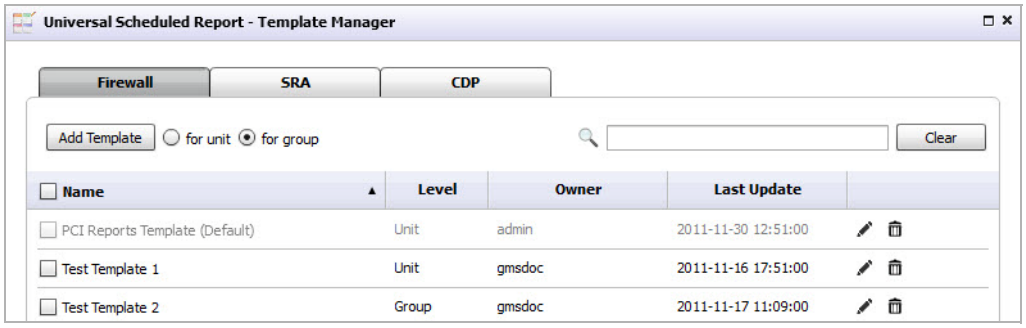
Step 6 The **Visible To Non-Administrators** checkbox is disabled by default, select the checkbox to enable this option. This allows the end users to view list of all the report templates at a read-only level.

Step 7 Select the checkbox next to the **Reports** you wish to use for this template.

Step 8 Select the checkbox next to the **Policies** you wish to use for this template.

Step 9 Click the **Add** button.

The configured template is now populated in the Template Manager list.



Editing an Existing Template

This section details the configuration procedures for editing an existing template. The Universal Scheduled Report > Template Manager allows you to filter the template list by Name, Level, Owner, and Last Update. Follow the steps below to use the search option to find and edit an existing template.

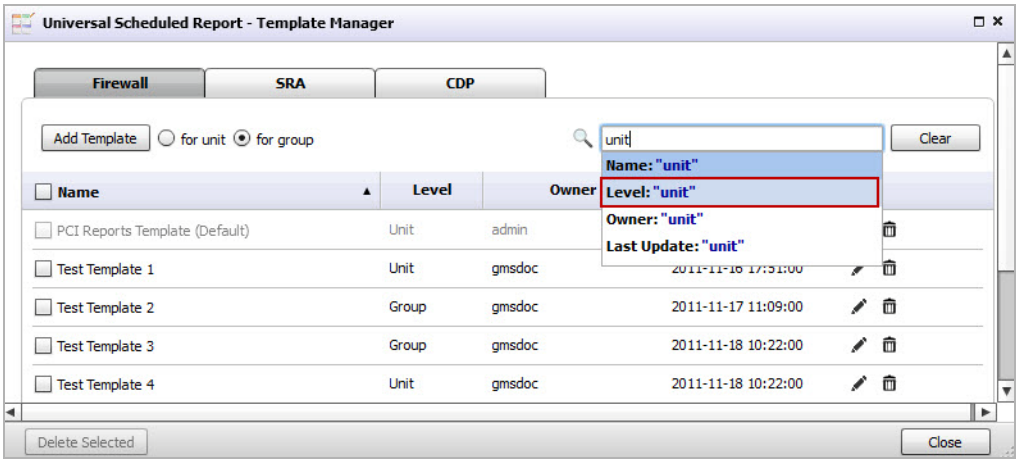
Searching for an Existing Template

Step 1 Navigate to the **Universal Scheduled Reports > Manage Template** page.

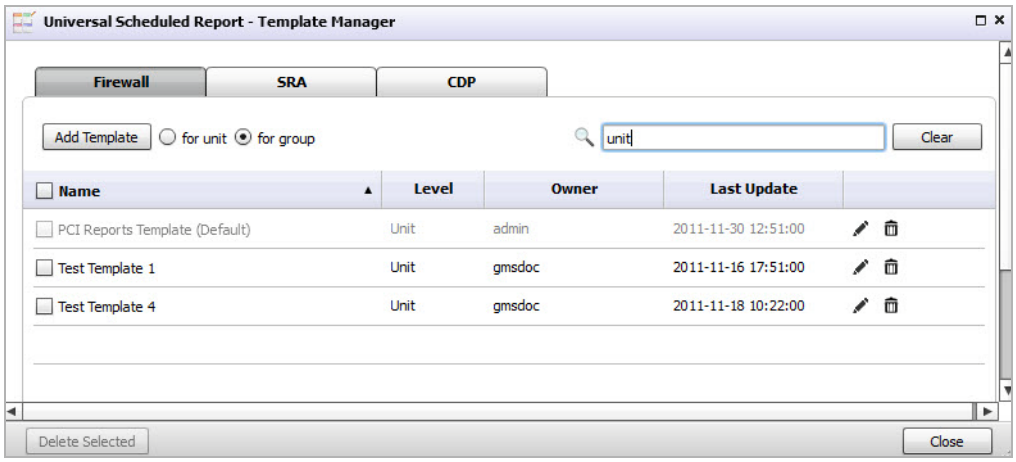
Step 2 Click the search text field, then enter your search criteria.

A pull-down appears under the search text field

Step 3 Select a filter for your search criteria by clicking **Name**, **Level**, **Owner**, or **Last Update** from the search pull-down list. In this example, we are entering “unit” for the search criteria and filtering the search results by level.



The Template Manager window displays the latest search results. Notice the template list now only shows report templates for level: units.



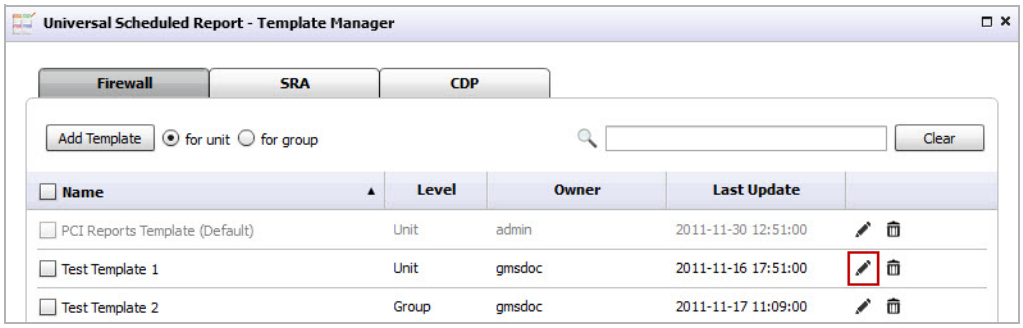
Note To clear your search results and return the reports template list back to default, click the **Clear** button.

Editing an Existing Template

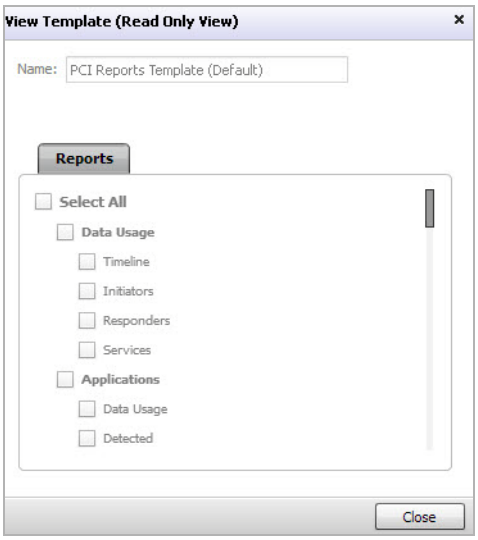
Now that you found an existing template using the search filter, it is time to use the edit option.

Warning **Editing an existing template also changes the associated scheduled reports (if applicable).**

Step 1 Click the icon for the report you wish to edit.



The Edit Template window displays



Step 2 Edit the name for your template.

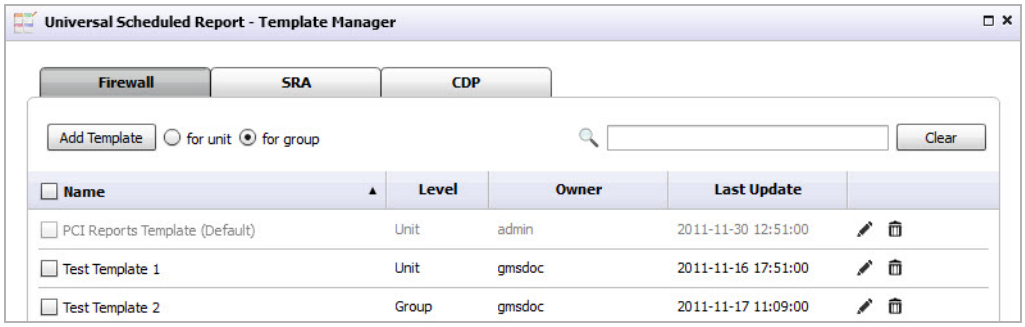
Step 3 The **Visible To Non-Administrators** checkbox is disabled by default, select the checkbox to enable this option. This allows the end users to view list of all the report templates at a read-only level.

Step 4 Select the checkbox next to the **Reports** you wish to use for this template.

Step 5 Select the checkbox next to the **Polices** you wish to use for this template.

Step 6 Click the **Update** button.

The configured template is now populated in the Template Manager list.



Deleting a Template

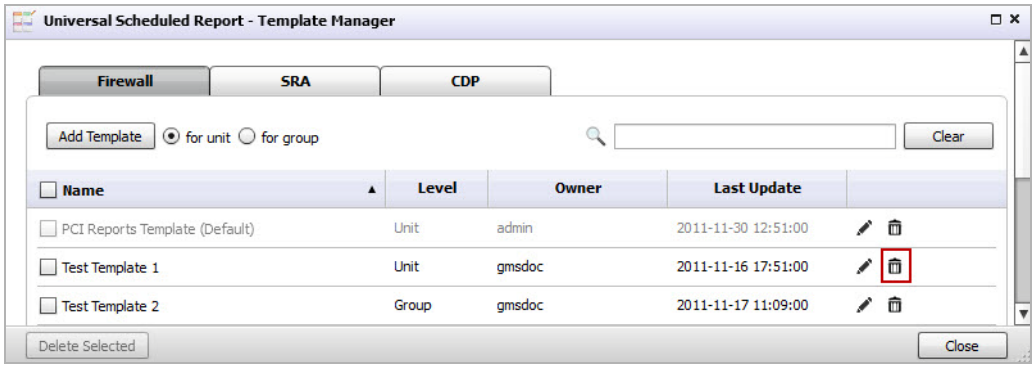
The Template Manager offers three different ways to delete a template: deleting a single template, deleting multiple templates, or deleting all templates. Use the "Searching for an Existing Template" section to search for templates to delete. Preform the following steps to delete a Universal Scheduled Report Template(s):

Warning **Deleting a template(s) creates a cascading task to remove it from the Scheduled Reports that are using this template.**

Deleting a Single Template

Step 1 Navigate to the **Universal Scheduled Reports > Manage Template** page.

Step 2 Click the icon for the template you wish to delete from the Template Manager list.

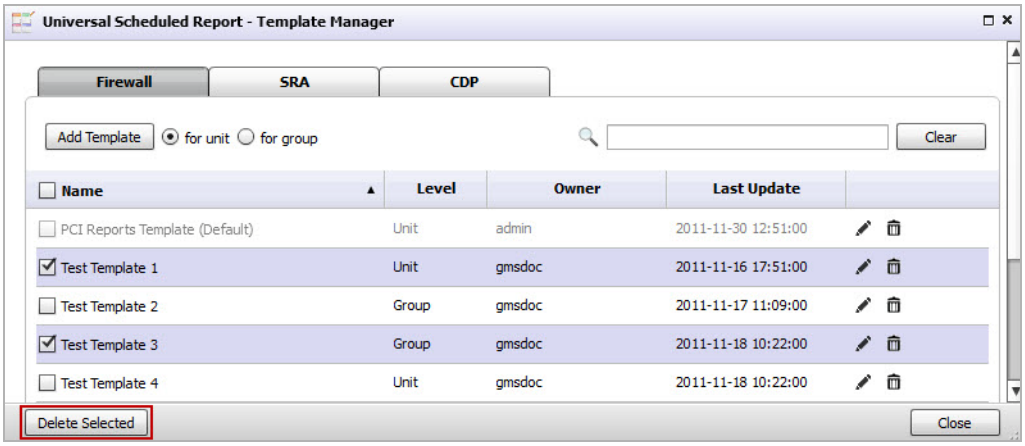


Deleting Multiple Templates

Step 1 Navigate to the **Universal Scheduled Reports > Manage Template** page.

Step 2 Click the checkboxes for the templates you wish to delete.

Step 3 Click the **Delete Selected** button. This button is grayed out by default until a checkbox is selected.

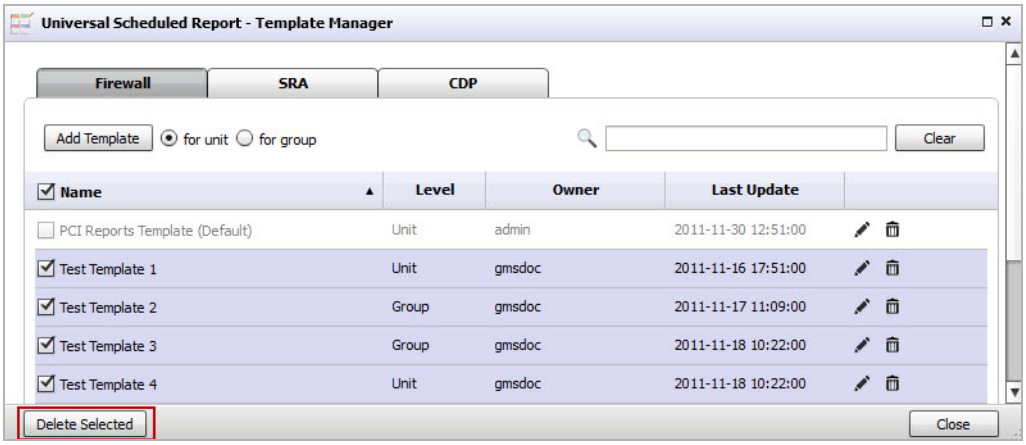


Deleting all Templates

Step 1 Navigate to the **Universal Scheduled Reports > Manage Template** page.

Step 2 Select the **Name** checkbox, this selects all templates in the list.

Step 3 Click the **Delete Selected** button. This button is grayed out by default until a checkbox is selected.



Adding a Scheduled Report Component

Using Universal Scheduled Reports gives you the ability to schedule reporting for multiple appliances at once, combined into a single report. The Scheduled Reporting is a wizard based tool that guides you through the steps for creating a scheduled report by manually selecting reports from the report listing or picking a template created in the “Using the Manage Templates Component” section, selecting a theme (cover logos, font colors, title, sub title), reporting properties (out put format, language), scheduling a type (weekly, monthly), and choosing a destination (up to 5 email addresses can be added for a single report). This section contains the following subsections:

- “Searching for a Group or Device” section on page 66
- “Creating a Universal Scheduled Report” section on page 69

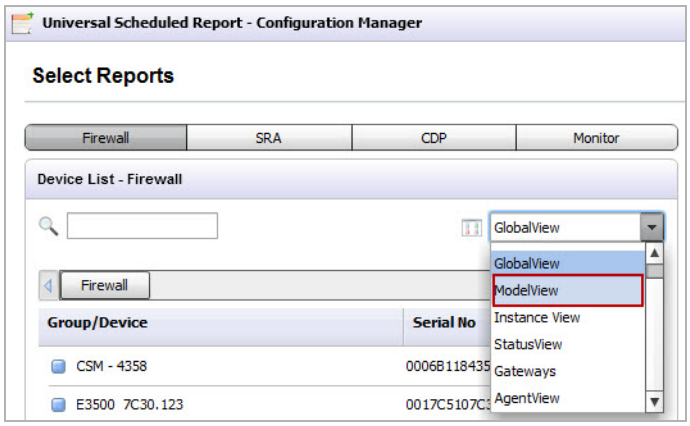
Searching for a Group or Device

The Search option allows you to filter the Group/Device list by manually entering a device in the search text field and selecting it from the search pull-down list. You can further filter the Group/Device list by clicking the View pull-down and selecting a view type. The following example guides you through the Device List search process, detailing the versatility of the Universal Scheduled Reports > Configuration Manager search options.

Example

In this example we are using the Configuration Manager search options to find a SonicWALL TZ 210 wireless-N device in the Device List.

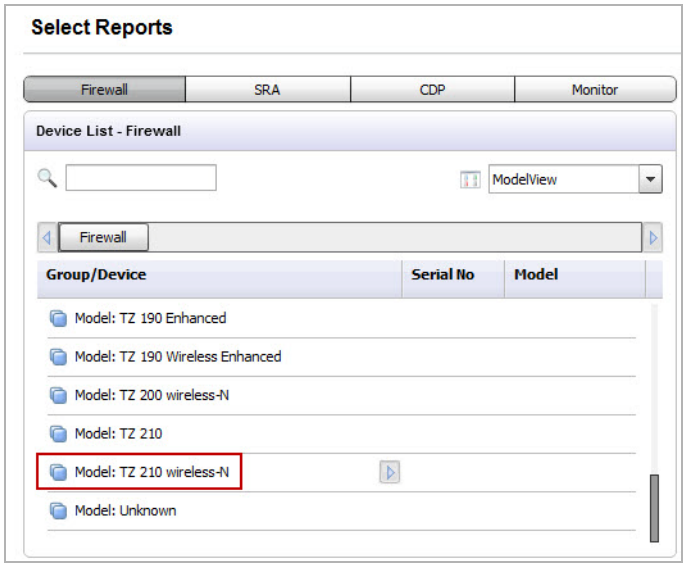
Step 1 Navigate to **Universal Scheduled Reports > Add A Scheduled Report**.
Note: The Monitor tab is only available for SonicWALL GMS.



Step 2 Select the **Firewall** tab, located at the top of the Configuration Manager window.

Step 3 Click the **View** pull-down, then select a view type from the list. In this example we are selecting **Model View** (Global View is selected by default), since we are searching for an exact appliance model. You can also filter the Device List by Firmware View, Global View, Instance View, Status View, or Gateway.

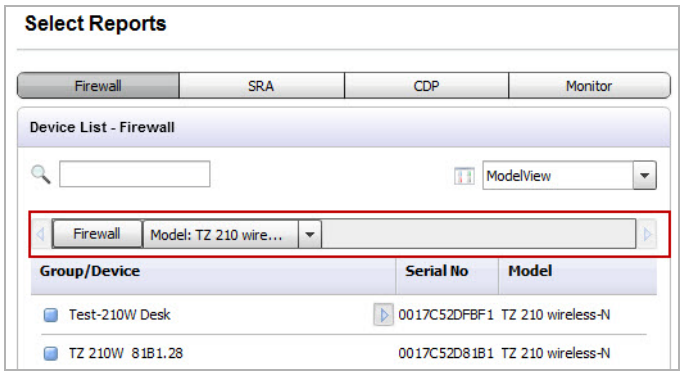
The Device List now displays all the appliance models.



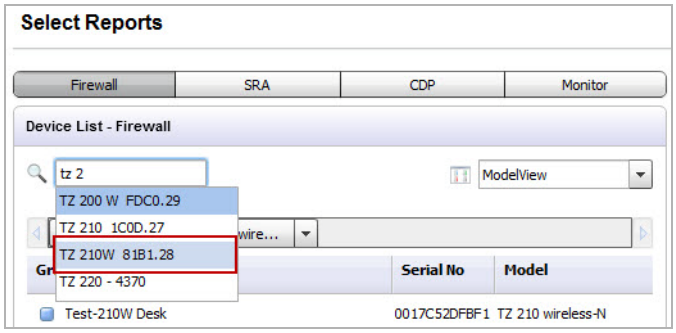
Step 4 Select the **Model: TZ 210 wireless-N**.

A list of devices for that appliance model displays.

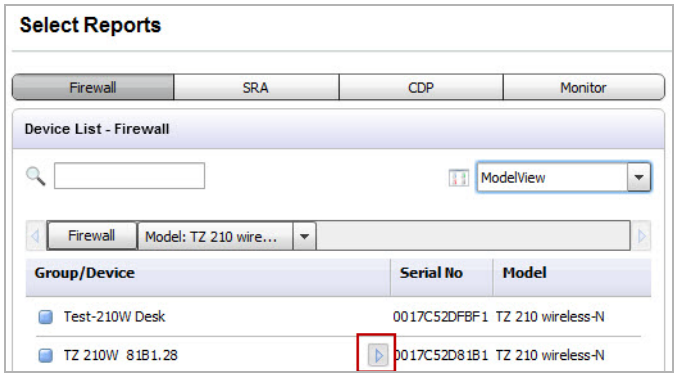
Note Notice that the search history bar populates each time you filter the list. You can use this to navigate back to previous search results.



You can also click the **Search** text-box (if you know the exact name of the device), then manually enter the device name or select the device from the pull-down list.



Step 5 Click the icon to schedule a report for that appliance. Refer to the "Creating a Universal Scheduled Report" section for configuration procedures.



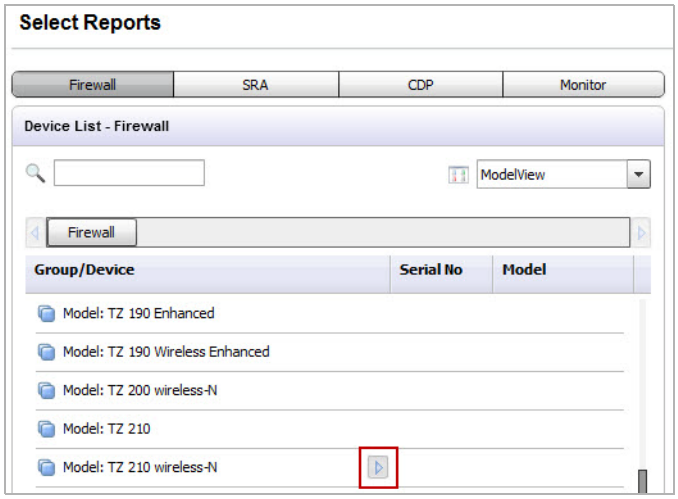
Creating a Universal Scheduled Report

The Universal Scheduled Reports > Configuration Manager allows you to create a single report for multiple appliance models/devices at a group and unit level. The following example guides you through the report configuration process, including: Selecting Reports, General Information, and Theme Information, detailing the versatility of Universal Scheduled Reporting.

In this example we are using the Configuration Manager to schedule a single report for a Firewall appliance model (group level) and SRA devices (unit level).

Selecting Reports

Step 1 Navigate to **Universal Scheduled Reports > Add a Scheduled Report**.
Note: The Monitor tab is only available for SonicWALL GMS.

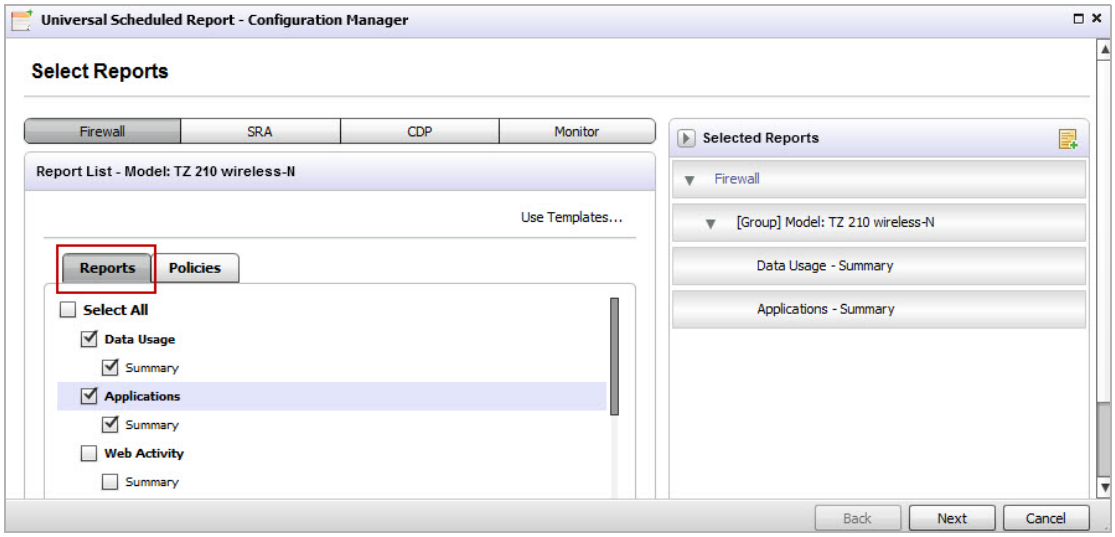


Step 2 Select the **Firewall** tab, located at the top of the Configuration Manager window.

Step 3 Search for the TZ 210 wireless-N model group. Refer to steps 1-3 in the "Searching for a Group or Device" section.

Step 4 Click the icon for the **Model: TZ 210 wireless-N**.

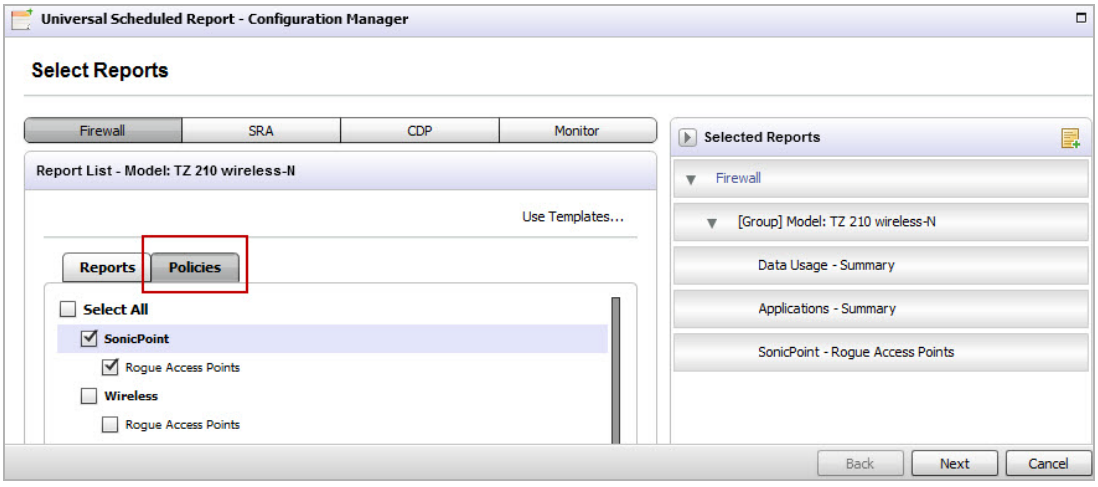
The Reports tab displays in the Reports List.



Step 5 Click the **Reports** tab, then select the checkboxes for reports you wish to include or click the **Use Templates** link to choose a template you created.

Note When you select reports in the Reports and Policies tabs, they populate in the list of Selected Reports located on the right side of the Configuration Manager page. The Selected Reports panel allows you to organize the list by dragging and dropping reports/devices, collapse the reports lists for each device (clicking the arrow next to the device name), and add a note to a report/device.

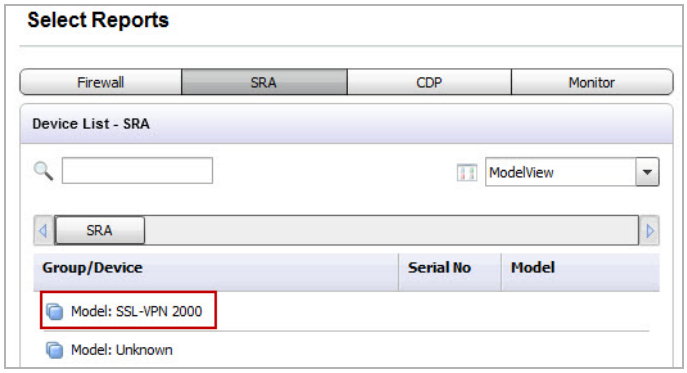
Step 6 Click the **Policies** tab, then select the checkboxes for the policies you wish to include or click the **Use Templates** link to choose a template you created.



The reports for the Firewall model group are now selected, next is choosing reports for the SRA device.

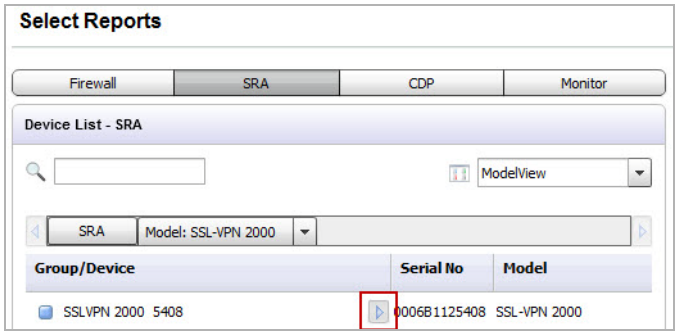
Step 7 Select the **SRA** tab.

The SRA models display in the Device List.



Step 8 Click the **Model: SRA 2000**.

The Device List displays all the SRA 2000 devices.

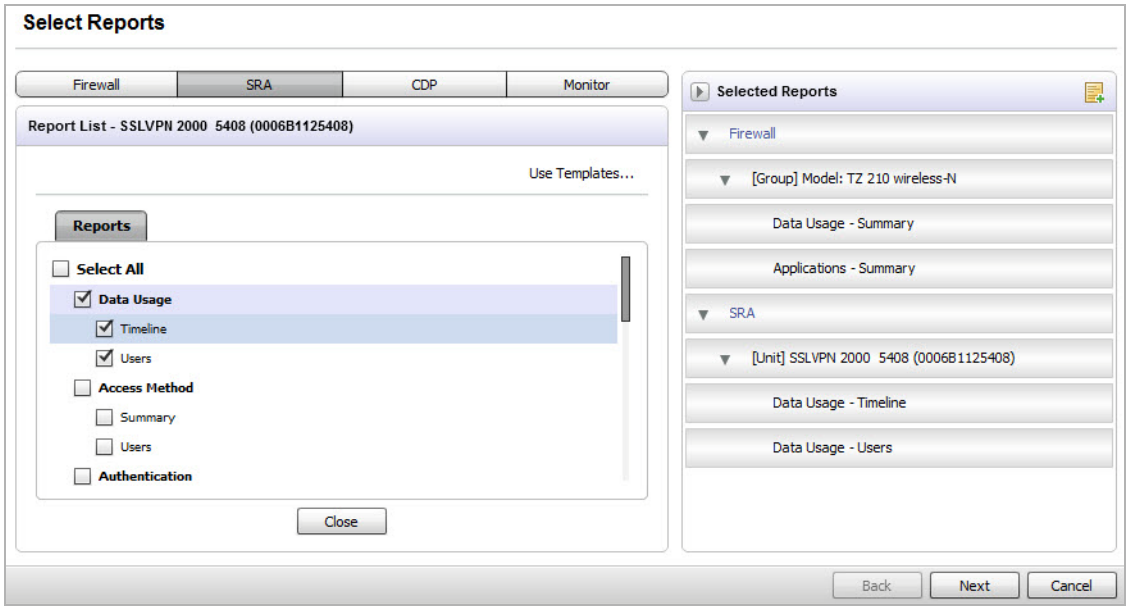


Step 9 Click the icon for the SRA 2000 5408.

The Reports window displays in the Reports List.

Step 10 Select the checkboxes for the reports you wish to include or click the **Use Templates** link to choose a created template.

Note The SRA only offers a Reports tab (no Policies tab).

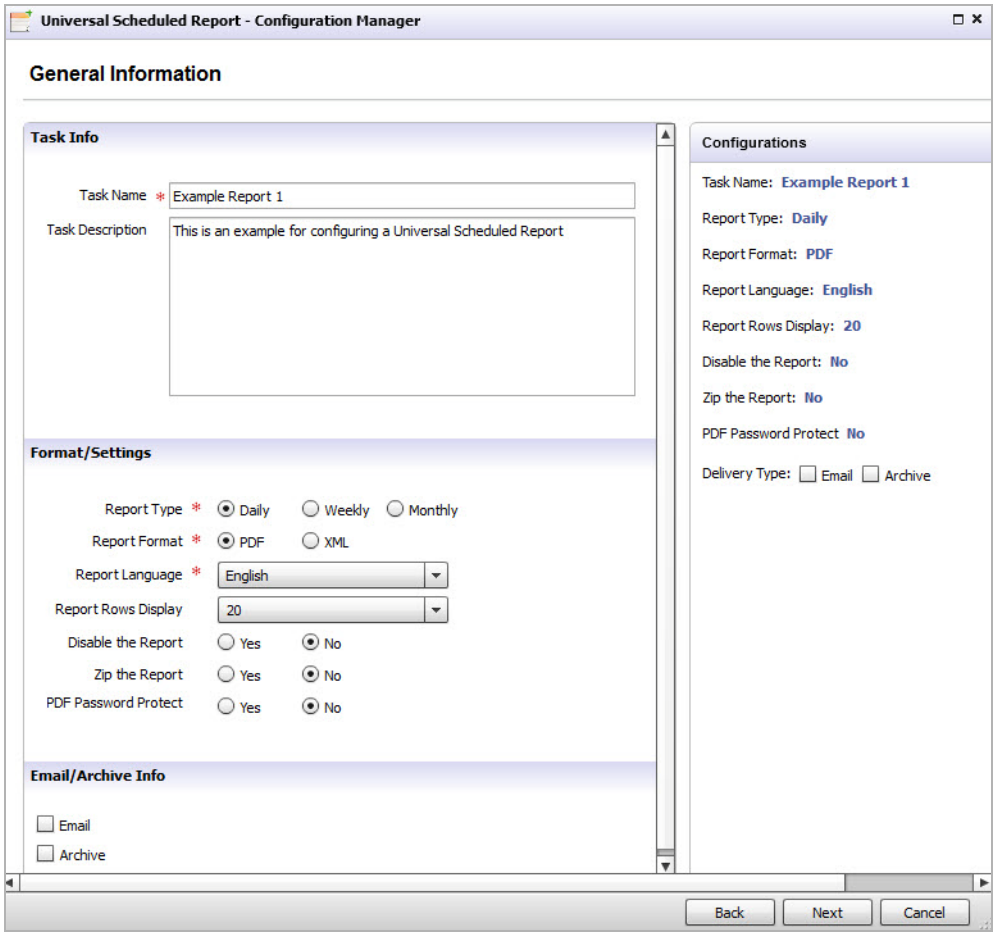


Step 11 Click the **Next** button.

General Information

The General Information page displays.

Note The settings entered in the Task Info, Format/Settings, and Email/Archive Info sections, populate in the Configurations panel located on the right side of the General Information page.

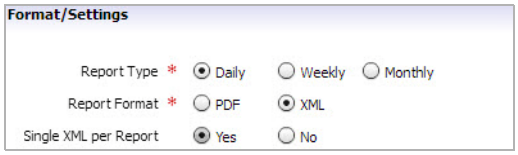


Step 12 Enter the following in the **Task Info** panel:

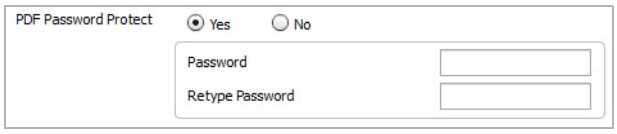
- Task Name: **Example Report 1**
- Task Description: **This is an example for configuring a Universal Scheduled Report**

Step 13 Select the following in the **Format/Settings** panel:

- Report Type: **Daily**, Weekly, or Monthly
- Report Format: **PDF** or XML
  If XML is selected, the following changes to the management interface occur:
  - The **Single XML per Report** radio buttons display. If you select the **Yes** radio button, one XML file per report will be generated. In this scenario, the number of XML files created is equal to the number of reports chosen.



  - The ZIP Password Protection option is grayed out.
- Report Language: **English**, Japanese, Chinese (Simplified), Chinese (Traditional), or Spanish
- Report Rows Display: **20**, 50, 100
- Disable the Report: Yes or **No**
- Zip the Report: Yes or **No**
- PDF Password Protect: Yes or **No** (If Yes is selected, a pop-up window appears and prompts you to enter the Password)

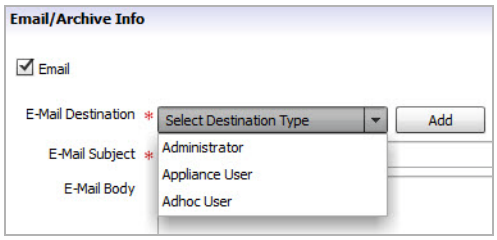


Step 14 Click the archive checkbox to save a PDF report to a new folder.

Step 15 Perform the following in the **Email / Archive Info** panel:

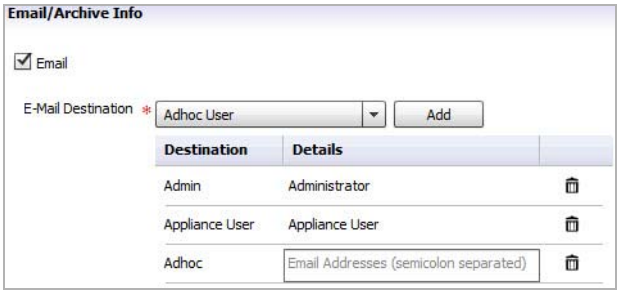
- Click the **E-mail** checkbox to send a PDF report to an email account or alias.

  The Email configuration options display.



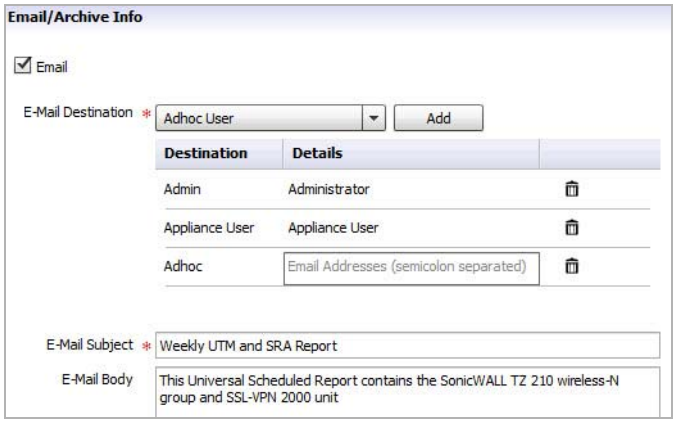
  - Click the **E-Mail Destination** pull-down, then select an **Administrator**, **Appliance User**, or Enter multiple **Adhoc** Users.
  - Click the **Add** button after each selected destination.

The E-Mail Destination populates in the list.

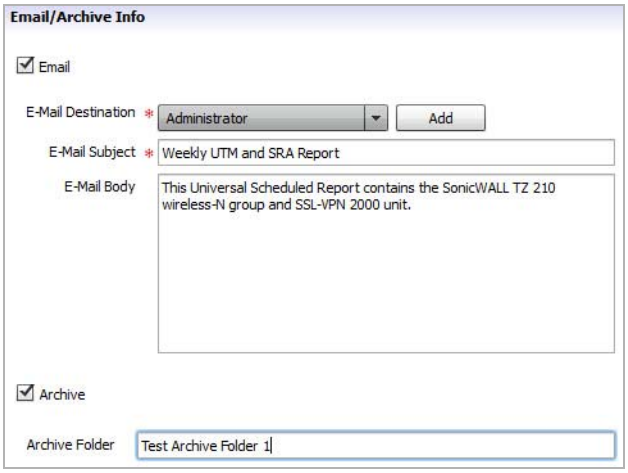


Note Multiple destinations can be sent in a single E-mail.

- Enter the E-mail Subject: **Weekly Firewall and SRA Report**
- Enter the E-Mail Body: **This Universal Scheduled Report contains the SonicWALL TZ 210 wireless-N group and SRA 2000 unit**



- Click the **Archive** checkbox to save a PDF report to a new folder.
  - Archive Folder: **Test Archive Folder 1**

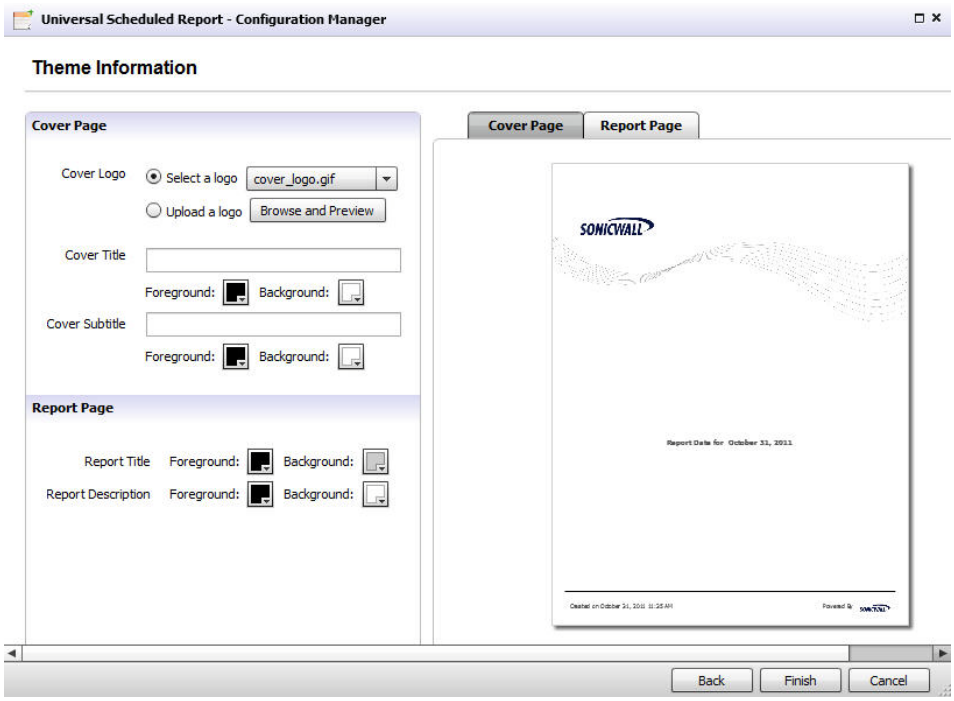


Step 16 Click the **Next** button.

Theme Information

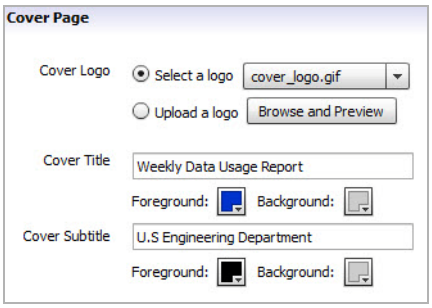
The Theme Information page displays. If **XML** is selected from the General Information page, the Theme Information page is not displayed.

Note The settings entered in the Cover Page and Report Page panels automatically update in the image located on the right side of the Theme Information page. To preview the cover / report pages, select the **Cover Page** or **Report Page** tab.



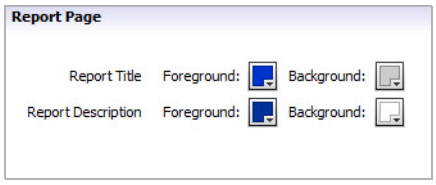
Step 17 Select / Enter the following in the **Cover Page** panel:

- Cover Logo: **Select a logo** (click the pull-down and select a cover logo image) or **Upload a logo** (click the **Browse and Preview** button to upload a logo)
- Cover Title: Enter a name (**Weekly Data Usage Report**) for your Universal Scheduled Report, then select or enter the foreground and background colors
- Cover Subtitle: Enter a subtitle (**U.S Engineering Department**) for your Universal Scheduled Report, then select or enter the foreground and background colors

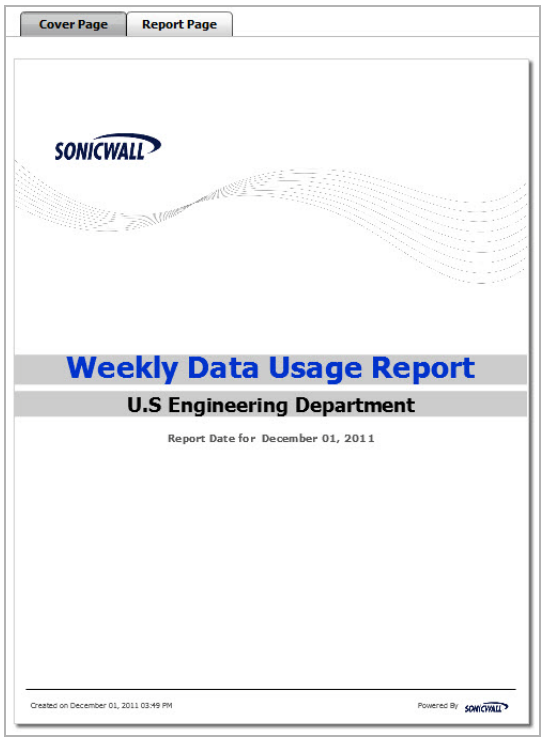


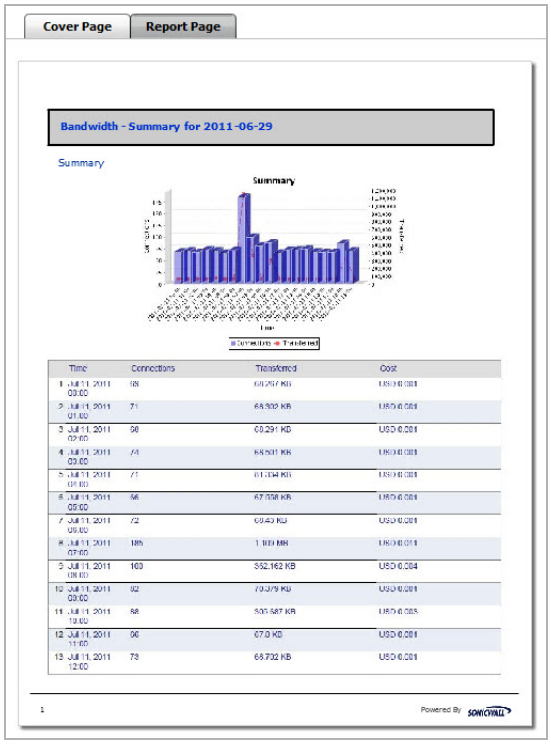
Step 18 Select or enter the following in the **Report Page** panel:

- Report Title: Foreground and Background colors
- Report Description: Foreground and Background colors



Step 19 Click the **Cover Page** and **Report Page** tabs to preview your Universal Scheduled Report.





Step 20 Click the **Finish** button.

Note When the Universal Scheduled Report PDF is exported, a table of contents is created. This allows you to quickly browse through your scheduled reports.

The report is now scheduled and can be found in the **Universal Scheduled Report > Manage Scheduled Reports** page.

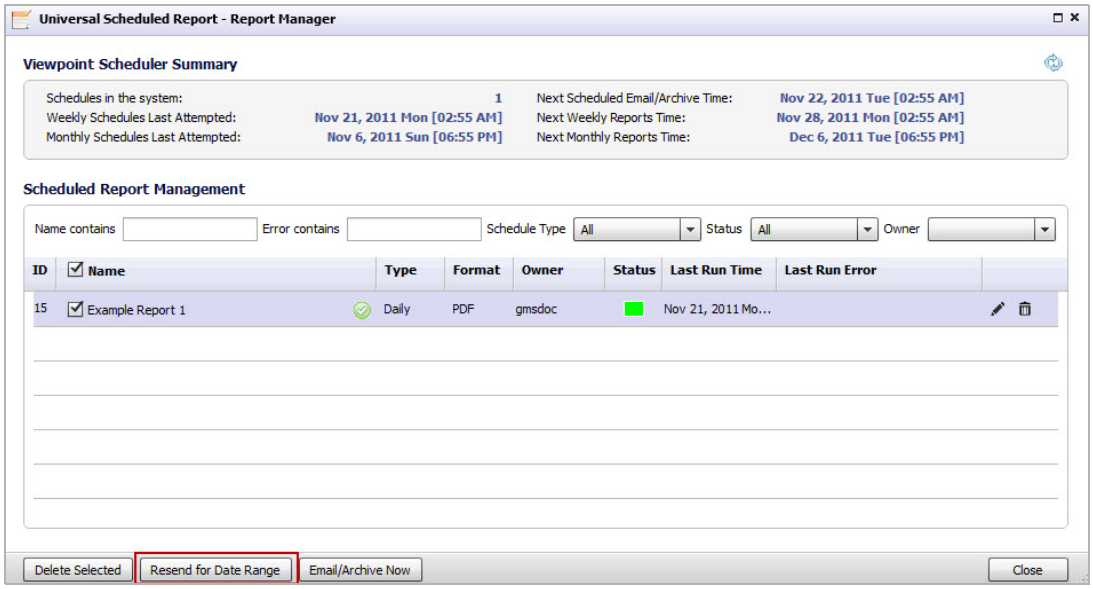
Managing the Scheduled Reports Component

Managing Scheduled Reports is used to manage the scheduled report task inventory by resending, Emailing / archiving now, editing, and deleting scheduled reports.

Resending a Scheduled Report

Preform the following steps to resend a scheduled report.

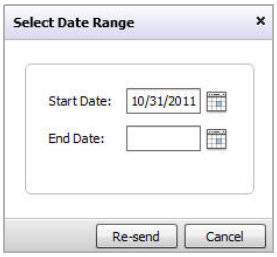
Step 1 Navigate to the **Universal Scheduled Reports > Manage Scheduled Reports** page.



Step 2 Use the filter options to search for a report in the Scheduled Report Management list, select the checkbox of the report you wish to resend.

Step 3 Click the **Resend for Data Range** button.

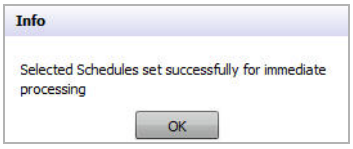
The Select Data Range pop-up window displays.



Step 4 Enter the Start / End dates by clicking the icon and selecting the dates.

Step 5 Click the **Re-send** button.

The Info pop-up window displays, confirming the schedule resend is complete.

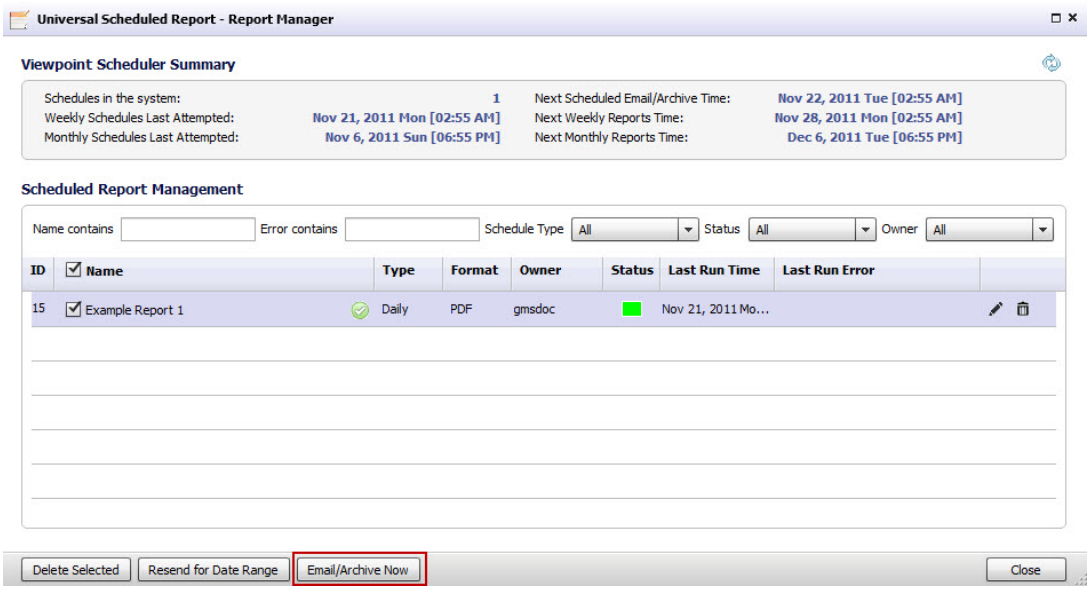


Step 6 Click the **OK** button.

Emailing / Archiving Now

Preform the following steps to Email / Archive a Universal Scheduled Report before its scheduled sending date.

Step 1 Navigate to the **Universal Scheduled Reports > Manage Scheduled Reports** page.

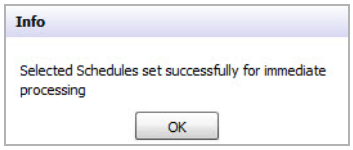


Step 2 Use the filter options to search for a report to Email /Archive in the Scheduled Report Management list.

Step 3 Select the checkbox next to the report name.

Step 4 Click the **Email/Archive Now** button.

The Info pop-up window displays, confirming the immediate processing of Email / Archive.



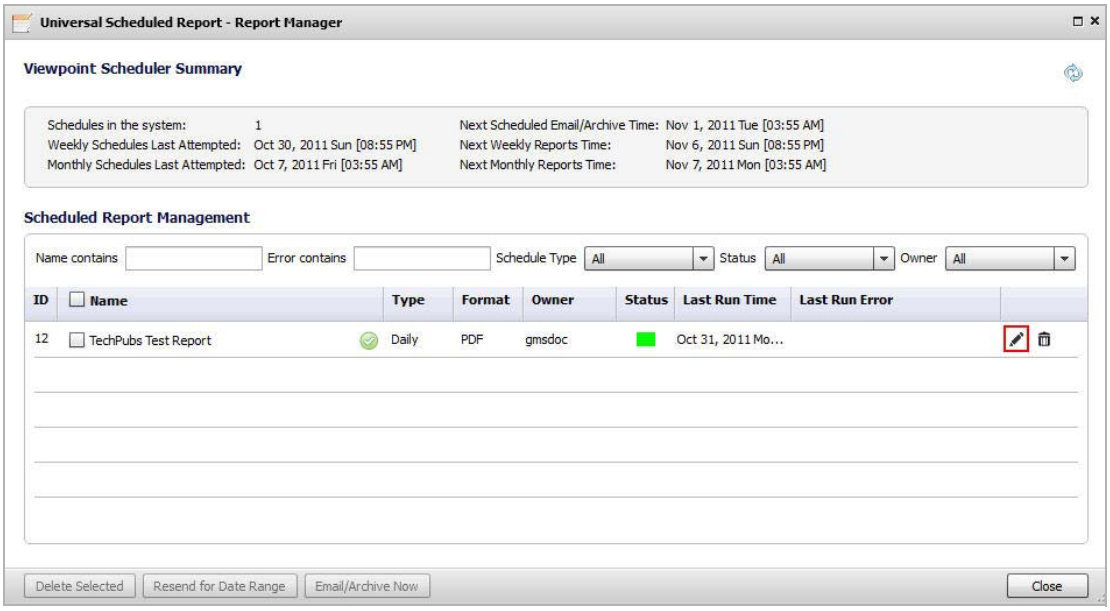
Step 5 Click the **OK** button

Your Scheduled report is now Emailed and Archived.

Editing a Scheduled Report

Preform the following steps to edit an existing scheduled report.

Step 1 Navigate to the **Universal Scheduled Reports > Manage Scheduled Reports** page.



Step 2 Use the filter options to search for a report in the Scheduled Report Management list, click the icon for that Report.

Step 3 To edit the Scheduled Report, use the same configuration procedure shown in the "Creating a Universal Scheduled Report" section.

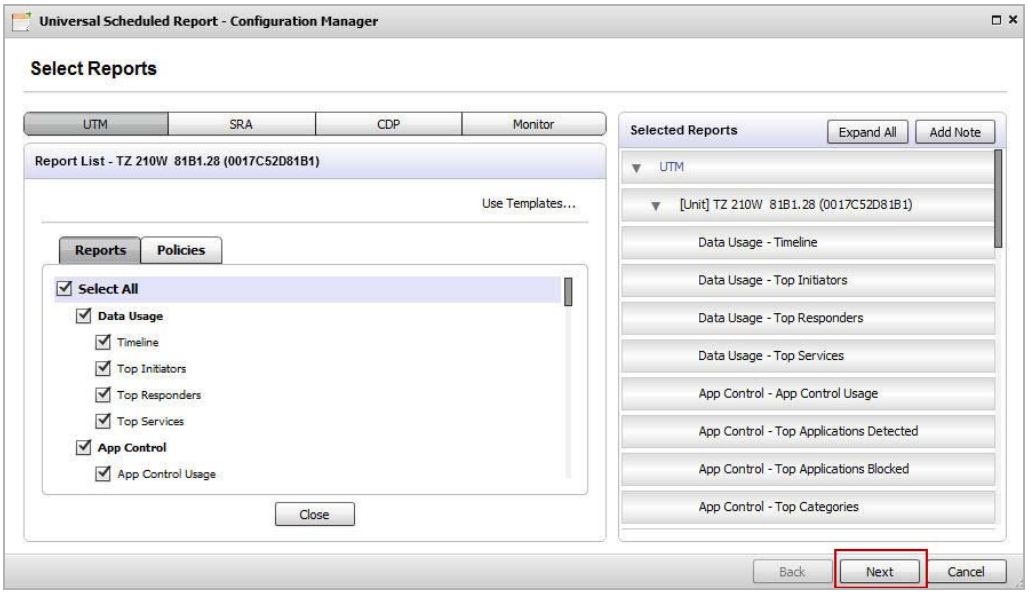
Disabling a Scheduled Report

Perform the following steps to disable a scheduled report.

Step 1 Navigate to the **Universal Scheduled Report > Manage Scheduled Reports** page.

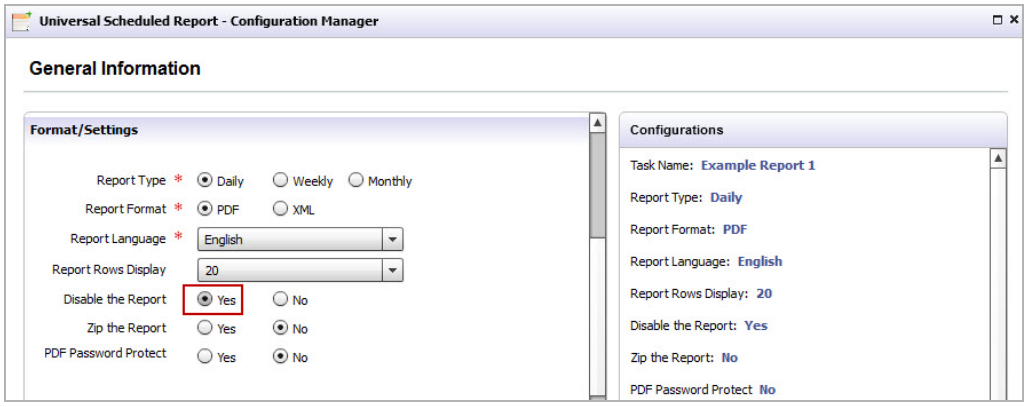
Step 2 Click on the icon for the report you wish to disable.

The Universal Scheduled Reports - Configuration Manager window displays.



Step 3 Click the **Next** button.

The General Information Page displays.



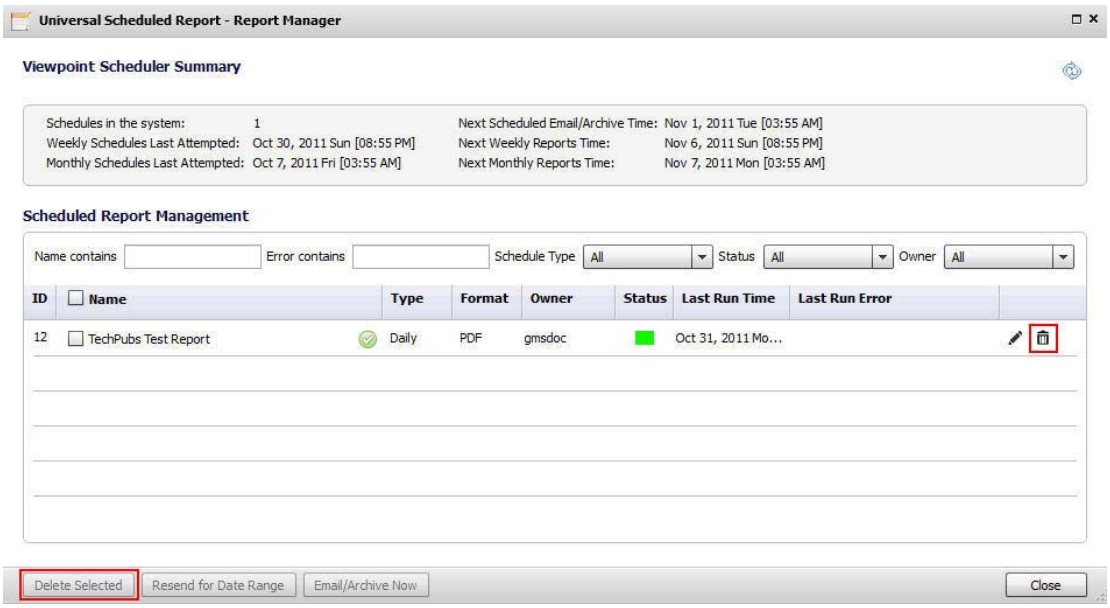
Step 4 In the Format / Settings panel, navigate to the **Disable the Report** option and click the **Yes** checkbox.

Note To enable the scheduled report, repeat steps 1-3, then click the **No** checkbox.

Deleting a Scheduled Report

Preform the following steps to delete an existing Universal Scheduled Report.

Step 1 Navigate to the **Universal Scheduled Report > Manage Scheduled Reports** page.



Step 2 Use the filter options to search for a report in the Scheduled Report Management list, select the checkboxes for the reports you want to delete.

Step 3 Click the **Delete Selected** button.

The selected reports are now deleted.

Note You can also use the icon to delete a specific Scheduled Report.

CHAPTER 5

Overview of Reporting

This chapter describes how to use Dell SonicWALL Analyzer reporting, including the type of information that can appear in reports. A description of the available features in the user interface is provided.

This chapter includes the following sections:

Dell SonicWALL Analyzer Reporting Overview

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

The Dell SonicWALL Analyzer Reporting Module creates dynamic, Web-based network reports from the reporting database.

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

You can create Custom reports by using the report filter bar, available in most report screens in the Analyzer UI. The report Filter Bar provides filters to allow customized reporting, including pre-populated quick settings for some filter fields. A Date Selector allows paging forward and backward in time, or selecting a particular time period for viewing, via a pull-down calendar. The search operator field offers a comprehensive list of search operators that varies depending on the search field, which can be either text-based or numeric. Refer to "Layout of Reports Display" on page 92 to see these items in the context of the Report page.

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

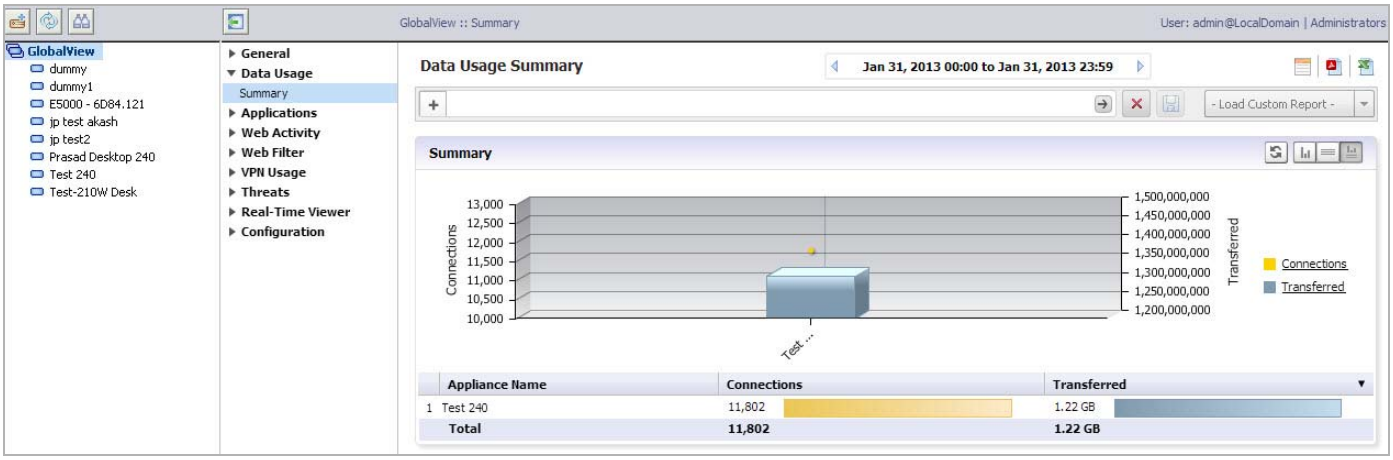
The Dell SonicWALL Analyzer Reporting Module provides an interactive interface that:

- Displays bandwidth use by IP address and service
- Identifies inappropriate Web use

- Provides detailed reports of attacks
- Collects and aggregates system and network errors
- Shows VPN events and problems
- Tracks Web usage by users and by Web sites visited
- Provides detailed daily firewall logs to analyze specific events.

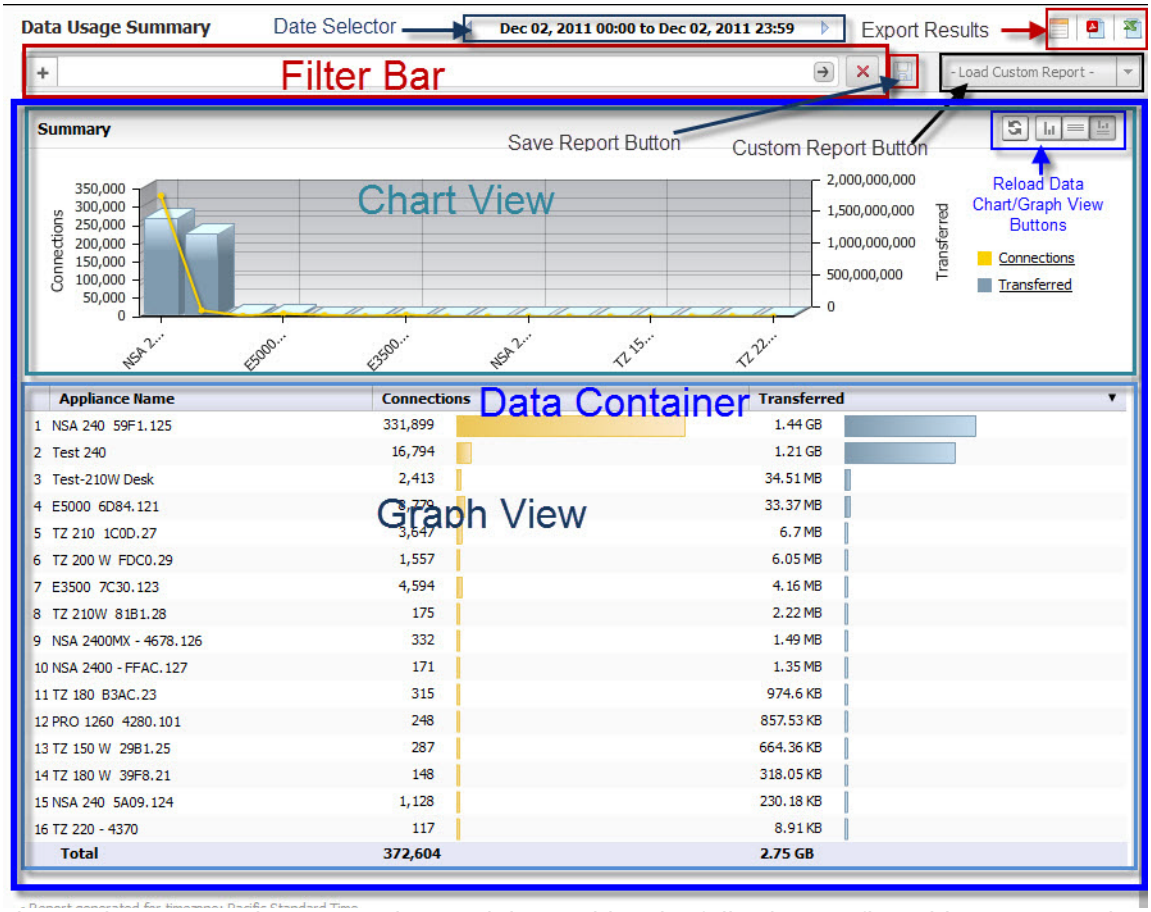
Viewing Reports

The Analyzer Reports view under the Firewall, SRA and CDP tabs is divided into three panes, as shown below: the TreeControl Pane, the middle pane with the Policies and Reports tabs, and the Reports pane.



- **TreeControl Pane**: A list of individual units referred to as the **TreeControl**. In the left pane, you can select the top level viewor a unit to display reports that apply to the selected view or unit The top level view is **GlobalView**.
- List of **Reports**: The middle pane provides two tabs: **Policies** and **Reports**. The **Reports** tab contains a list of available reports that changes according to your selection in the **TreeControl** pane: **GlobalView** provides a general summary of various functions, and unit view provides specific details. The reports are divided into categories. You can click on the top level report in a category to expand it to view the list of reports in that category, then click on an individual report name to view that report. To keep a category in expanded view, click on the category while pressing the **Ctrl** key. Otherwise, the expanded entry will collapse when the next entry is expanded.

- The **Reports Pane**: The right pane displays the report that you selected in the middle pane for the view or unit that you selected in the **TreeControl**. For most reports, a search bar is provided at the top of the pane. Above the search bar, a time bar is provided. You can view the report for a particular time by clicking right and left arrows, or clicking on the center field to get a pull-down menu with more options. Click on icons in the upper left corner to send the report to a PDF or UDP file. These files can then be printed for reference. A quick link to the Universal Scheduled Reports menu is also provided, allowing you to set up scheduling and other functions.



The SonicWALL Analyzer reporting module provides the following configurable reports under the Firewall and SRA tabs:

Table 1 Firewall Reports

Data Usage*	Provides an overall data usage report.
User Activity Reports	Produces a Detail report of user activity.
Applications*	Provides information on application access and firewall reports
Web Activity*	Provides Web usage reports, including initiators and sites.
Web Filter*	Provides web filter event reports, including by initiators, by sites, and by category.
VPN Usage*	Provides VPN usage reports on policies, services, and initiators.
Threats (Summary Only)	Access attempts by appliance.

Intrusions	Provides event reports about intrusion prevention, targets, initiators, as well as detailed timelines.
GAV	Provides reporting on virus attacks blocked.
Anti-Spyware	Provides reporting on attempts to install spyware.
Attacks	Provides event reports about attacks, targets, and initiators,
Authentication	Provides login reports.
Analyzers	Provides a detailed analysis of logs or activities.
Configuration	Configures settings for Summarizer and Log Analyzers.
Events	Creates, configures, and displays alerts.
Custom Report	Provides Internet Activity and Website Filtering reports with details from raw data Custom Reports are only available at the unit level.
* Multi-Unit Report Available	Provides a high-level activity summary for multiple units.

Note All reports that are displayed in the Firewall > Reports tab are also available in the Universal Scheduled Reports. However, the By Initiator and By Site reports related to Web Activity are available only as Scheduled Reports and are not displayed in the Firewall > Reports tab.

Table 2 SRA Reports

General	Provides general unit and license status.
Data Usage*	Provides an overall data usage report.
User Activity Reports	Produces a Detail report of user activity.
Access Method	Provides information on application access and firewall reports
Authentication	Provides login reports.
WAF*	Provides Web Application Usage (WAF) usage reports.
Connections*	Provides web filter event reports.
Analyzers	Provides a detailed analysis of logs or activities.
Events	Used to configure and view Alerts.
Custom Report	Provides Internet Activity and Website Filtering reports with details from raw data Custom Reports are only available at the unit level.
* Multi-Unit Report Available	Provides a high-level activity summary for multiple units.

Table 3 CDP Reports

General	Provides general unit and license status.
Multi-unit Summary Reports	Provide a high-level summary of disk capacity.
Capacity	Provides a report on disk capacity for an individual appliance.
Backup Activity	Provides a report on backup activity, including top agents and top file extensions backed up.

Navigating Dell SonicWALL Analyzer Reporting

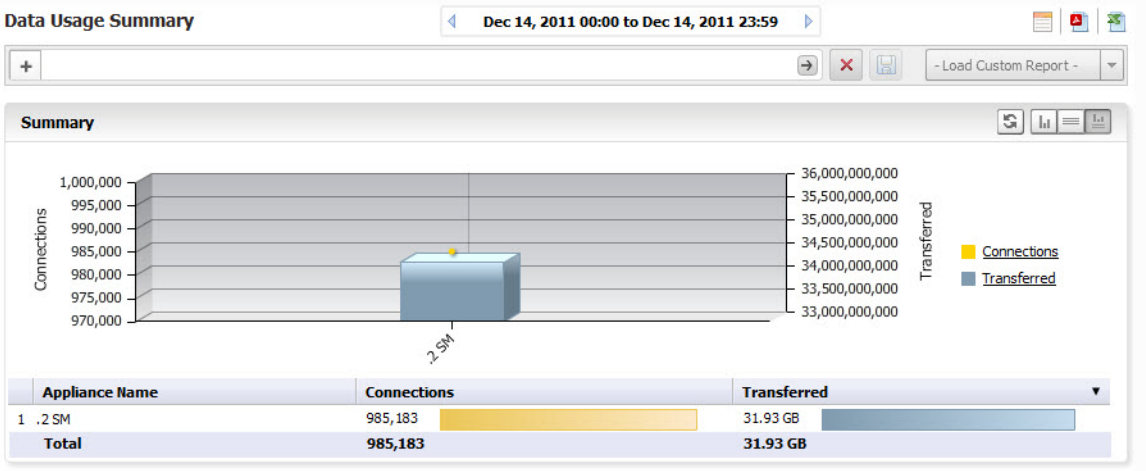
Dell SonicWALL Analyzer Reporting is a robust and powerful tool you can use to view detailed reports for individual SonicWALL appliances.

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

Global Views

From the Global viewof the Firewall Panel, Summary reports are available forall SonicWALL appliances connected to Dell SonicWALL Analyzer. The Summary provides a high level report for all appliances. More detail is available from the Unit view.

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



Summary pages are available for the major functions on the middle pane. By default, they display both the Chart View and Grid View. You can use the toggle buttons to the right to display either view, or both.

Note The selected Chart of Grid view remains in effect only for the specified screen. Changing screens will default back to the Chart and Grid View.

Unit View

The Unit view provides a detailed report for the selected SonicWALL appliance.

Dell SonicWALL Analyzer provides interactive reports that create a clear and visually pleasing display of information. You can control the way the information is displayed by adjusting the settings through toggles that allow you to display a graphical chart, a grid view containing the information in tabular format, or both (default). Reports are scheduled and configured in the Universal Scheduled Reports settings. For more information, refer to the "Using the Universal Scheduled Reports Application" section on page 60.

The Reports tab provides a list of available Reports. Click on the type of report to expand the list items and view the available reports in that screen group.

Tip At times, you may wish to see multiple screen groups at the same time. Ctrl-click to keep a previously-expanded topic from collapsing when you select a new report category. For example, you may want to view Data Usage, Applications, and Intrusions simultaneously, to see what detail sections are available. Control-click on these entries to see all the screen groups under these entries simultaneously.

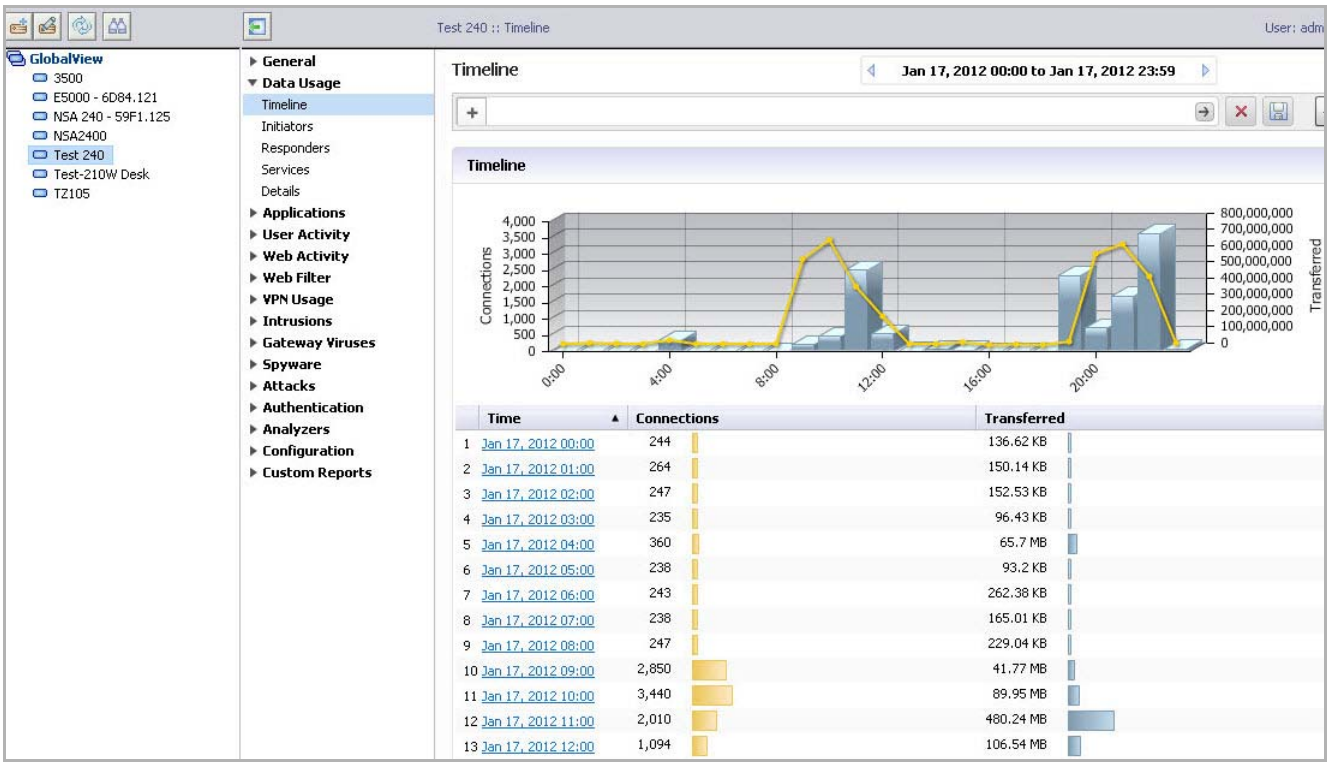
The reports available are usually the reports that appear as sections in the Details view. The Details entry is a shortcut to a view of all the available reports.

To access the Reports, use the following steps:

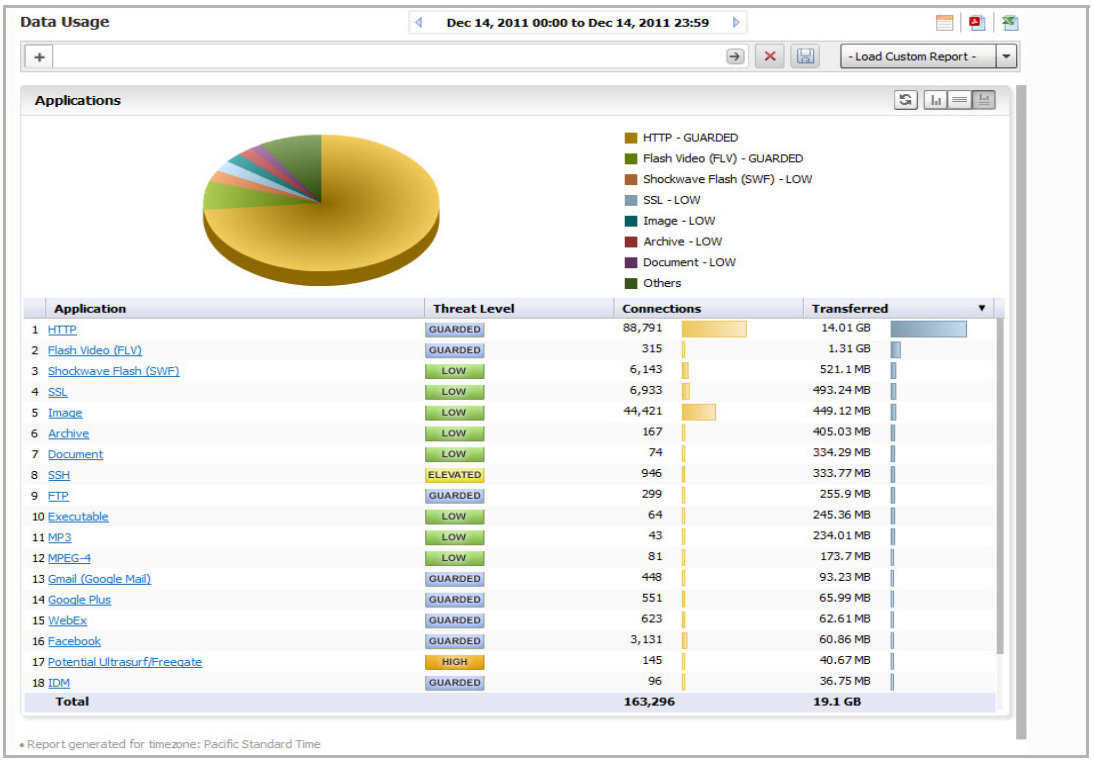
Step 1 Click on the desired tab at the top of the Dell SonicWALL Analyzer interface.

Step 2 To open the Unit view, click on a device in the TreeControl pane.

Step 3 Click on the desired report in the list of reports in the middle pane.



The default view of a root-level report always shows the chart and grid view of the report. The Sections displayed in the Grid View depend on the Report item selected and the filters applied to it. Additional information can be displayed by mousing over certain elements of the Report.



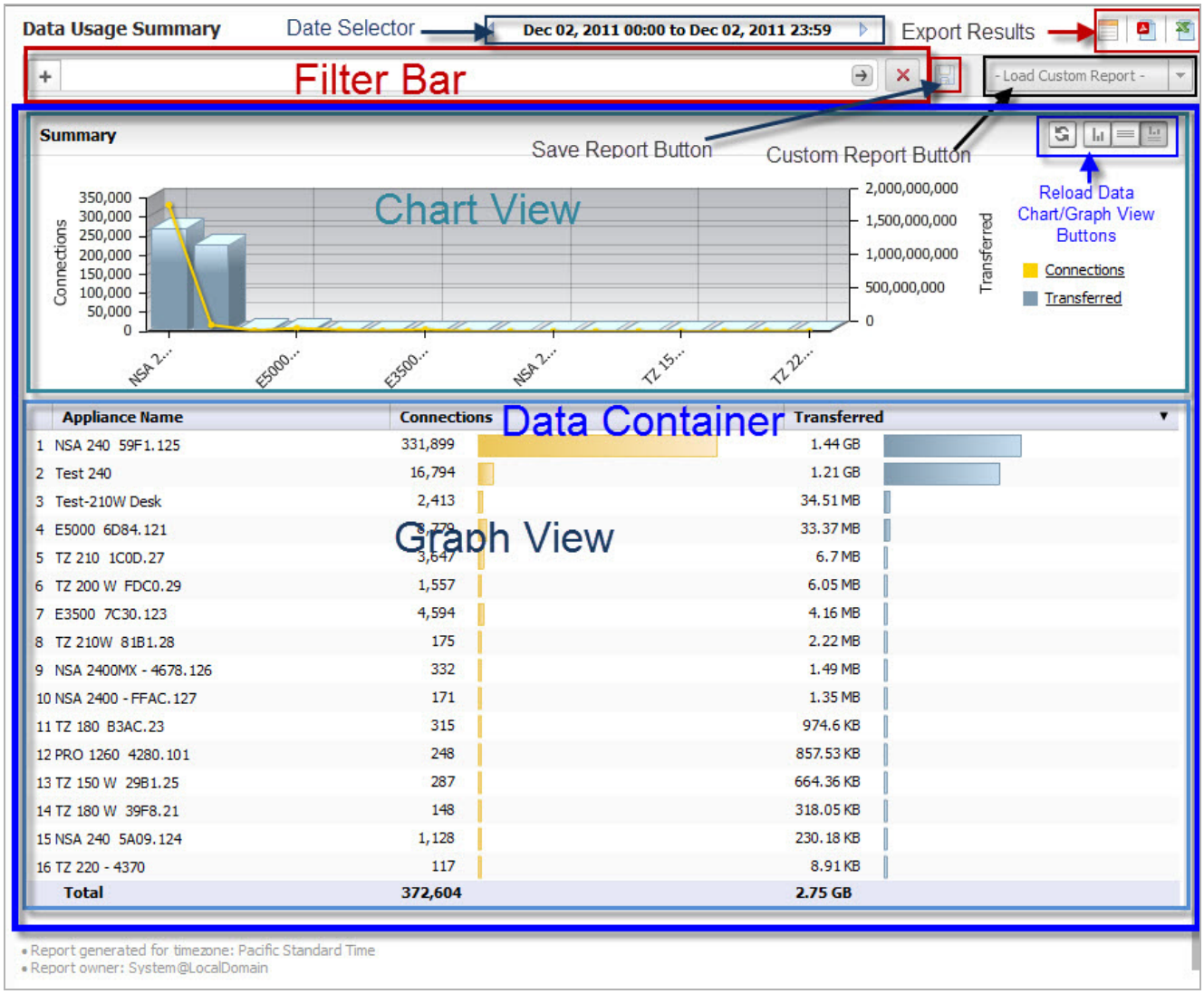
Note As you navigate the Firewall panel with a single SonicWALL appliance selected and apply filter settings, your filter settings will remain in effect throughout the session. To remove filter settings, click on the search bar “Remove Filters” button. (Refer to the graphic in Layout of Reports Display, below.)

Layout of Reports Display

The Report Display is comprised of the following areas:

- The Filter Bar area, which includes the Time Bar, Export buttons and Custom Reports buttons, and data filter functions
- Report Data Container, containing the Chart and/or Grid Views

The figure below shows the layout of the Report.



The Report contains the following areas:

- The **Date Selector** Bar
- The **Filter Bar**

- Export Options, including:
  - **Schedule Report** Button: brings up the Universal Scheduled Reports menus
  - **Export to CSV**
  - **Export to PDF**
- **Save** button

- **Load Custom Report** button
- **Report Data Container**. The **Report Data Container** consists of the Chart View and the Grid View, the **Show Chart**, **Show Grid**, and **Show Chart and Grid** toggle buttons, and the **Reload Data** button.

Note The Chart view is clickable. You can drill down to Detail sections simply by clicking on areas of interest in the bar-chart or pie-chart.

The Date Selector

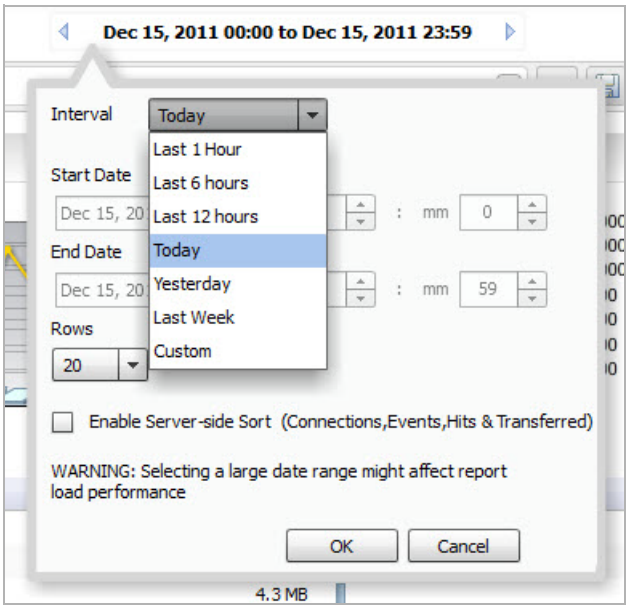
The **Date Selector** allows you to generate a report for only a specific date and time range. Use the right and left quick-link arrows to move backward and forward in time, a day at a time. Clicking the time field on the Date Selector brings up a pull-down menu that allows you to customize your time and date ranges.

Setting a Date or Date Range

By default, summary reports display only information for a single date. However, by using the **Time Selector** pull-down menu, you can fine-tune the time, date, or range of times and dates you want to see. Over-time reports display information over a date range.

Selecting a Date and Time

The **Time Selector** allows you to specify any time or date interval desired, whether by day, or in hour/minute intervals. To select a single date for a report, either use the Date Selector bar and the left and right arrows to page through reports by date, or click on the displayed date field in the Time Selector to display the pull-down schedule menu.



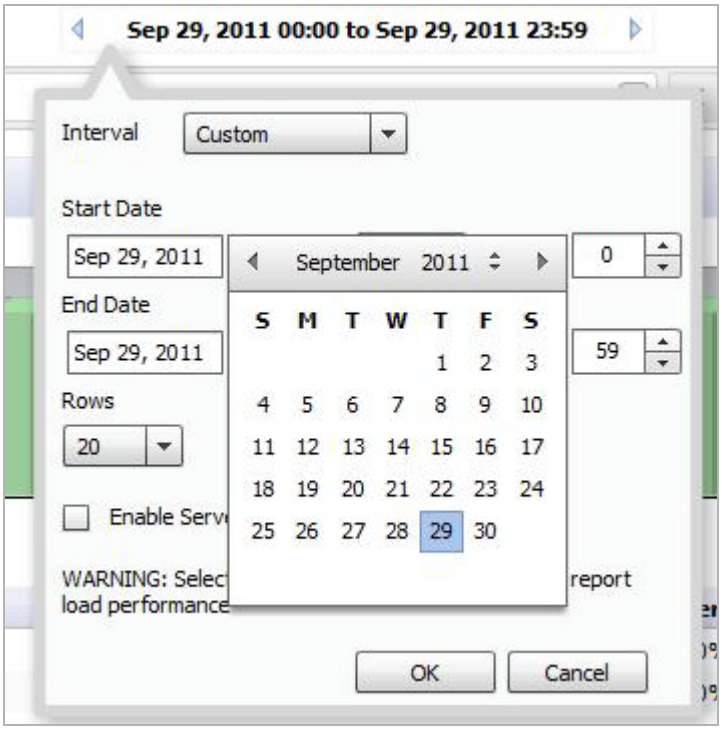
You can select from:

- Last 1 hour
- Last 6 hours
- Last 12 hours
- Today - 00:00 to 23:59
- Yesterday - 00:00 to 23:59
- Last Week - the previous 7 days, from 00:00 to 23:59
- Custom - a custom time and date range

In the pull-down schedule menu, you can specify a recent time snapshot, or click on **Custom** to select the starting and ending dates and times. The **Custom** option allows you to select a specific time and date or range from the **Interval** menu.

Step 1 To set up a custom time range, click in the Time Selector Bar. The Interval pull-down menu appears.

In the Interval menu, you can either set the date manually or by using the pull-down calendar. In the calendar, you can set the month by clicking the desired dates. If no data is available for a specific date, that date will not be available (grayed out).



Step 2 Set a specific start and ending time by specifying hours and minutes you want to monitor. The default for a date is an interval starting at hour 0 minute 0 (midnight) and ending at 23:59 (11:59 PM).

Step 3 The Interval menu also lets you set how many lines of information appears in the graph view. Click the date, and when the Interval pull-down appears, specify the number of rows. Select **5**, **10**, **20**, **50**, or **100** from the **Rows** pull-down list to limit the display to a the specified number of lines, for easier viewing.

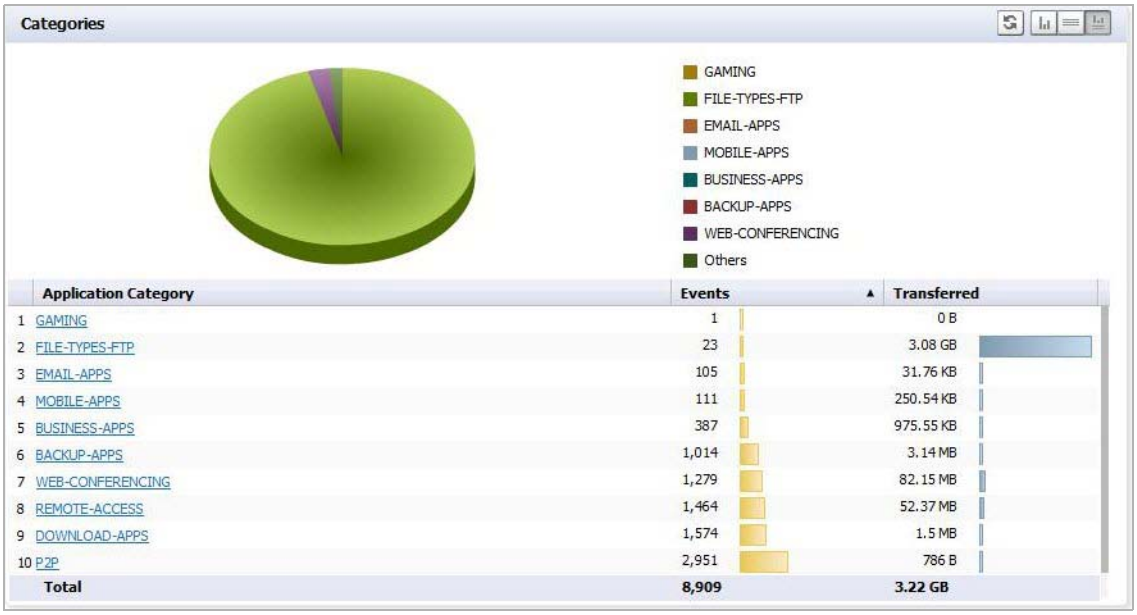
Step 4 Click **OK** to generate the report.

Report data is sorted and ranked according to how many rows are displayed. By specifying a limited number of rows to be displayed in the graph section of the Report, rankings will apply only to the data in those rows. If you reverse the sort order by clicking on the column bar, only the displayed items will be re-sorted.

To re-sort according to all collected data in the database, click on the **Enable Server Side Sort** checkbox on the pull-down menu. The ranking of the grid items will then reflect all data from the total entries.

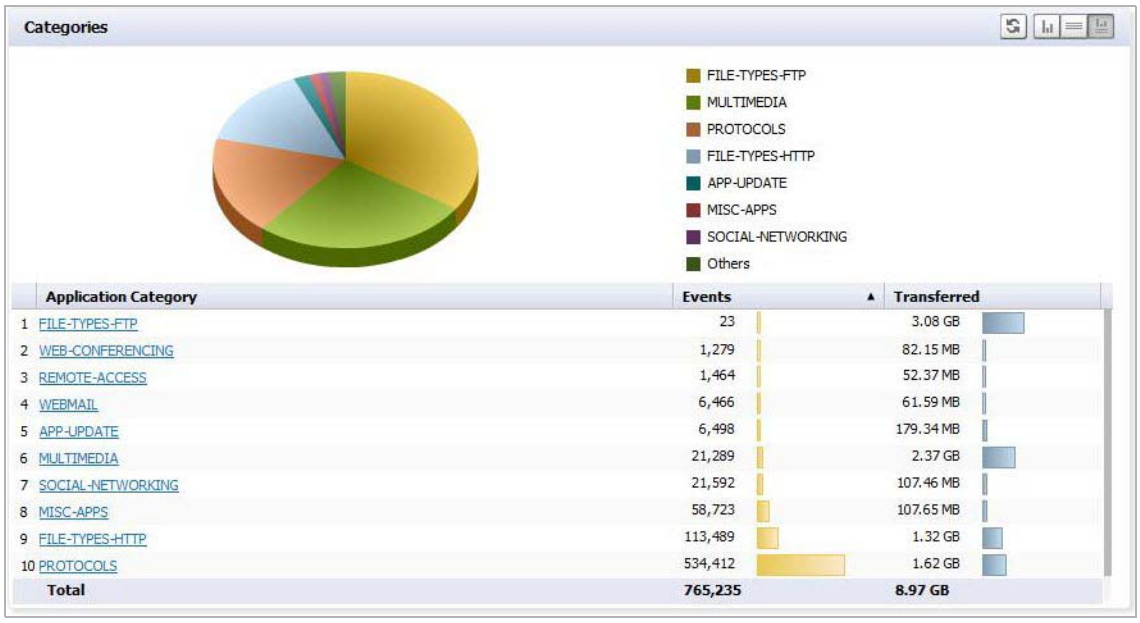
By default, Client-side Sort is used, which sorts only the currently viewable data, which was retrieved the first time the data base was clicked on.

For example, the snapshot below shows data displayed only as it pertains to ten rows.



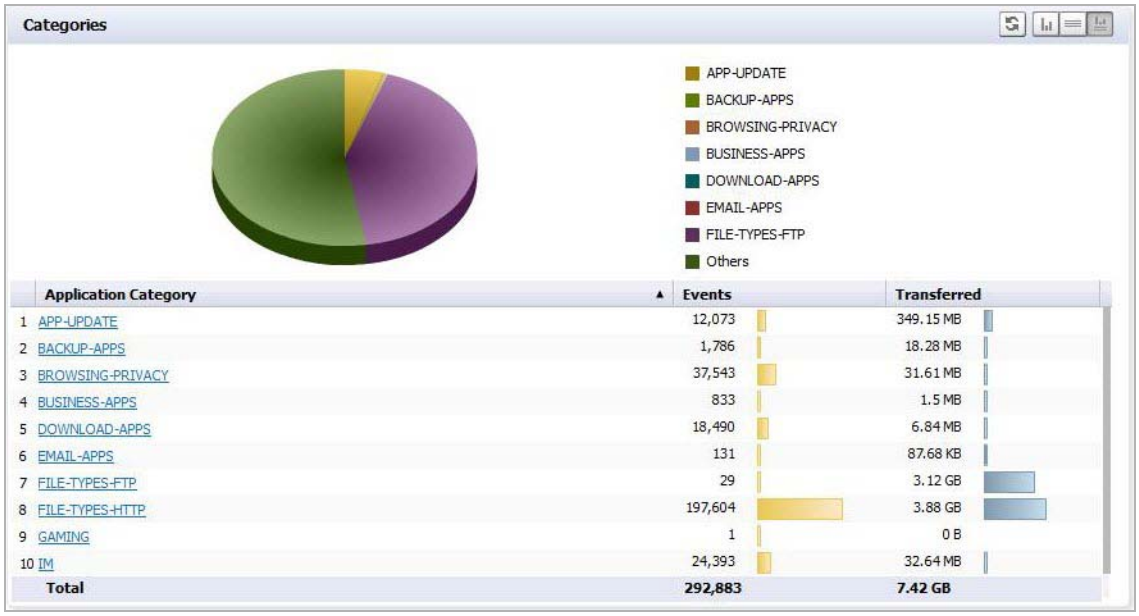
	Application Category	Events	Transferred
1	GAMING	1	0 B
2	FILE-TYPES-FTP	23	3.08 GB
3	EMAIL-APPS	105	31.76 KB
4	MOBILE-APPS	111	250.54 KB
5	BUSINESS-APPS	387	975.55 KB
6	BACKUP-APPS	1,014	3.14 MB
7	WEB-CONFERENCING	1,279	82.15 MB
8	REMOTE-ACCESS	1,464	52.37 MB
9	DOWNLOAD-APPS	1,574	1.5 MB
10	P2P	2,951	786 B
	Total	**8,909**	**3.22 GB**

If you re-rank the column to see the lowest number of hits, it will rank only the items displayed in the ten rows you selected.



	Application Category	Events	Transferred
1	FILE-TYPES-FTP	23	3.08 GB
2	WEB-CONFERENCING	1,279	82.15 MB
3	REMOTE-ACCESS	1,464	52.37 MB
4	WEBMAIL	6,466	61.59 MB
5	APP-UPDATE	6,498	179.34 MB
6	MULTIMEDIA	21,289	2.37 GB
7	SOCIAL-NETWORKING	21,592	107.46 MB
8	MISC-APPS	58,723	107.65 MB
9	FILE-TYPES-HTTP	113,489	1.32 GB
10	PROTOCOLS	534,412	1.62 GB
	Total	**765,235**	**8.97 GB**

Use **Enable Server Side Sort** to sort data based on all underlying data records, not the client-side sort. Server side Sort retrieves current data from the back end database. Client-side sort merely rearranges the data already retrieved. You can still constrain your display to 10 rows, but the display will re-sort based on the total data collected in the back-end database, and not just the data previously displayed.



	Application Category	Events	Transferred
1	APP-UPDATE	12,073	349.15 MB
2	BACKUP-APPS	1,786	18.28 MB
3	BROWSING-PRIVACY	37,543	31.61 MB
4	BUSINESS-APPS	833	1.5 MB
5	DOWNLOAD-APPS	18,490	6.84 MB
6	EMAIL-APPS	131	87.68 KB
7	FILE-TYPES-FTP	29	3.12 GB
8	FILE-TYPES-HTTP	197,604	3.88 GB
9	GAMING	1	0 B
10	IM	24,393	32.64 MB
	Total	**292,883**	**7.42 GB**

Export Results

The Export Results icons allow you to save a report in either PDF or Excel format.

These buttons provide the following export options:

To the left of the **Export Results** icons is the **Schedule Report** icon. This button brings up the Universal Scheduled Report Configuration Manager, allowing you to create a schedule for generating the specified report, which will then be emailed to you. For more information, refer to the "Using the Universal Scheduled Reports Application" section on page 60.

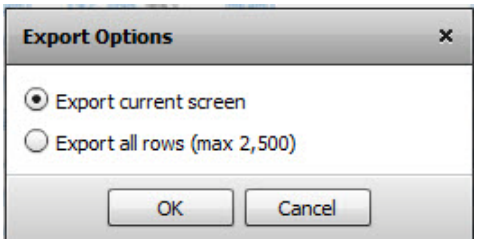
The Export Results icons allow you to save to a file, either in PDF or Excel format.

- **Export to PDF**: This button will allow you to save the displayed report data to a PDF file. The PDF can export a maximum of 2500 rows.
- **Export to CSV**: This button allows you to send the report to a file in Microsoft Excel Comma Separated Value (CSV) format. Excel can export a maximum of 10,000 rows.

Tip

To print a report, export it to PDF, using the **Export to PDF** button, then print out the PDF file.

If a very large Report file, such as a system log, is being exported, the number of lines that can be saved is limited. When you click the icon, you will see a message like the following:



Select whether to print only the currently-displayed screen, or the maximum number of rows.

The Filter Bar

The Filter Bar provides filtering functions to narrow search results, to view subsets of report data.

The Filter Bar is at the top of the Report. It contains the Add Filter (+) button for adding filters and Go button to apply filters, as well as the Clear Filter button to clear all filters.

Using the Filter Bar allows you to view subsets of the report data, based on a set of pre-defined filters.

Adding Filters

Filters can be added in two ways, either explicitly through the Filter Bar, or implicitly by clicking on the hyperlinks in the grid sections of a displayed report. As hyperlinks are clicked, those link criteria are added to the Filter bar as if it was added explicitly. Refer to "Adding Filters Implicitly" section on page 100 for more information.

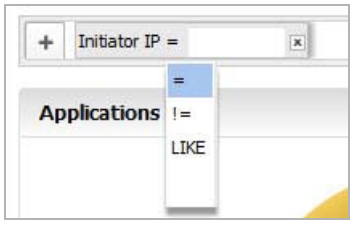
Use the Filter Bar to add pre-defined filters from a pull-down menu and to specify parameters for those filters. Filter values will be matched in the database during report generation.

Click the **Add Filter** button (+) on the left to display a pull-down menu, which can then be used to fine-tune the report data by selecting categories.

Filters can also be added by right-clicking on a column entry and selecting the Filter option from the pull-down menu.

Filter criteria are context-dependant, meaning that Dell SonicWALL Analyzer finds the specific filter operators applicable to the entry. Many filter operators are used in connection with a text string or numeric filter input value that determines what data to include in the report. This control uses auto-complete to suggest a set of candidate values, or you can manually enter a different value. Manually-entered values should be checked for blanks, illegal characters etc.

Operators are specified by clicking on the default operator to bring up the pull-down menu of available operators.



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 restrict the information displayed in the Detail report.

The operators are defined as shown in Table 4.

Table 4 Filter Operators

Operator	Definition
IN RANGE	Subnet data that is in the specified range will be included in the report.
NOT IN RANGE	Subnet data that is not in the specified range 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 not equal to the input numerical value will be included in the report

You can also use wild-cards (*) in filters to match anything. For instance, you might want to match a User name. You would select LIKE as the operator, and use * in connection with a string. For example, “joh* would match all users starting with “joh,” such as John, Johnny, Johan, etc.

Using the Filter Bar

Use the Filter Bar to manually (explicitly) add filters.

Step 1 To add a filter, click on the Add Filter (+) menu and select a filter from the pull-down menu. Available Filter categories may differ, depending on the report, and may require parameters.

Some filter fields use operators with text or numeric values. Others might have pre-filled values. For example, the Initiator Country filter displays a pull-down list, allowing you to display results based on a selected country.

Step 2 Click the **Go** button (right-hand arrow) to add a filter Each filter must be applied by clicking on **Go** before you can select and apply the next filter. The filter bar will show all filters added, whether added from the menu bar or pull-down menu.

As filters are added, items that have been filtered out disappear from the listings, reappearing only when the associated filter, or all filters, are removed.

Step 3 To remove a filter, click the + next to the filter in the menu bar and click the **Go** (right arrow) button. To clear all filters, click the Clear Filter (x) next to the filter fields.

Adding Filters Implicitly

Dell SonicWALL Analyzer also allows adding filters directly to a drillable (hypertext-linked) column to create a “criteria control,” where you can set a value for the filter. Adding a filter to a column allows you to restrict the display to view only the data related to the entry of interest.

In second-level reports with multiple subsections, filters can be added simply by clicking on the hyperlinked data in the report section.

Step 1 To add a filter to a “drillable” column containing hypertext links, right-click on a hypertext column cell and select **Add Filter** from the resulting pull-down context menu.

Because the filter is context-sensitive, it may suggest a set of candidate values, or you can manually enter a different value. A new filter will be automatically added to the filter bar, and the report will be updated accordingly.

Once added, the filter is added to the filter area of the Search Bar and no longer appears in the pull-down list. The report will display only results restricted by that filter.

Step 2 To remove the filter, click the x next to that filter, or clear all filters by clicking the red X button to the right of the field.

Saving/Viewing a Filtered Report

The **Save Report** pop-up menu allows you to save the currently-displayed report with a specified name of no more than 20 characters. You can also overwrite an already-saved report with the current report or overwrite the report to show a new date range.

Saved reports, even if created for a specific unit, are available for all units of that appliance type. For example, if a report for the X1 interface was created for a specific unit, this report is available from any unit: there is no need to create a X1 report for different units.

Note Custom Reports created by a specific user are viewable by that user, and no one else. Domain Administrators can view all available reports.

Step 1 To save a report, along with its filter criteria, click the **Save Report** icon.

Step 2 Assign it a file name for later reference.

Step 3 To view a saved Custom Report, click the **Custom Reports** button to bring up a menu that contains a list of all saved Custom reports available for viewing. Selecting a Custom Report from this pull-down loads data for the selected report into the Report Data Container.

Step 4 You can also load a saved report from the Report tab on the middle bar menu. Click **Custom Reports** on the Reports tab and select the desired report to load it into the Data Container.

Step 5 Click on the appropriate Export Results icon to save a report to a PDF file or Excel spreadsheet. To print a copy of the report, click on the PDF icon and save it to a file, then print the PDF file.

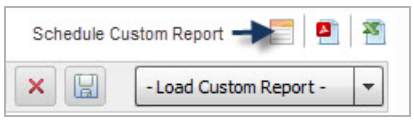
Tip Saved Reports can be modified or deleted by clicking on **Custom** > **Manage Reports**.

Scheduling Reports

You can schedule a report to be created and sent to you in email, using the Universal Scheduled Reports function.

The **Schedule Reports** icon is located to the right side of the toolbar above the Load Custom Reports button.

Click this icon to bring up the Universal Scheduled Report Configuration Manager.



When the Configuration Manager menu comes up, it will be pre-filled with the information about the current Reports page. Using this report, you can set up specific tasks, chose the format for the report, and other options. For more information on using Universal Scheduled Reports, refer to the section: Universal Scheduled Reports.

Report Data Container

The Report Data Container is the screen space where the report data is displayed.

Dell SonicWALL Analyzer provides interactive reporting to create a clear and visually pleasing display of information in the Report Data Container. The Root-level baseline report shows the Chart View, usually containing a timeline or a pie chart and a Graph View.

You can control the way the information is displayed by adjusting the settings through toggles or by configuring reports in the dashboard interface.

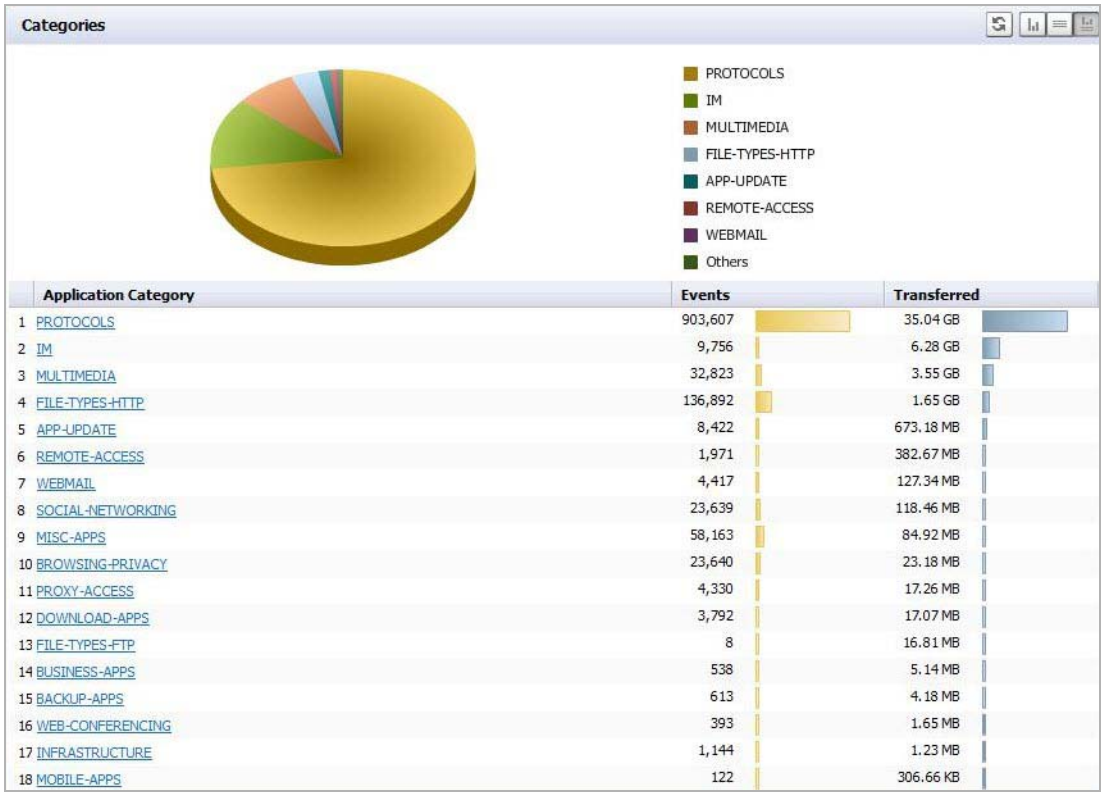
Reports have a Date Selector and Filter Bar at the top, with the Report Data Container below it.

Detail-level reports are available either by “drilling down” on hyperlinks in the Root-level view, or, for some types of Reports, as a shortcut on the Report tab.

Note Cell data in the report container can be copied by right-clicking the cell and selecting **Copy Cell Data** from the pull-down menu.

Layout of the Data Container

The Report Data Container is comprised of a number of Sections. Sections are usually arranged vertically stacked on top of each other. Each section has a “Title Bar” which contains the “Section” title on the left and a group of buttons on the right.The Report itself may contain one or more Sections of data, which are different facets of the report data.



	Application Category	Events	Transferred
1	PROTOCOLS	903,607	35.04 GB
2	IM	9,756	6.28 GB
3	MULTIMEDIA	32,823	3.55 GB
4	FILE-TYPES-HTTP	136,892	1.65 GB
5	APP-UPDATE	8,422	673.18 MB
6	REMOTE-ACCESS	1,971	382.67 MB
7	WEBMAIL	4,417	127.34 MB
8	SOCIAL-NETWORKING	23,639	118.46 MB
9	MISC-APPS	58,163	84.92 MB
10	BROWSING-PRIVACY	23,640	23.18 MB
11	PROXY-ACCESS	4,330	17.26 MB
12	DOWNLOAD-APPS	3,792	17.07 MB
13	FILE-TYPES-FTP	8	16.81 MB
14	BUSINESS-APPS	538	5.14 MB
15	BACKUP-APPS	613	4.18 MB
16	WEB-CONFERENCING	393	1.65 MB
17	INFRASTRUCTURE	1,144	1.23 MB
18	MOBILE-APPS	122	306.66 KB

Note Root level reports available in the Reports panel usually contain only one section.

The Report Data Container sections either appear as a chart view, a grid view, or both.

The default display mode is **Show Chart and Grid**. In this mode, the data is available for viewing as both a **‘Chart’** and a **‘Grid’**. This layout can be controlled by switching between 3 display mode options, any of which can be turned on/off at any time, using the utility toggle button group on the Section Title Bar.

The display modes available on this layout are:

- **Show Chart**: In this mode only the chart is visible and takes up all the available space inside the section container. Charts show a timeline or pie chart.
- **Show Grid**: In this mode only the Grid is visible.The Grid Display may contain more than one Section,
- **Show Chart and Grid**: In this mode both the *chart* and the *grid* are visible and are vertically stacked.

  Switching between these modes is handled through the utility toggle buttons.

Only one mode can be active at a time.

 A ***'Reload Data'*** button is present on the title bar in *all the layouts* described above. Clicking this button will instruct the application to refresh the section data.

You can determine if you have reached the final section in a multi-section Grid View by checking if there is a message about the relevant time-zone at the bottom left of the report. If this message is present, there are no more Grid sections available.

Viewing Syslog Data of Generated Reports

Different types of section data are available under the root-level report. The section level reports are available through the Details entry on the middle pane Reports tab, for some Reports. You can also drill down from the root level report to the second level Detail views, containing multiple subsections, by right-clicking a hyperlink and selecting “Drilldown” from the pull-down menu. The syslog fields corresponding to the applied filter will come up.

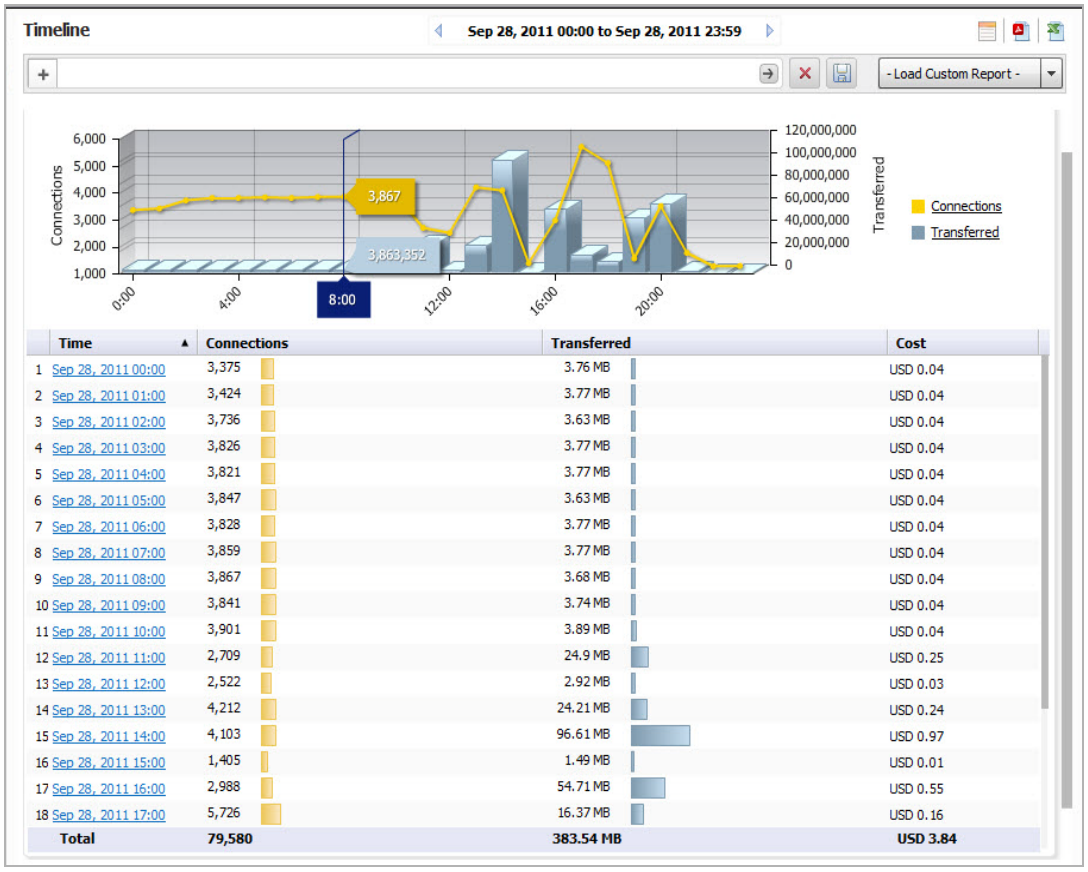
Drilling Down

Sections in the Grid display may contain drillable columns, containing hypertext links to bring up a Detail Report. A ‘drillable’ column appears as a column in the data grid, where the child values appear underlined and in blue, and act as a hyperlink to additional information. Click on any of these values to drill down to another report, using the value on which drill-down has been executed as a filter. When you click on a drillable link, this filter will be added to the Filter Bar.

Drilling down navigates to a new Detail report, filtered by the data on which the drill-down was executed. Drillable reports can display multiple grid sections in the sub-reports, or bring up a System Analyzer view, depending on the item selected.

The following example illustrates how you can drill down through the **Data Usage** Report by clicking on a drillable entry to gain more information and filter the results.

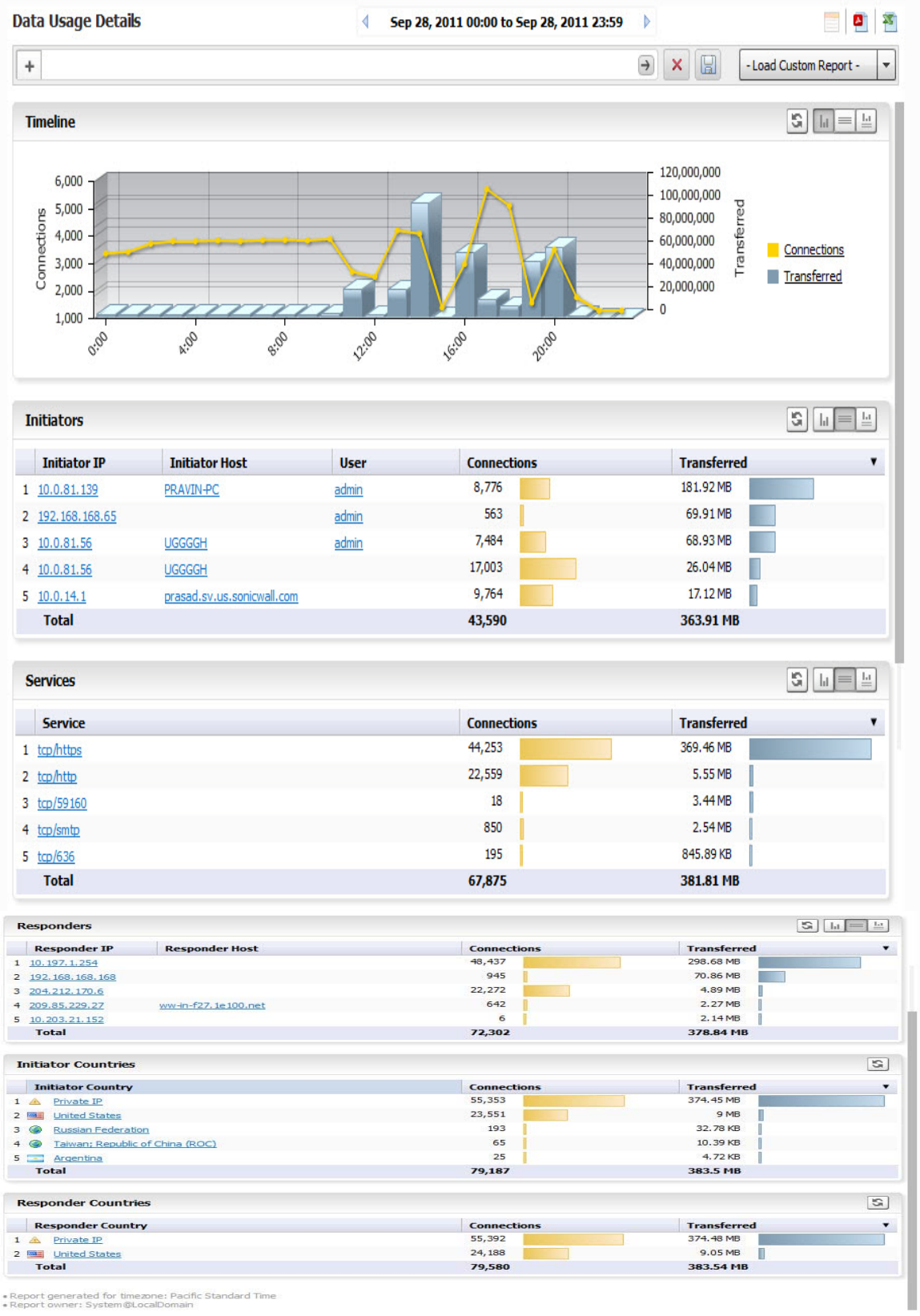
Step 1 Click on an appliance, then click **Data Usage** on the Reports tab. You will see a timeline showing connections.



	Time	Connections	Transferred	Cost
1	Sep 28, 2011 00:00	3,375	3.76 MB	USD 0.04
2	Sep 28, 2011 01:00	3,424	3.77 MB	USD 0.04
3	Sep 28, 2011 02:00	3,736	3.63 MB	USD 0.04
4	Sep 28, 2011 03:00	3,826	3.77 MB	USD 0.04
5	Sep 28, 2011 04:00	3,821	3.77 MB	USD 0.04
6	Sep 28, 2011 05:00	3,847	3.63 MB	USD 0.04
7	Sep 28, 2011 06:00	3,828	3.77 MB	USD 0.04
8	Sep 28, 2011 07:00	3,859	3.77 MB	USD 0.04
9	Sep 28, 2011 08:00	3,867	3.68 MB	USD 0.04
10	Sep 28, 2011 09:00	3,841	3.74 MB	USD 0.04
11	Sep 28, 2011 10:00	3,901	3.89 MB	USD 0.04
12	Sep 28, 2011 11:00	2,709	24.9 MB	USD 0.25
13	Sep 28, 2011 12:00	2,522	2.92 MB	USD 0.03
14	Sep 28, 2011 13:00	4,212	24.21 MB	USD 0.24
15	Sep 28, 2011 14:00	4,103	96.61 MB	USD 0.97
16	Sep 28, 2011 15:00	1,405	1.49 MB	USD 0.01
17	Sep 28, 2011 16:00	2,988	54.71 MB	USD 0.55
18	Sep 28, 2011 17:00	5,726	16.37 MB	USD 0.16
	Total	**79,580**	**383.54 MB**	**USD 3.84**

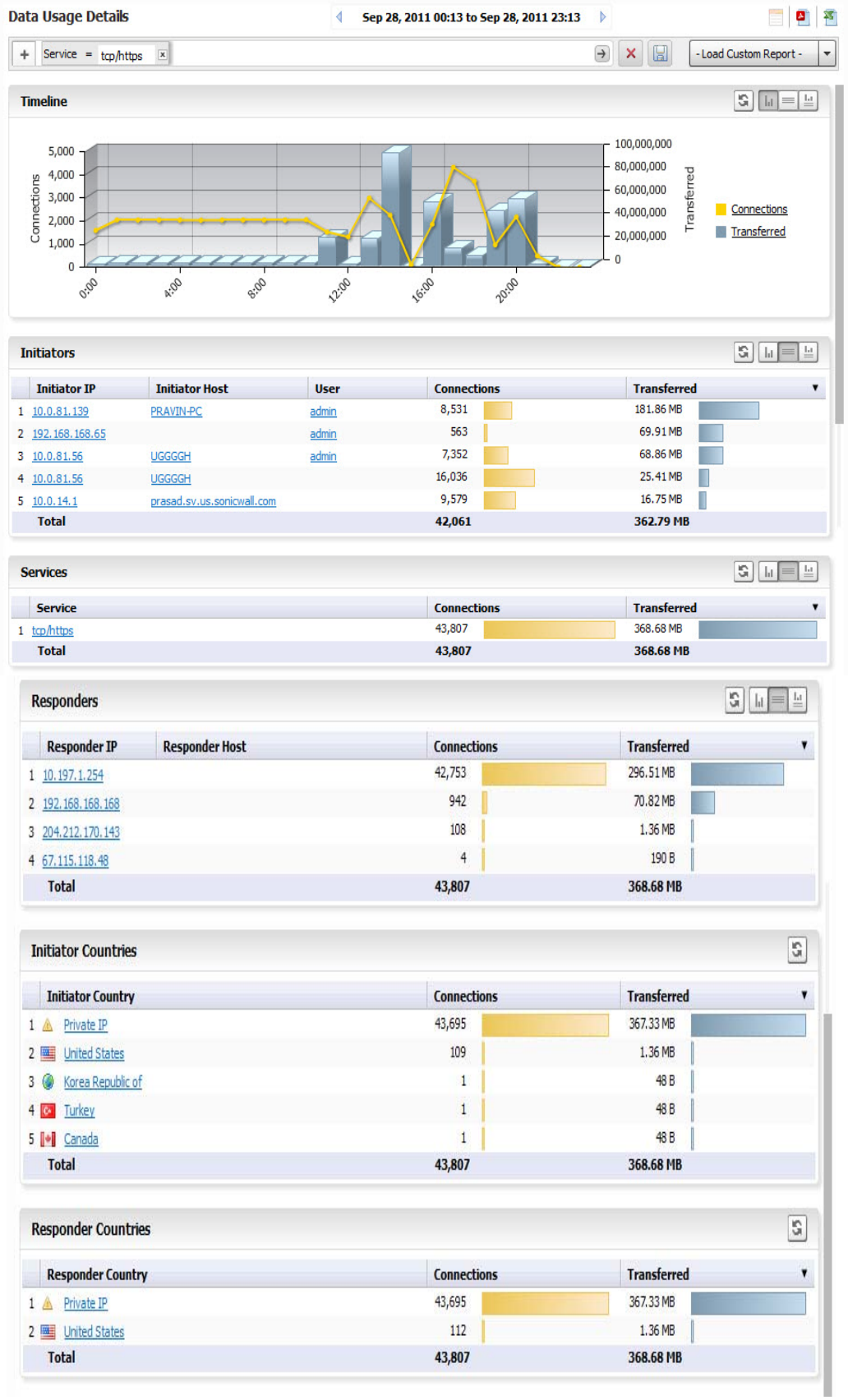
Step 2 Click on a hyperlinked Time to go to the Detail view of the Report. The Detail view contains multiple sections, including Initiators, Responders, Service types, Initiator Countries, and Responder Countries. Depending on the number of entries, you may need to scroll down to see all the sections.

Note You can also apply a filter through the Filter Bar or by right-clicking the entry. Select the filter and click **Go**. The Report will show the detail view applicable to that filter.



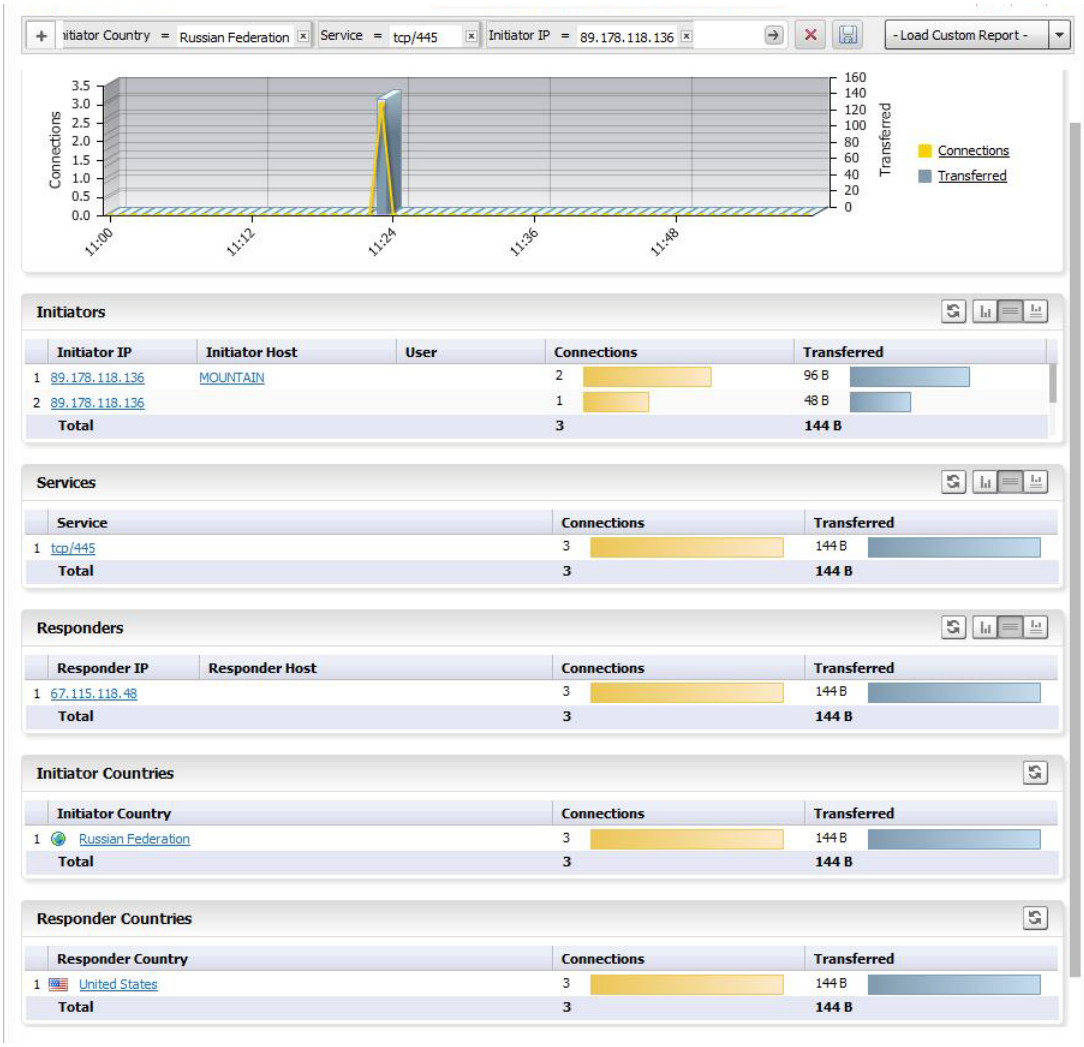
Step 3 To further filter the output, to view only tcp/https usage, click on the tcp/https entry under **Services**. A **Detail** report, filtered to show only usage of tcp/https, comes up. Notice that a

Service entry has been added to the Filter Bar.



Notice that the Report now focuses on the filter constraint from the drilled-down column.

Since this report also contains drill-down areas, you can drill down even further to add additional constraints to the results.



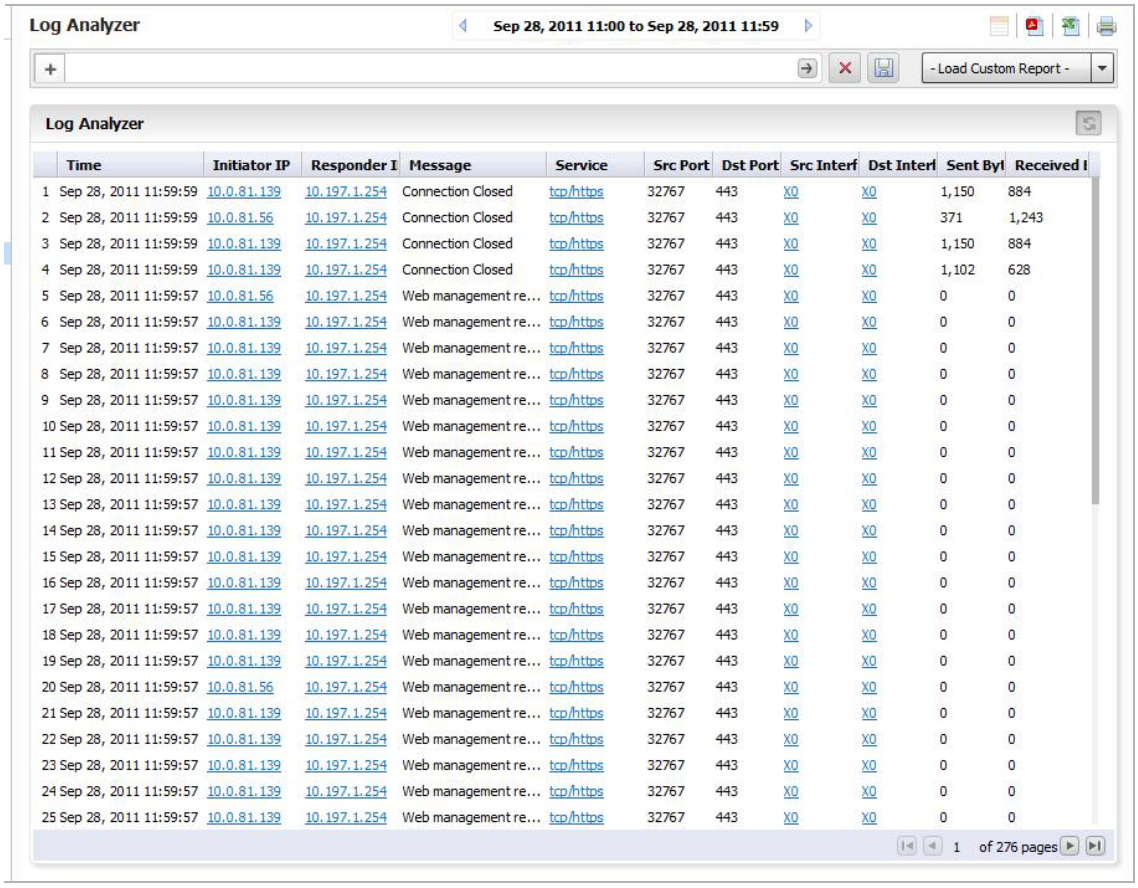
Note Many report categories contain a Details item in the list of reports. This link provides a shortcut directly to the Detail view of all sub-sections of the report. You can apply filters directly to the Detail view to further constrain the displayed information.

The Log Analyzer provides the most detailed Report information.

Step 4 To view the Log Analyzer, go to the **Reports** tab once you have drilled down to the desired level of detail and click on **Analyzers** > **Log Analyzer**.

Note Because Log Analyzer Reports can contain a very large amount of data, you may wish to limit the amount of data displayed on the page. The amount of data in the report can also affect the loading speed.

The Log Analyzer contains information about each connection, including port and interface information, number of Bytes sent, etc.



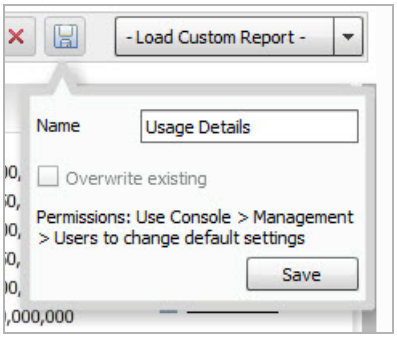
You can drill down through the Log Analyzer Report as well. Clicking on a column item adds an additional filter and narrows down your results, allowing you to zoom in on specific instances.

Some Log Analyzer reports can be reached as the final step of a drilldown process.

The bottom bar of the Log Analyzer contains a page bar, which allows you to navigate through the report by paging forward and backward, or going to the specific page of interest.

Custom Reports

Specific customized reports can be generated and saved by means of the Save icon. Click the Save icon to bring up a drop down allowing you to save a custom report.



This menu will be pre-filled with a name reflecting the report it was based on. If an earlier report with this name was generated, you can choose to overwrite it or save a new copy, or assign it a different name.

The new Custom report will be added to the pull-down menu accessed when you click **Load Custom Report**. It will also be added to the Reports Tab list under Custom. When a specific Custom report is selected on the Load Custom Report pull-down menu, the button will reflect the name of that report.

Custom Reports can also be accessed or deleted by going to **Reports** > **Custom** > **Manage Reports**.

Troubleshooting Reports

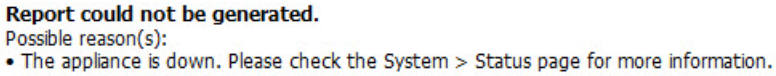
One of the most common reasons when a report does not display is that no data is available for the selected appliance. There are several reasons why you might see this error. Analyzer displays the most likely reason(s) and gives you instructions for ways to resolve the problem.

The most common examples are shown below.

Appliance is in a Provisioned State:

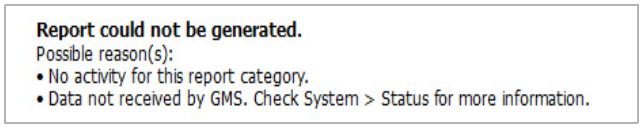
Analyzer is waiting for a handshake response signal from the appliance. Generally, the TreeControl menu will also flag the appliance with a lightning bolt on a yellow background.

Appliance is Down



Report Could Not Be Generated

There might be no data available for a variety of reasons. The most common causes are listed in this message, along with actions to take.



Managing Dell SonicWALL Analyzer Reports on the Console Panel

There are management settings for the Analyzer Reporting Module on the Analyzer **Console** panel. A Reports selection is available on the left menu bar, which allows you to set up certain tasks in the right-hand Management pane, which contains limited configuration screens, used for managing scheduled email report configuration, system debug-level logging, and show legacy reports.

In this pane, you can set CDP Summarizer parameters and schedule emailing or archiving of reports.

Data deletion or storage specified in these menus will take place after completion of the current reports run.

Reports generated by pre 7.1 releases of Dell SonicWALL Analyzer can still be viewed, but require specific configuration. See “Show Legacy (pre Analyzer 7.1) Reports” section on page 173.

CHAPTER 6

Viewing Firewall Reports

This chapter describes how to generate reports using the SonicWALL Analyzer Reporting Module. The following section describes how to configure the settings for viewing reports:

Firewall Reporting Overview

The Reports available under the Firewall tab provide specific information on data gathered by the SonicWALL Analyzer interface.

For a general introduction to reporting, see the "Dell SonicWALL Analyzer Reporting Overview" section on page 85.

The Firewall reports display either summary or unit views of connections, bandwidth, uptime, intrusions and attacks, and SRA usage, displayed in a Data Container. Information can be viewed in either chart (timeline or pie chart) form, or tabular (grid) format. The list of available reports allows you to navigate to a high-level or specific view.

All of the reports in Analyzer report on data gathered on a specific date or range of dates. Data can be filtered by time constraints and data filters.

Benefits of Firewall Reporting

Firewall Reports allow you to access both real-time and historical reports and view all activity on SonicWALL Internet security appliances. By monitoring network access, logins, and sites accessed, you can enhance system security, monitor internet usage, and anticipate future bandwidth needs.

You can gain more information from the display, simply by hovering the mouse pointer over certain sections. Additionally, by clicking on selected sections of a pie chart or bar-graph timeline view, you can view more information or view different aspects of the information presented.

Firewall Reports Tab

The Firewall tab gives you access to the Firewall's reports section of the SonicWALL Analyzer management interface. Reporting supports both graph and non-graph reports, and allows you to filter data according to what you wish to view. It supports multiple product-licensing models.

Firewall Reports provide the following features:

- Clickable reports with drill-down support on data rows
- Report data filtering through the Search Bar
- Log Analyzer

You can view Reports either as Summary reports for all or selected units on the SonicWALL Analyzer network, or view detailed reports for individual units.

Viewing Available Firewall Report Types

To view the available types of reports for the Firewall appliances, perform the following steps:

Step 1 Log into your Analyzer management console.

Step 2 Click the **Firewall** tab.

Step 3 Select an appliance or global view from the TreeControl.

Step 4 Expand the desired selection on the Reports list and click on it.

Note All Reports show a one-day period unless another interval is specified in the Time Bar.

The following types of reports are available:

Global Level Reports:

- Data Usage
  - Summary: connections, listed by appliance, for one day (default)
- Applications
  - Summary: connections, listed by application, for one day (default)
- Web Activity
  - Summary: hits, listed by appliance, for one day (default)
- Web Filter
  - Summary: access attempts, listed by appliance, for one day (default)
- VPN Usage
  - Summary: VPN connections, listed by appliance, for one day (default)
- Threats
  - Summary: connection attempts, listed by appliance, for one day (default)

Note Summary Reports are not drillable and no Detail view is available.

Unit Level Reports

Detail views are available for all Report items unless otherwise noted.

- Data Usage
  - Timeline: connections for one day (default)
  - Initiators: Top Initiators, listed by IP address, Initiator Host, User, and Responder, displayed as a pie chart

    - Responders: Top Responders, listed by IP address, Responder Host, and Initiator, displayed as a pie chart
    - Services: connections, listed by service protocol, displayed as a pie chart
    - Details: provides a shortcut to the Detail view normally reached by drilling down. Detail sections include: Initiators, Services, Responders, Initiator Countries, and Responder Countries. Additional filtering/drilldown takes you to the Log Analyzer
- Applications
    - Data Usage connections, listed by application and threat level
    - Detected: events, listed by application and threat level
    - Blocked: blocked events, listed by application and threat level
    - Categories: types of applications attempting access
    - Initiators: events displayed by Initiator IP and Initiator host
    - Timeline: events over one day
- User Activity
    - Details: a detailed report of activity for the specified user
- Web Activity
    - Category: hits and browse time listed by information category
    - Sites: sites visited by IP, name, and category, with hits and browse time
    - Initiators: Initiator host and IP with category and user
    - Timeline: site hits with time of access and browse time
    - Details: provides a shortcut to an access timeline and Detail view normally reached by drilling down. Detail sections include: Categories, Sites, and Initiators.
- Web Filter
    - Category: hits and browse time listed by information category
    - Sites: sites visited by IP, name, and category, with hits and browse time
    - Initiators: Initiator host and IP with category and user
    - Timeline: site hits with time of access and browse time
    - Details: provides a shortcut to an access timeline and Detail view normally reached by drilling down. Detail sections include: Categories, Sites, and Initiators.
- VPN Usage
    - Policies: lists connections by VPN Policy
    - Initiators: Initiator host and IP with category and user
    - Services: Top VPN Services by Service Protocol
    - Timeline: VPN connections over a 1 day period
- Intrusions
    - Detected: number of intrusion events by category
    - Targets: number of intrusion events by target host and IP
    - Timeline: intrusions listed by time of day
- Gateway Viruses
    - Blocked: blocked virus attacks and number of attempts at access
    - Targets: targeted hosts and IP addresses

    - Initiators: initiating users, hosts, and IP addresses of the virus attack
    - Timeline: times when the virus attempted to gain access, displayed over time
  - Spyware
    - Detected: spyware detected by the firewall
    - Blocked: spyware blocked by the firewall
    - Targets: targeted hosts and IP addresses
    - Initiators: initiating users, hosts, and IP addresses of spyware download
    - Timeline: times when the spyware accessed the system, displayed over time
  - Attacks
    - Attempts: type of attack and times access was attempted
    - Targets: host and IP address, and number of times access was attempted
    - Initiators: top attack initiators by IP and host
    - Timeline: time and number of attempts at access, displayed over time
  - Authentication: authenticated users, their IP addresses, and type of login/logout
    - User Login
    - Admin Login
    - Failed Login
  - Custom Reports: allows access to saved custom reports
  - Analyzers
    - Log Analyzer: provides a detailed event-by event listing of all activity. The Log Analyzer is drillable, but no Detail sections are available.

The Report contains a filter bar at the top, plus the actual Data Container. The default Data Container contains an interactive chart view, which contains either a grid view, containing a text version of the information. One or more sections may be present in the grid view. Toggle buttons allow you to display the Chart view, Grid view, or Chart and Grid view.

Grid sections are arranged in columns. Columns may be rearranged to view them from the top down or bottom up, by clicking the up and down arrows in the column headings. You can narrow results by applying a filter to a column: right-click on a column heading and click **Add Filter**.

Hypertext-linked columns are drillable, meaning you can click on the hypertext entry to bring up a Detail view with more information on the desired entry. Detail views might have multiple sections.

The Detail views are usually reflected in the sub-headings under the Reports list, which provide a shortcut directly to the Detail Report. To go to the full Detail view, click the **Details** entry in the Reports list. From the Detail view, you can access the system logs, for event-by-event information, or further filter the results. For more information on using the Log Analyzer to view and filter syslog reports, see the “Using the Log Analyzer” section on page 126.

Details views can contain multiple sections. To determine if you have reached the end of the list of sections, check for the time zone message, which indicates the end of the Detail View.

Reports with hyperlinked columns can be filtered on the column or by drilling down on the hyperlinked entry.

You can also get to a filtered Detail view by clicking the section representing the desired information in the pie chart.

To save a filtered view for later viewing, click on the **Save** icon on the Filter Bar. The saved view will now appear under Custom Reports.

To learn more about Custom reports, see the “Custom Reports” section on page 132

How to View Firewall Reports

The sections contain the following information:

- Node information—Information on the firewall(s) is displayed at the global or unit level.
- Syslog Categories—The types of syslog data selected to be collected for the selected appliance.
- Syslog Servers—The IP address and Port number of the syslog servers configured to collect data from the selected appliance.
  - Synchronize Appliance Information with Analyzer—Click the **Synchronize Appliance Information Now** link to refresh status data about the monitored appliances. This status information is normally updated every 24 hours.
- Getting Started With Analyzer—Click the **Open Getting Started Instructions In New Window** link to open the Analyzer installation and initial configuration instructions in a separate window.

The Firewall Summary reports display an overview of bandwidth, uptime, intrusions and attacks, and SRA usage for managed SonicWALL Firewall appliances. The security summary report provides data about worldwide security threats that can affect your network. The summaries also display data about threats blocked by the SonicWALL security appliance.

Viewing Global Summary Reports

Summary reports for data usage, applications, web usage and filtering, VPN usage, and threats for managed SonicWALL appliances are available at the global level, through the TreeControl menu. Summary reports are available for:

- Data Usage
- App Control
- Web Usage
- Web Filtering
- VPN Usage
- Threats

Group-level Summary reports provide an overview of information for all Firewalls under the group node for the specified period. The report covers the connections and transfers by appliance for Data Usage, App Control, and VPN Usage, For Web Usage and Web Filters, hits are also included. Web filters and Threats list attempts at connection. Unless specified differently in the Date Selector, the Summary report covers a single day. Global Summary reports are not drillable.

The Dashboard Summary report displays statistics, alerts, graphical summary reports, and a list of available custom report templates. Displayed statistics can include total bandwidth, total attacks and other measurable information. The alerts list is displayed when the configured threshold has been reached. A wide range of graphical reports are also available for display.

You can configure the **Dashboard > Summary** report contents in the **Firewall > Configuration > Settings** page.

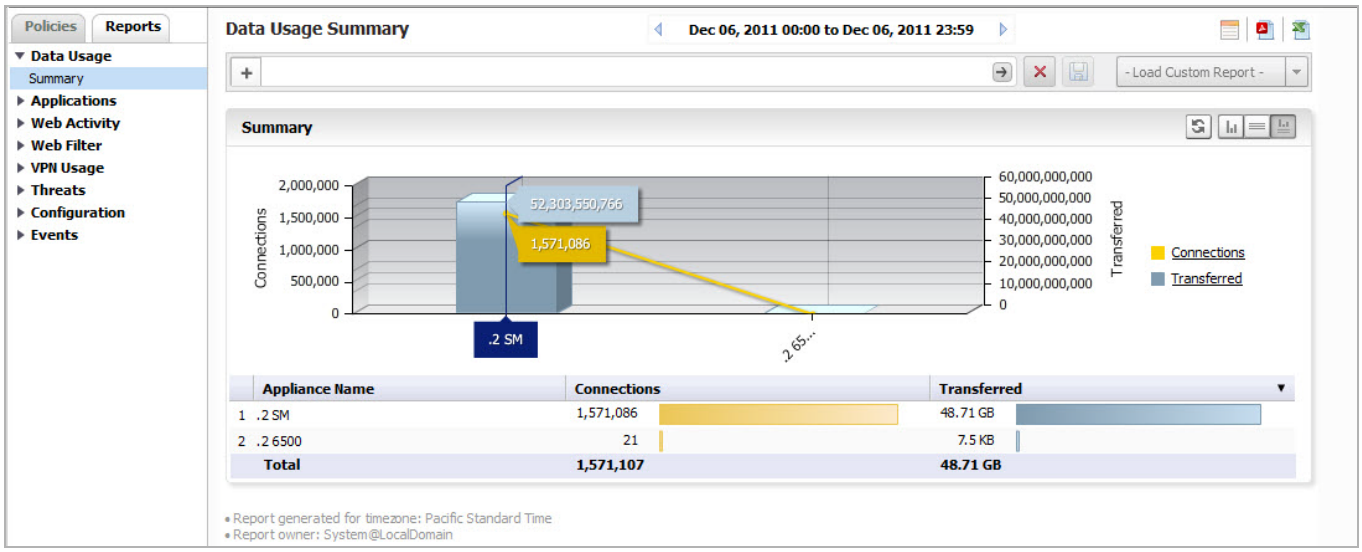
To view the Summary report, perform the following steps:

Step 1 Click the **Firewall** tab.

Step 2 Select the global icon.

Step 3 Click **Data Usage** > **Summary**.

The timelines at the top of the page display the totals, and the grid section sorts the information by appliance or applications.



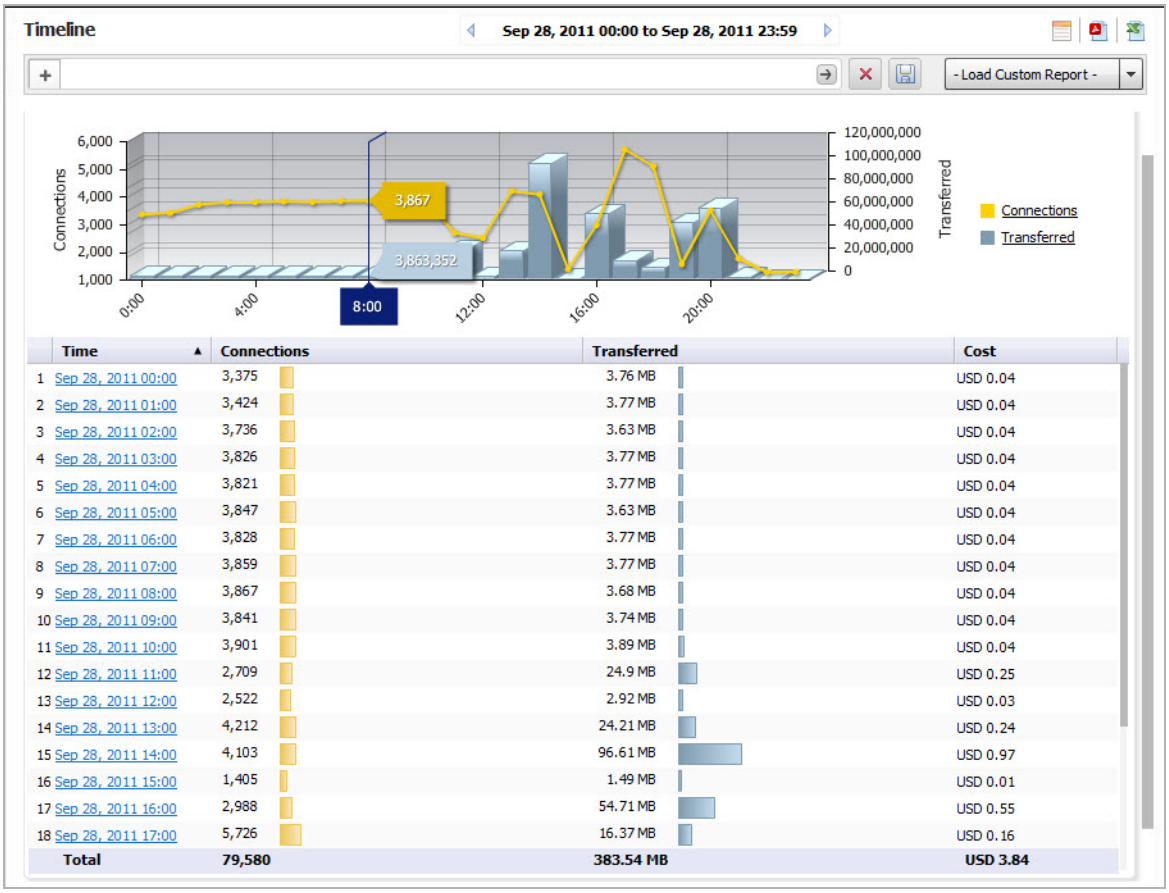
Unit level reports display status for an individual SonicWALL appliance.

Viewing Data Usage Reports

Step 1 Click the **Firewall** tab.

Step 2 Select the global iconor a SonicWALL appliance.

Step 3 Click **Data Usage > Timeline**. (This is the default view when the Firewall Report interface comes up.)



	Time	Connections	Transferred	Cost
1	Sep 28, 2011 00:00	3,375	3.76 MB	USD 0.04
2	Sep 28, 2011 01:00	3,424	3.77 MB	USD 0.04
3	Sep 28, 2011 02:00	3,736	3.63 MB	USD 0.04
4	Sep 28, 2011 03:00	3,826	3.77 MB	USD 0.04
5	Sep 28, 2011 04:00	3,821	3.77 MB	USD 0.04
6	Sep 28, 2011 05:00	3,847	3.63 MB	USD 0.04
7	Sep 28, 2011 06:00	3,828	3.77 MB	USD 0.04
8	Sep 28, 2011 07:00	3,859	3.77 MB	USD 0.04
9	Sep 28, 2011 08:00	3,867	3.68 MB	USD 0.04
10	Sep 28, 2011 09:00	3,841	3.74 MB	USD 0.04
11	Sep 28, 2011 10:00	3,901	3.89 MB	USD 0.04
12	Sep 28, 2011 11:00	2,709	24.9 MB	USD 0.25
13	Sep 28, 2011 12:00	2,522	2.92 MB	USD 0.03
14	Sep 28, 2011 13:00	4,212	24.21 MB	USD 0.24
15	Sep 28, 2011 14:00	4,103	96.61 MB	USD 0.97
16	Sep 28, 2011 15:00	1,405	1.49 MB	USD 0.01
17	Sep 28, 2011 16:00	2,988	54.71 MB	USD 0.55
18	Sep 28, 2011 17:00	5,726	16.37 MB	USD 0.16
	Total	**79,580**	**383.54 MB**	**USD 3.84**

Viewing User Activity Logs

Web User Activity logs allow you to filter results to view only the activity of a specific use**r.**

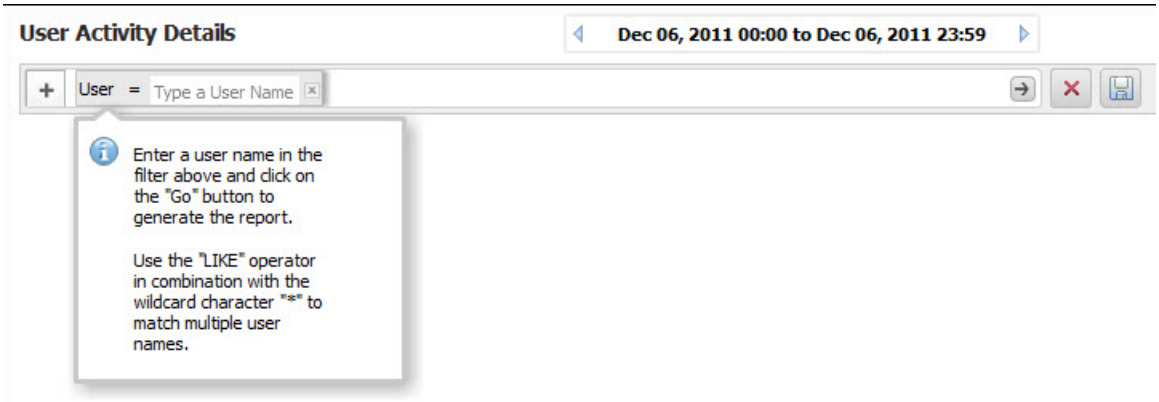
The User Activity Analyzer provides a detailed report listing activity filtered by user. If a user report has been saved previously, bringing up the User Activity Analyzer will display a list of saved reports under the Filter Bar.

If you wish to create a new report, use the Filter Bar to create a new report.

Step 1 Click the **Firewall** tab.

Step 2 Select a SonicWALL appliance.

Step 3 Click on **User Activity** > **Details** to bring up the **User Activity Analyzer**. The User Activity Analyzer generates a Detail report based on the user name.



If no user activity reports were saved, only the Filter Bar will display, with the User filter pre-selected. You can enter a specific user name, or use the LIKE operator wildcards (*) to match multiple names.

Step 4 Enter the name of the user into the field and click the Go (arrow) button to generate the report

The customized User Activity Details report will display a timeline of events, Initiators, Responders, Services, Applications, Sites visited, Blocked site access attempted, VPN access policy in use, user authentication, Intrusions, Initiator Countries, and Responder Countries associated with that particular user.

Data for a particular user may not be available for all of these categories.

Viewing Applications Reports

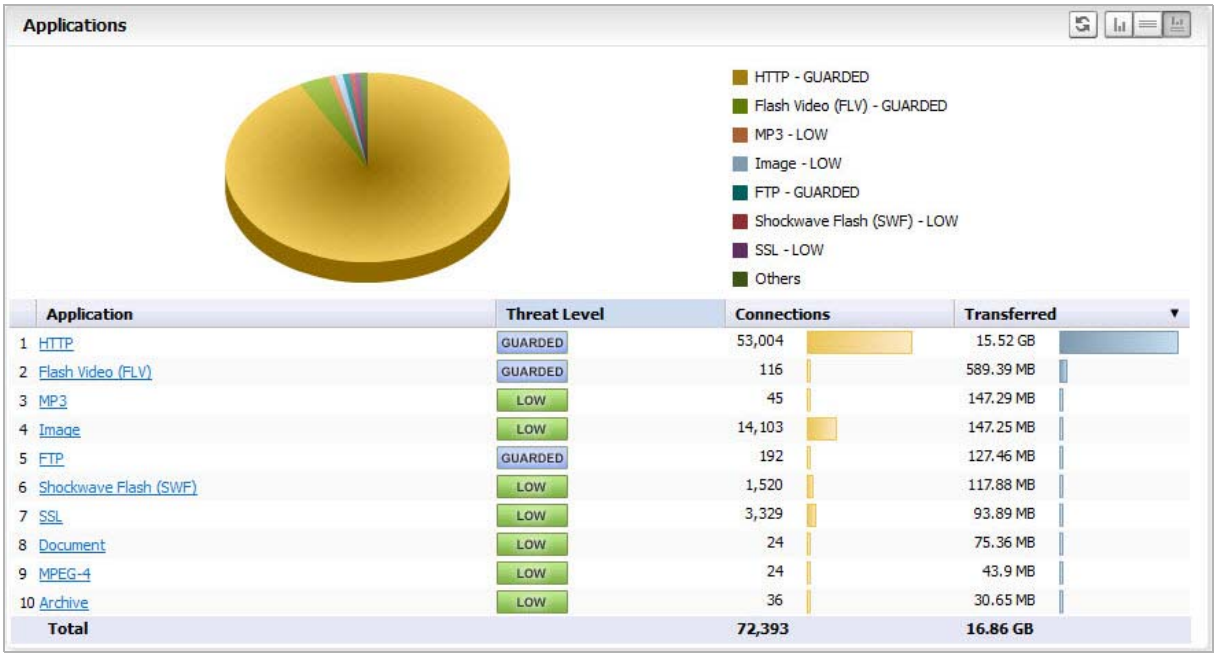
Application Reports provide details on the applications detected and blocked by the firewall, and their associated threat levels.

Step 1 Click the **Firewall** tab.

Step 2 Select a SonicWALL appliance.

Step 3 Click **Application > Data Usage**.

The Applications Report displays a pie chart with the application and threat level it poses.



	Application	Threat Level	Connections	Transferred
1	HTTP	GUARDED	53,004	15.52 GB
2	Flash Video (FLV)	GUARDED	116	589.39 MB
3	MP3	LOW	45	147.29 MB
4	Image	LOW	14,103	147.25 MB
5	FTP	GUARDED	192	127.46 MB
6	Shockwave Flash (SWF)	LOW	1,520	117.88 MB
7	SSL	LOW	3,329	93.89 MB
8	Document	LOW	24	75.36 MB
9	MPEG-4	LOW	24	43.9 MB
10	Archive	LOW	36	30.65 MB
	Total		**72,393**	**16.86 GB**

You can drill down for additional Details views on connections over time (Timeline view), Data Usage, Detected applications, Blocked applications, Categories of applications, top initiators.

Viewing Web Activity Reports

Web Activity Reports provide detailed reports on browsing history.

Step 1 Click the **Firewall** tab.

Step 2 Select a SonicWALL appliance.

Step 3 Click **Web Activity > Categories**.

The Web Activity Report displays a pie chart with the Top Categories of type of access, total browse time, and hits.

You can drill down for additional Details views on connections over time (Timeline view), Sites visited, Categories of sites, and Top Initiators. A Details entry links directly to the details view of all entries.

Viewing Web Filter Reports

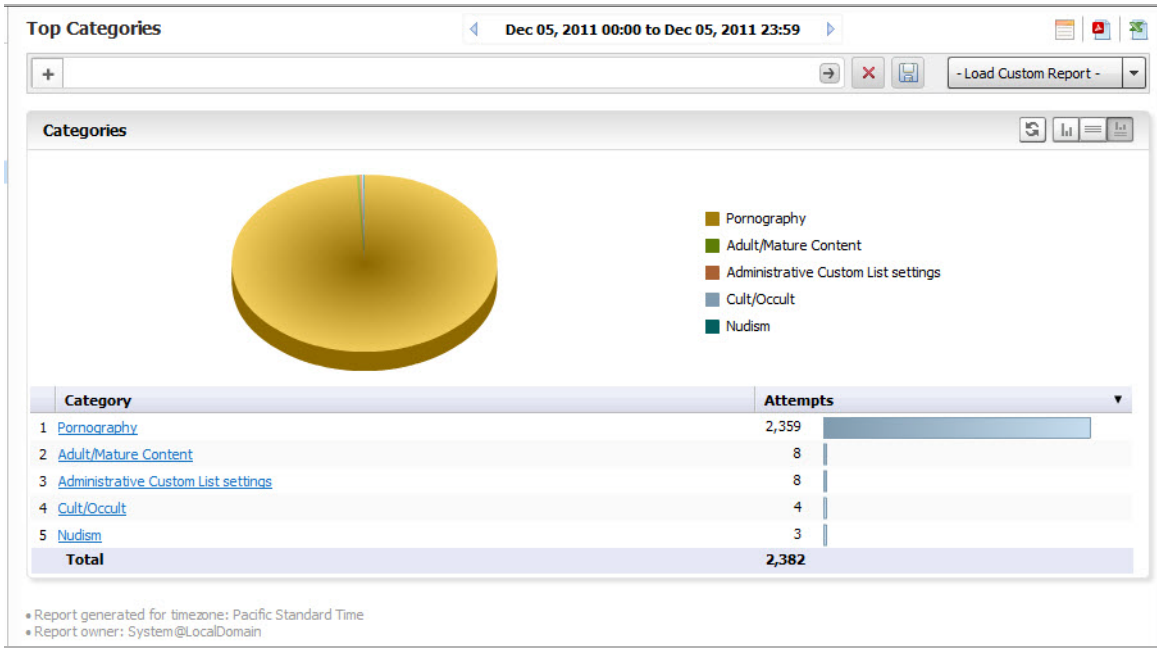
Web Filter Reports provide detailed reports on attempts to access blocked sites and content.

Step 1 Click the **Firewall** tab.

Step 2 Select the global icon or a SonicWALL appliance.

Step 3 Click **Web Filter > Categories**.

The Web Filter Report displays a pie chart with the Top Categories of blocked access and total attempts to access.



You can drill down for additional Details views on connections over time (Timeline view), Sites visited, Categories of sites, and Top initiators. A Details entry links directly to the details view of all entries.

Viewing VPN Usage Reports

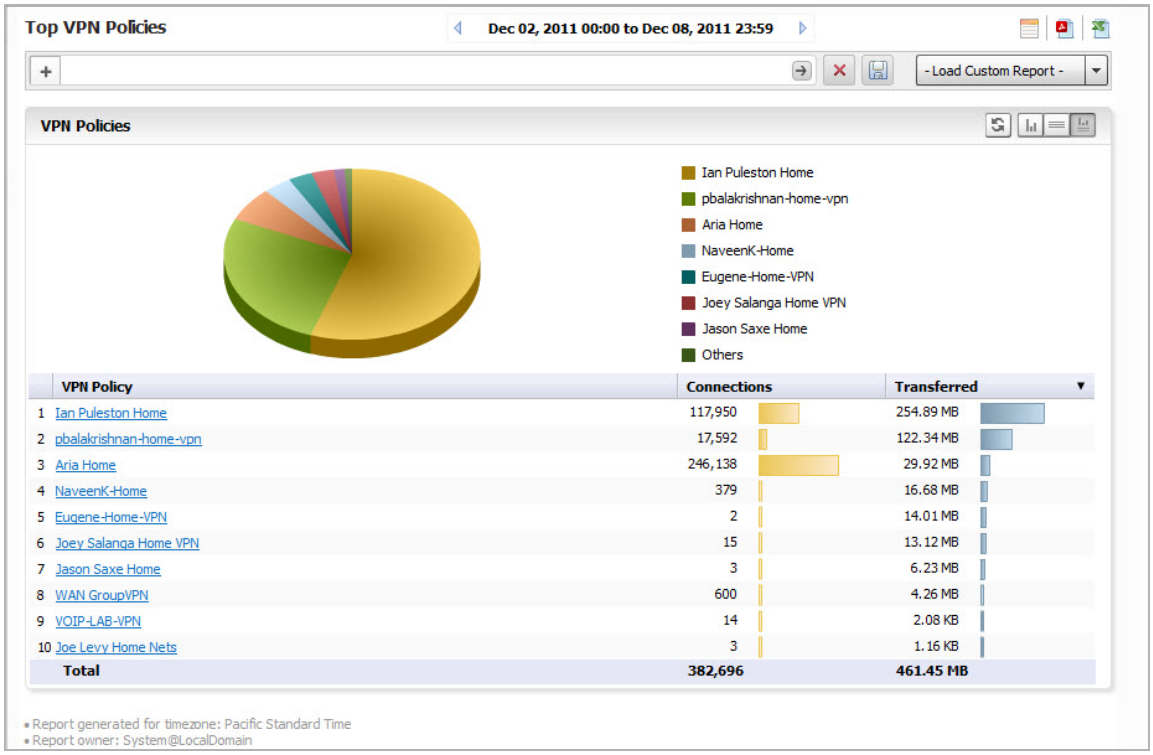
VPN usage reports provide details on the services and policies used by users of virtual private networks.

Step 1 Click the **Firewall** tab.

Step 2 Select a SonicWALL appliance.

Step 3 Click **VPN Usage > Policies.**

The VPN Usage Report displays total connections for each VPN Policy item as a pie chart and tabular grid view.



You can drill down for additional Details views on Service protocols and Top initiators.

Viewing Intrusions Reports

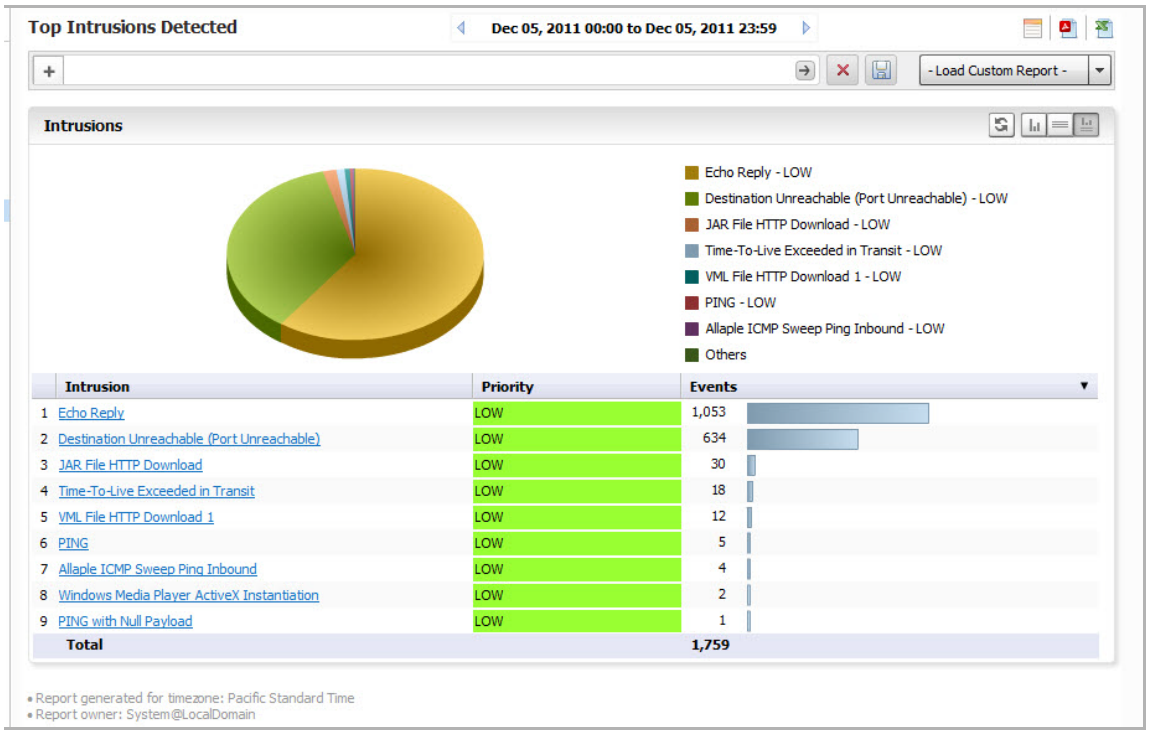
Intrusion Reports provide details on types of intrusions and blocked access attempts.

Step 1 Click the **Firewall** tab.

Step 2 Select a SonicWALL appliance.

Step 3 Click **Intrusions > Detected** .

The Attacks report provides a pie chart and a list of the initiating IP addresses, hosts, and users, with number of attempts for each.



Drill down for additional Detail views of Intrusion Categories, Targets, Initiators, Ports affected, Target Countries, and Initiator Countries.

Viewing Gateway Viruses Reports

The Gateway Viruses reports provide details on the Top Viruses that were blocked when attempting to access the firewall.

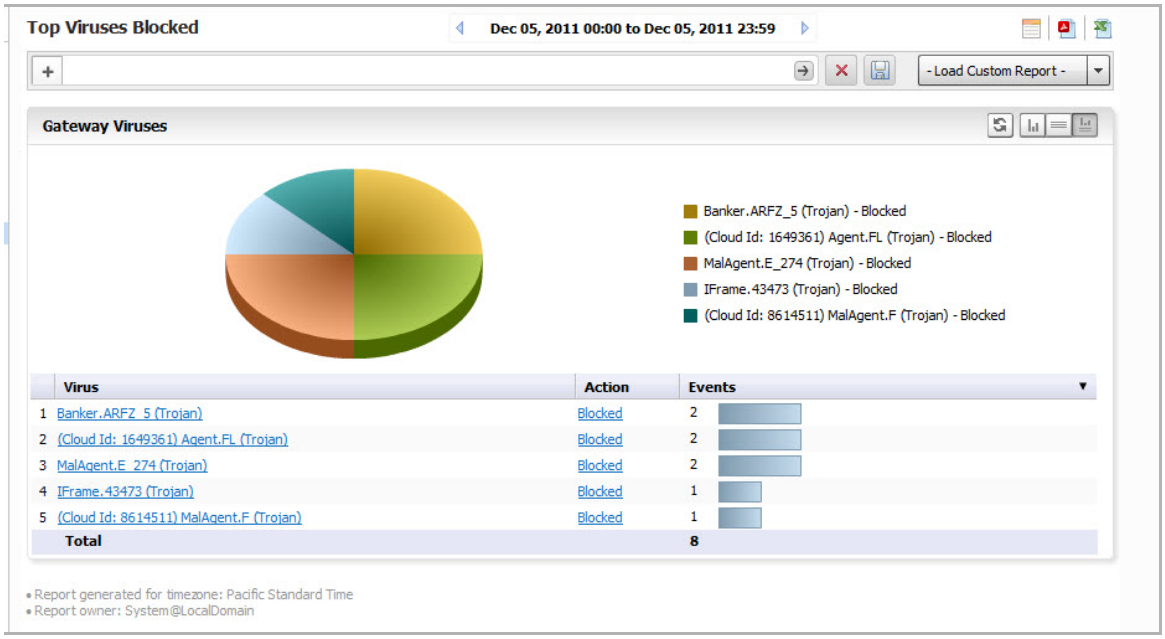
Step 1 Click the **Firewall** tab.

Step 2 Select a SonicWALL appliance.

Step 3 Click **Gateway Viruses > Blocked** .

The Top Viruses report appears.

The report provides details on the viruses blocked, the targets, initiators, and a timeline of when they attempted access.



Drilling down provides a list of virus identity, Targets, Initiators, Target Countries, and Initiator Countries.

Viewing Spyware Reports

The Spyware report gives details of the spyware that was detected and/or blocked, the targets, initiators, and a timeline of when they attempted access.

Step 1 Click the **Firewall** tab.

Step 2 Select a SonicWALL appliance.

Step 3 Click **Spyware > Detected**.

The report provides details on the types of spyware detected and blocked, targets.

Drilling down provides a list of virus identity, Targets, Initiators, Target Countries, and Initiator Countries.Drilling down lists countries of origin, and target countries.

Viewing Attacks Report

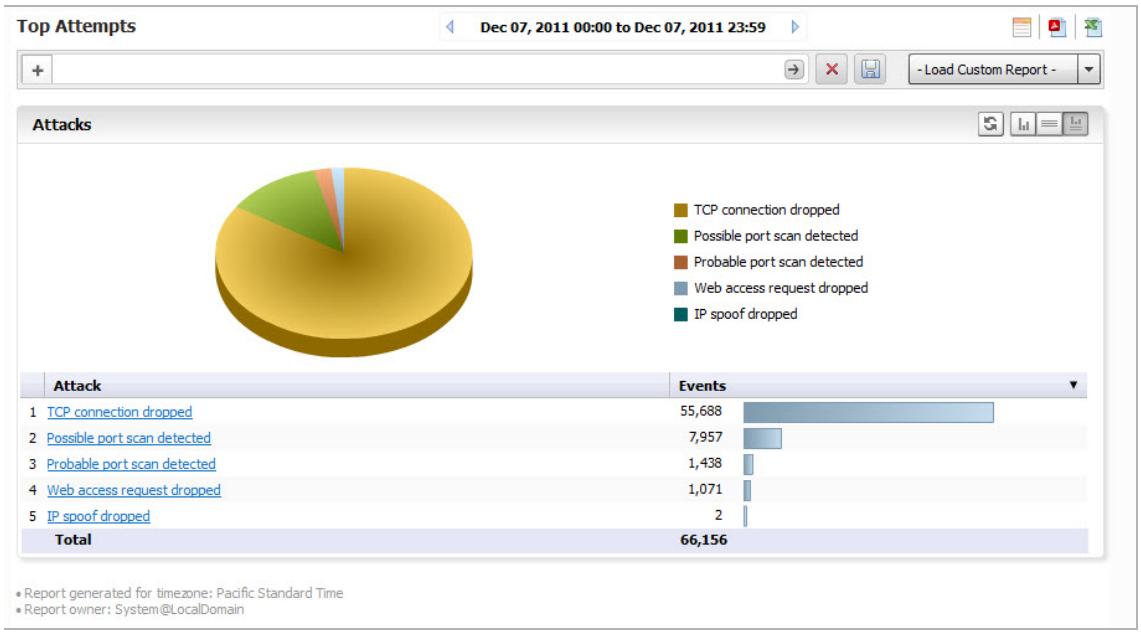
The Attacks report lists attempts to gain access, target systems, initiators, and a timeline of when the attack occurred.

Step 1 Click the **Firewall** tab.

Step 2 Select a SonicWALL appliance.

Step 3 Click **Attacks > Attempts**.

The Attacks report provides a pie chart and a list of the initiating IP addresses and hosts.



Drill down for additional Detail views of Intrusion Categories, Targets, Initiators, Ports affected, Target Countries, and Initiator Countries.

Viewing Authentication Reports

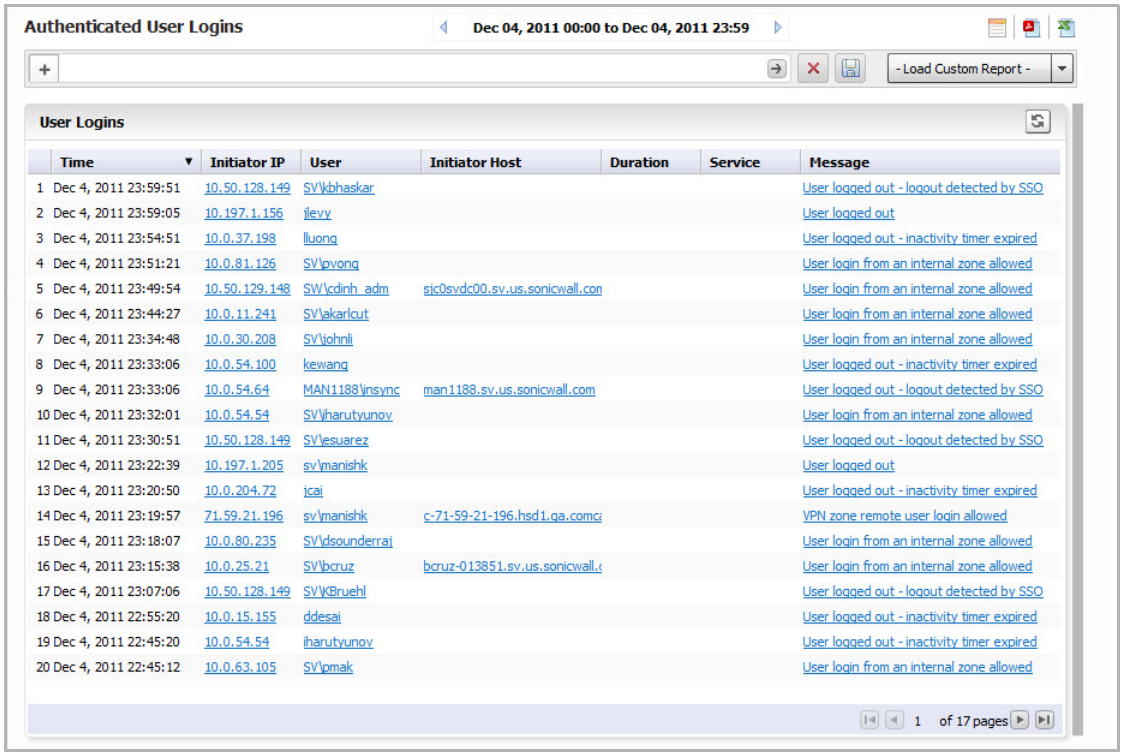
Authentication reports provide information on users attempting to access the Firewall.

Step 1 Click the **Firewall** tab.

Step 2 Select a SonicWALL appliance.

Step 3 Click **Authentication > User Login**.

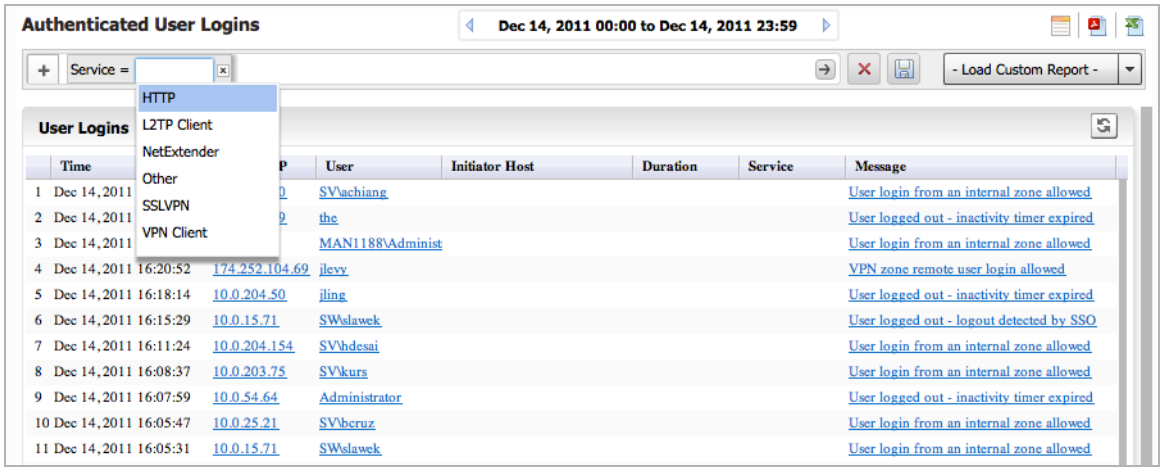
The Authentication report displays a list of authenticated users, their IP addresses, service, time they were logged in, and type of login/logout. Additional Reports are available for Administrator logins and failed login attempts.



Clicking on hyperlinks provides additional filtering for the reports.

You can filter on the Service to view SRA and other appliances by drilling down to the syslog.

Step 1 Go to the filter bar and click on the + and select **Service** from the pull-down menu. Click on the = operator, and click on the field next to it to bring up the pull-down menu. Select SSLVPN from the pull-down list



Step 2 Click **Go** to view a report for that Service.

Note For the Duration and Service categories to be present, the Firewall appliance firmware must be at least version 5.6.0.

Using the Log Analyzer

The Log Analyzer allows advanced users to examine raw data for status and troubleshooting. The Analyzer logs contain detailed information from the system logs on each transaction that occurred on the specified SonicWALL appliance. These logs can be filtered or drilled down to further narrow the focus of the information, allowing analysis of data about alerts, interfaces, bandwidth consumption, etc. The Log Analyzer is only available at the individual unit level.

Because of space constraints, some column items, particularly the log event messages, may not be fully visible in the Reports pane. To view the full report, export the report to an Excel spreadsheet to view, sort, or organize messages.

Log information can be saved for later analysis and reloaded from Custom Reports.

To load a report for viewing, either:

- Click **Load Custom Report** and select from the pull-down list of saved Custom Reports.
- Click on **Analyzers** > **Log Analyzer** to view the current log.

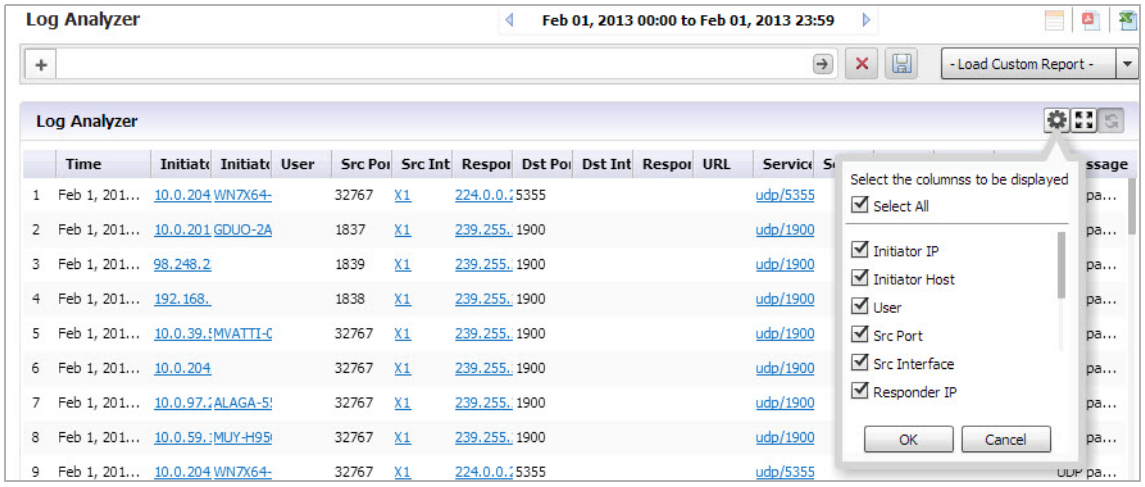
Note The Log Analyzer entries display raw log information for every connection. Depending on the amount of traffic, this can quickly consume a large amount of space in the database. It is highly recommended to be careful when choosing the number of days of information to be stored.

Viewing the Log Analyzer

The log displays information specific to either a particular report or overall system information, depending on the path used to reach the log, either from the individual report level or from the Log Analyzer entry on the Reports tab. Entries in the Analyzer log will vary, according to the relevant report type. You can customize the log entries by using the following options:

Show/Hide Log Columns

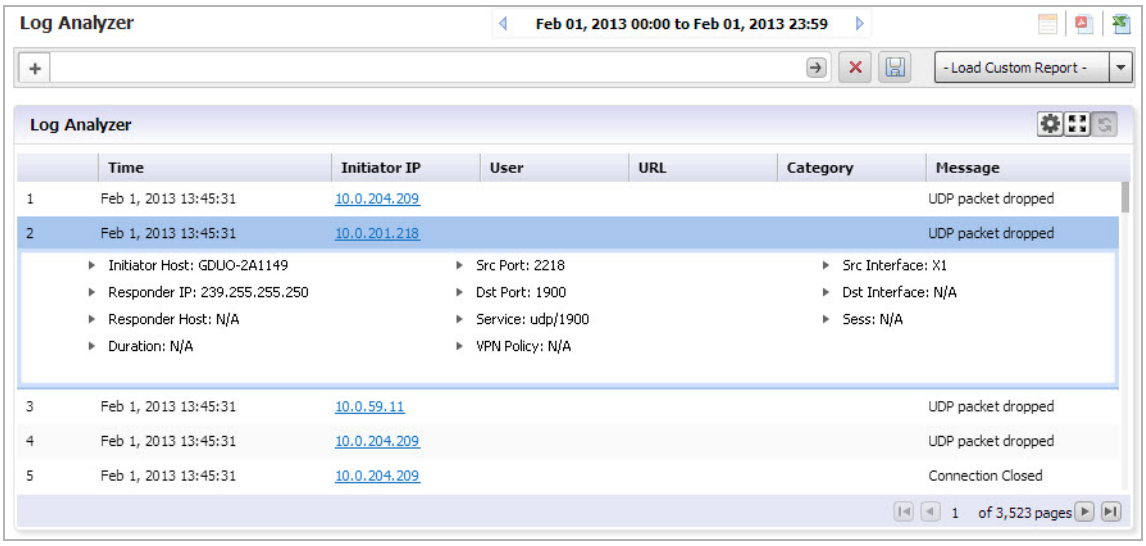
Use the Show/Hide Columns function to hide columns that you do not want to display in the Analyzer Log. Just click the **Configure the Log Analyzer** icon, then select the columns that you want to display and deselect the ones that you do not want to display. By configuring the displayed columns, the Log Analyzer gives a more clean, concise, and meaningful way to view the logs, instead of displaying unnecessary columns that take up valuable real estate.



Note “Serial number” column and “Time” column are not part of the list to be configured because they are necessary for any displays.

Row-Based Expansion

Instead of showing all the column info at once, the row-based expansion simplifies the screen and gives on-demand info through a single click.



Click on each row to pull down the hidden column information.

Note This feature is only available after you sort the columns using the show/hide function.

Full Screen Mode

Switch to full screen mode by clicking the **Full Screen Mode** toggle icon. This will populate the entire browser screen with the Log Analyzer page, hiding the tree control and reports panels.

Session-Based Configurations

All column configurations for the Log Analyzer are recorded in each session. This is so that within the session, users can have the desired/configured tabular view of the Log Analyzer at all times.

Priority

The log event messages are color-keyed according to priority. Red is the highest priority, followed by yellow for Alerts. Messages without color keys are informational, only. The color categories are:

- Alert: Yellow
- Critical: Red
- Debug: White
- Emergency: Red
- Error: White

- Info: White
- Notice: White
- Warning: White

Color keys allow you to immediately focus on the priority level of the message, and filter data accordingly.

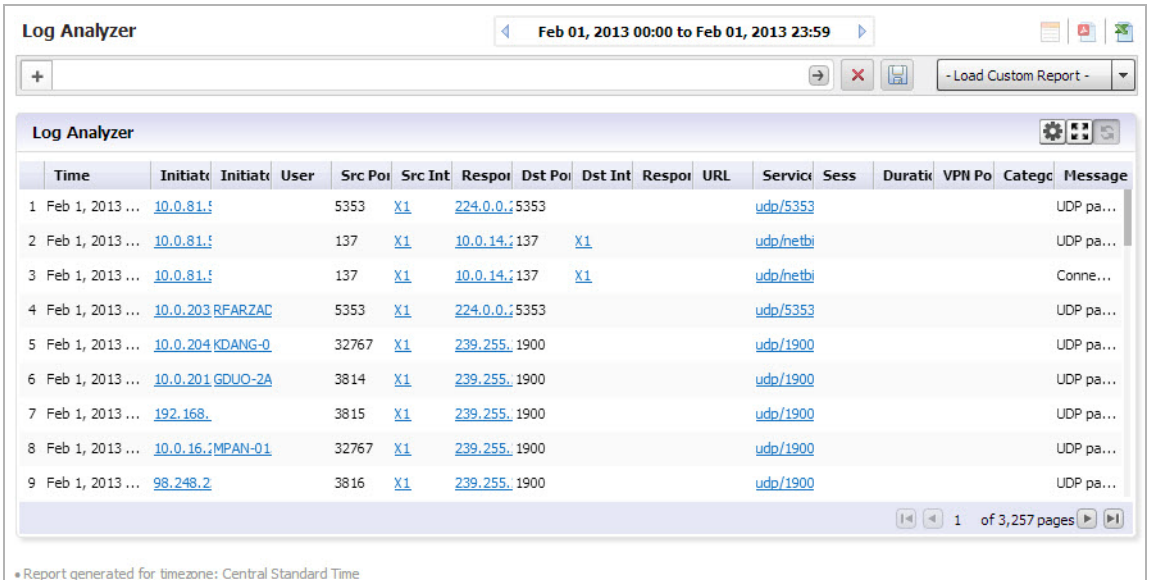
Filtering the Analyzer Log

The Log Analyzer allows you to add filters to view user-or incident-specific data. The Log analyzer can be reached either by drilling down in individual reports, or from the Analyzers item under the Reports tab.

To view the Analyzer Log, perform the following steps:

Step 1 Select a SonicWALL appliance from the TreeControl pane.

Step 2 Click to expand the **Analyzer** tree and click on Log Analyzer. The saved Log Analyzer report page displays.



Note Because system logs have a large number of entries, it is advisable to constrain the number of entries displayed on the page.
Saved system logs are limited in the number of rows that will be saved. If saving to PDF, a maximum of 2500 rows will be saved. If saving to Excel, a maximum of 10,000 rows will be saved.

Step 3 To add a filter, click on the + in the Filter Bar and specify the desired filter item and parameters.

Available filters include filters for Application, Category, DST Interface, DST Port, Duration, Initiator Country, Host, or IP address, Interface, Message, Priority, Responder country, IP, or Name, Service, Session, Src Interface, Src Port, URL, User, or VPN Policy. This full list is available from the Log Analyzer Entry.

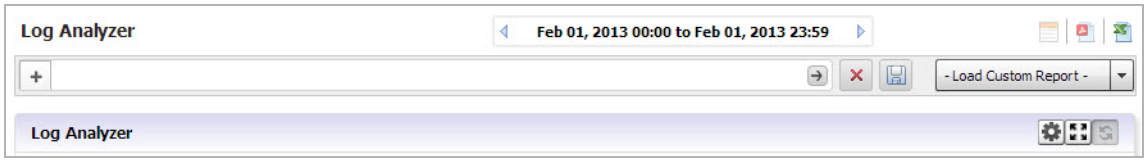
If you are viewing the log in the Log Analyzer view for a specific application entry, only those filters specific to that entry will be available.

Log views are drillable, and will add filters as column entries are drilled. Click on an entry of interest to add a filter and further constrain the information displayed.

Log Analyzer Use Case

In the following use case, we will sort and filter the captured event information to evaluate threats targeted toward the X0 default interface.

On the Reports tab, click on **Analyzers** > **Log Analyzers**.

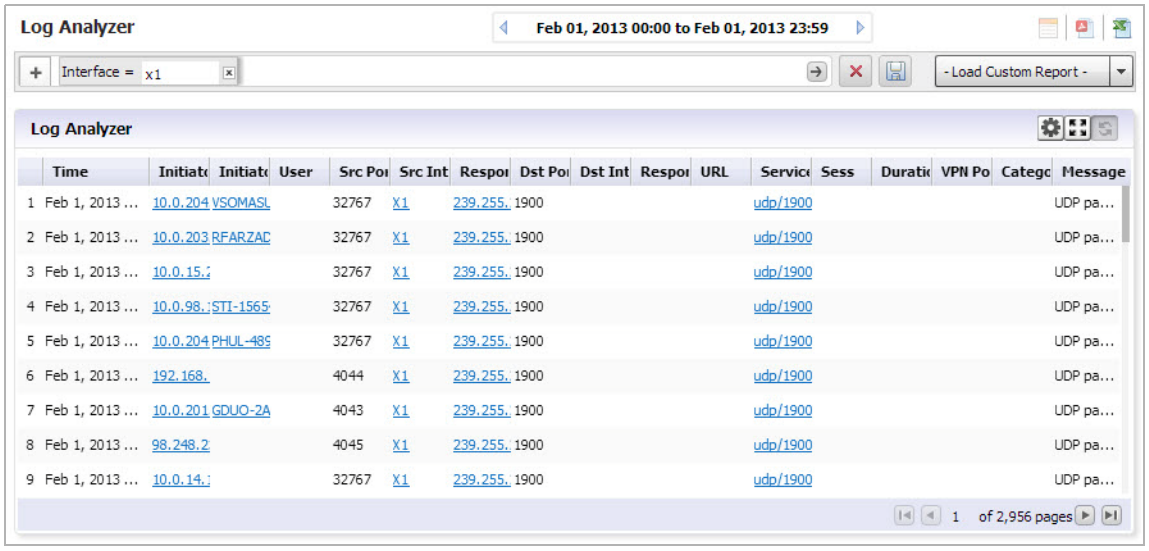


Step 1 In the Log Analyzer, click on the + to add a filter, and select the **Interface** filter.

Step 2 Type in *X1* to specify the default interface filter.

Step 3 Click on the **Go** button.

The Log Analyzer will be filtered on the X1 port interface.



This will allow you to begin debugging, or further investigate use of the database.

More information can also be found by using Universal Scheduled Reports.

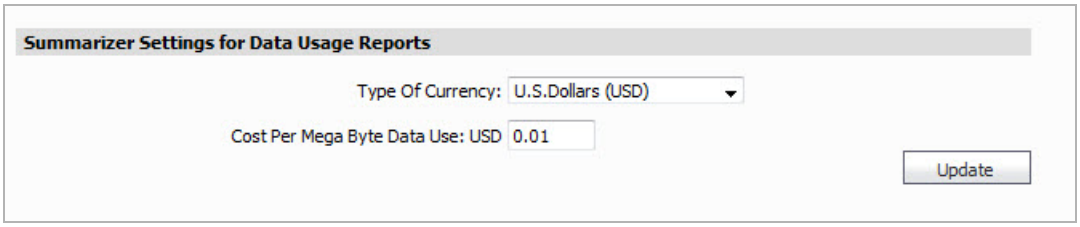
Configuration Settings

Configuration settings allow you to set up certain parameters for how data is displayed in Reports. You can set up currency cost per Megabyte for the Summarizer, or add filters for the Log Analyzer reports.

Setting Up Currency Cost for Summarizer

The Data Usage page contains a Cost per connection entry. You can set what currency and the cost per Megabyte.

Step 1 Click **Configuration** > **Settings** on the Reports tab.



Step 2 Select the currency of the desired country and the cost per MB.

Step 3 Click **Update**. The cost will be immediately reflect on the Data Usage page.

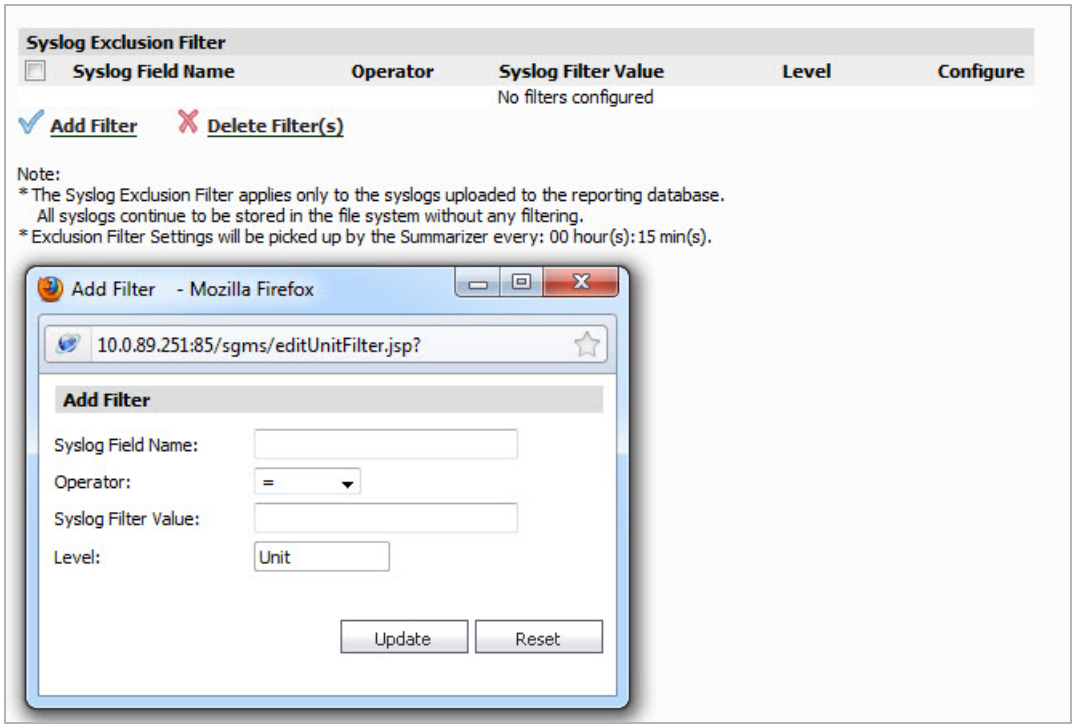
Adding Syslog Exclusion Filters

Exclusion Filters restrict what information is used to generate Reports. This is achieved by filtering out syslogs (based on the criteria specified in the Syslog Filter screen) from being uploaded to the Reports database. These filtered syslogs are, however, stored in the file system and archived, thus ensuring that all syslogs are available for audit trailing purposes. Excluding data from being uploaded to the Reporting database in this way can be useful in maintaining confidentiality regarding use history, or eliminating data corresponding to certain users who are not of interest. For instance, you might use an Exclusion Filter to eliminate data from the company CEO. This screen is used to specify syslog filters for the unit selected in the TreeControl. A similar screen exists for system wide syslog filtering, in the Console Panel's **Reports** > **Syslog Filter** screen

Step 1 To add an Exclusion filter, click on **Configuration** > **Filters**.

The Syslog Exclusion Filter page comes up. This page allows you to view what filters are currently applied, add filters, or remove filters.

Step 2 To configure and add an Exclusion Filter, click **Add Filter**. The Add Filter menu comes up.



Step 3 Specify the field you want to modify, and select an operator and value. Click **Update**.

The Reports will now be filtered according to the selected criteria. Exclusion Filter settings are picked up by the Summarizer at specified regular intervals.

Custom Reports

You can configure a report with customized filters, then save it for later viewing and analysis. Saving a Report allows you to view it later, by loading it through the Custom Reports interface. Custom Reports can either be saved directly, or configured through Universal Scheduled Reports. You can either load the report through the Custom Report pull-down on the Search Bar, or click **Reports** > **Custom** and choose from the list of saved Custom reports.

Regularly scheduled Custom Reports can be configured through the Universal Scheduled Reports interface, accessible through the Custom Reports icon in the upper right corner. These reports can be set up to be emailed to you on a regular schedule.

Custom Reports are available at the unit level for all appliances visible on the Firewall tab. The Log Analyzer must be enabled for the appliance.

The Manage Reports screen (**Custom Reports** > **Manage Reports**) allows you to view what Custom Reports are available and delete reports from the system.

For more information on configuring and scheduling custom Reports refer to the Universal Scheduled Reports section.

CHAPTER 7

Viewing SRA Reports

This chapter describes how to view SonicWALL Analyzer Secure Remote Access Reports. SRA reporting includes reports for the Web Access Firewall (WAF) and summarization for SRA appliances using Secure Remote Access (SRA).

This chapter contains the following sections:

SRA Reporting Overview

This section provides an introduction to the Secure Remote Access reporting feature. SonicWALL SRA appliances are protected by the user portal on the Web Application Firewall (WAF).This section contains the following subsections:

After reading the Analyzer SRA Reporting Overview section, you will understand the main steps to be taken in order to create and customize reports successfully.

For a general introduction to reporting, see the "Dell SonicWALL Analyzer Reporting Overview" section on page 85.

SRA Reports Tab

The SRA tab gives you access to the Secure Remote Access (SRA) Reports section of the Analyzer management interface. Reporting supports both graph and non-graph reports, and allows you to filter data according to what you wish to view.

What is SRA Reporting?

Secure Remote Access (SRA) reporting allows you to configure and design the way you view your reports and the manner in which you receive them. This feature offers various types of static and dynamic reporting in which you can customize the way information is reported.

SonicWALL Analyzer SRA reporting provides a visual presentation of User connectivity activity, Up_Down status, and other reports related to remote access. With SRA reporting, you are able to view your reports in enhanced graphs, create granular, custom reports, create scheduled reports, and search for reports using the search bar tool.

Custom reports are also available in SRA reporting. SonicWALL appliances managed with SRA provide Resource Activity reports for tracking the source, destination, and other information about resource activity passing through a SonicWALL SRA device that can then be saved as a Custom report, for later viewing.

Custom Reports can be created through an intuitive, responsive interface for customizing the report layout and configuring content filtering prior to generating the report. Two types of reports are available: Detailed Reports and Summary Reports. Both provide detailed information, but are formatted to meet different needs. A Detailed Report displays the data in sortable, resizable columns, while a Summary Report provides top level information in graphs that you can click to drill down for detailed information. By customizing the report, you can then save it for later viewing and analysis.

Once you set up a Custom Report that meets your needs, you can save the report for later viewing, then manage it through the Custom Reports Manage Reports entry, or export the report as a PDF or CSV (Excel) file.

Benefits of SRA Reporting

SRA reports provide visibility into the resource use by logged in users, leading to policies that enhance the user experience and the productivity of employees. The following capabilities contribute to the benefits of the SRA reporting feature:

- SRA Detail Level Reports can track events to the minute or second of the day for forensics and troubleshooting
- Interactive charts allow drill-down into specific details
- Table structure with ability to adjust column width of data grid
- Improved report navigation
- Report search
- Scheduled reports

How Does SRA Reporting Work?

Syslog information for SonicWALL remote appliances is sent to the Analyzer syslog collector and uploaded to the Reports Database by the summarizer. The frequency of upload is nearly real-time: data is uploaded to the Reports database as soon as the Syslog Collector closes the file. The file is closed and ready for upload as soon as it reaches 10,000 MB per file or if the file has been open for 3 minutes, whichever comes first.

This database is saved using a date/time suffix, and contains tables full of data for each appliance. All the syslog data received by SonicWALL Analyzer is available in the database.

SRA Reporting supports scheduled reports to be sent on a daily, weekly, or monthly basis to any specified email address.

Using and Configuring SRA Reporting

This section describes how to use and configure SRA reporting. See the following subsections:

Viewing Available SRA Report Types

To view the available types of reports for SRA Web Application Firewalls (WAF), perform the following steps:

1. Log into your Analyzer management console.
2. Click the **SRA** tab.

   The following types of reports are available:

   Global **Level Reports**:

   - Data Usage
     - Summary: connections per SRA appliance
   - WAF
     - Summary: connections listed by appliance for one day (default)
   - General
     - Status: number of units in the system and their Analyzer license status

   Unit Level Reports

   Clicking on hyperlinks in the Unit Level Reports takes you to the Analyzer Log, where you can view more information.

   - Data Usage
     - Timeline: total connections listed by hour
     - Users: connections listed by user
   - User Activity
     - Details: a detailed report of activity for the specified user
   - Access Method
     - Summary: connections per connection protocol (HTTPS, NetExtender, etc)
     - Users: top users by protocol
   - Authentication
     - User login: authenticated user logins by time and IP protocol. User Login reports combine admin users with all other users in the same report.
     - Failed login: Failed login attempts with initiator IP address.
   - WAF
     - Timeline: total threats detected per appliance
     - Threats Detected: top threats detected per day
     - Threats Prevented: top threats prevented per day
     - Apps Detected: top applications detected per day

- Apps Prevented: top applications blocked per day
- Users Detected: number of concurrent users per day
- Users Prevented: number of blocked users prevented per day

– Connections
- Timeline: a summary of offloaded connections under the group node per SRA appliance, listed for one day.
- Applications: offloaded connections by application
- Users: offloaded connections by user

– Analyzers
- Log Analyzer: logs of all activity

– Configuration: menus allow setting Report display options
- Log Analyzer Filter: applies filters to the system logs uploaded to the reporting database

– Events: these menus allow setting options
- Alert Settings: provides search functions, adding or removing Alerts
- Current Alerts: displays current applicable Alerts.Custom

Note You can use the Date Selector to select reports covering other intervals than those listed here.

Configuring SRA Scheduled Reports

SRA reports are scheduled through the Universal Scheduled Reports interface. Additionally, you can configure alerts and filter the syslog.

To configure SRA scheduled reports and summarization, click on the Schedule Report icon. The Universal Schedule Report menu comes up. For more information on scheduling and configuring reports, refer to the section on Universal Scheduled Reports.

Navigating Through Detailed SRA Reports

SRA reports display either summary or unit views, displayed in a Data Container. Information can be viewed in either chart (timeline or pie chart) form, or tabular (grid) format. The list of available reports allows you to navigate to a high-level or specific view. Data can be filtered by time constraints or data filters.

Drillable reports give access to additional information by clicking on hyperlinks to go to the Detail view. For some reports, you can go directly to the detail views by clicking **Details** in the Policies/Reports pane.

Data filtering can be applied either by using the Filter Bar, drilling down through hyperlinked data, or applying a filter to a drillable data column.

Viewing SRA Summary Reports

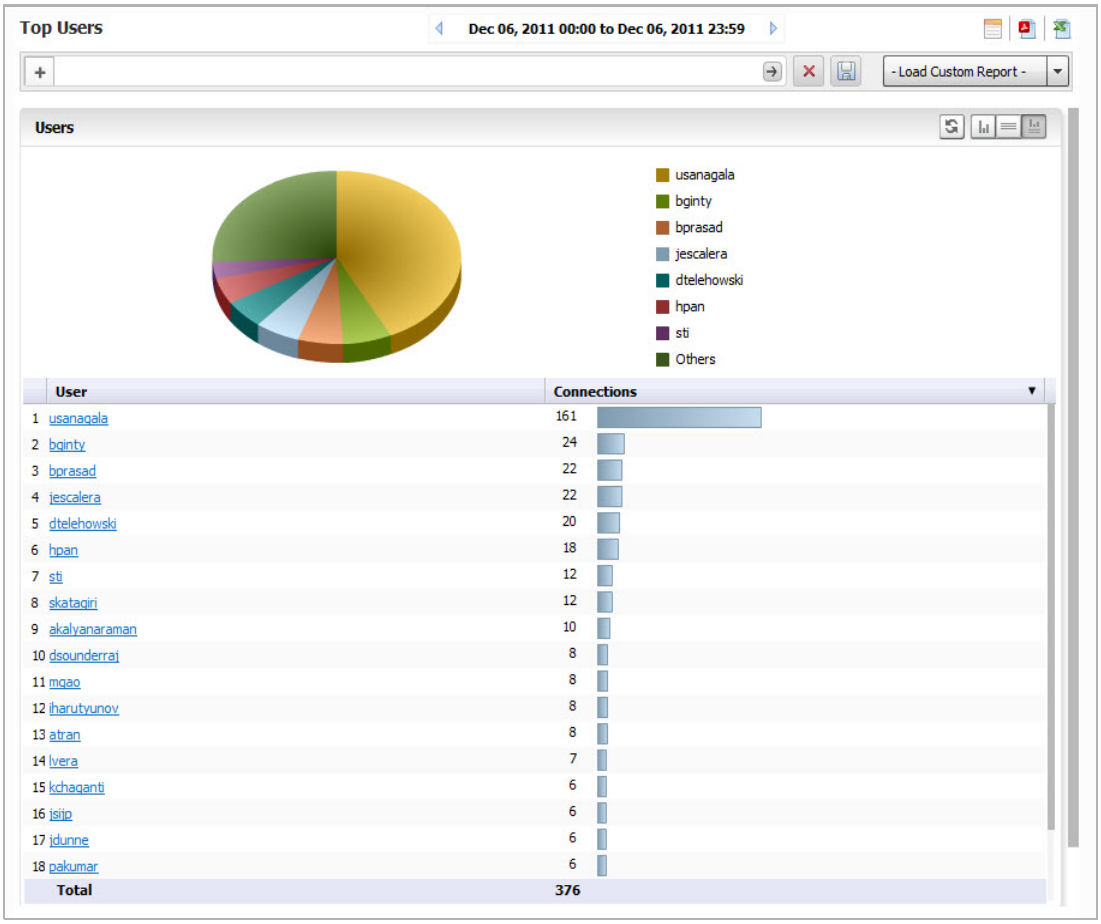
The SRA group level Summary report displays all SRA interfaces under that group level node, along with the total number of threats detected on the specified day.

The SRA Summary report is available for Data Usage, Web Application Firewall (WAF), and Connections. It shows the number of connections handled by the SRA appliances on the specified day or interval. The grid-level reports lists each appliance by name, along with the number of connections. To view the Data Usage Summary report, perform the following steps:

Step 1 Click the **SRA** tab.

Step 2 Select the global icon.

Step 3 Expand the **Data Usage, WAF, or Connections** tree and click **Summary**. The Summary page displays.



For more information, click on an individual appliance in the TreeControl menu. More settings, as well as more detailed information, is available at the Unit View level.

Viewing SRA Unit-Level Reports

Unit View reports provide detail about Data Usage, Access Method, Authentication, WAF Access, Connections, and Uptime and Downtime. You can also view the results from the Analyzers or saved Custom Reports.

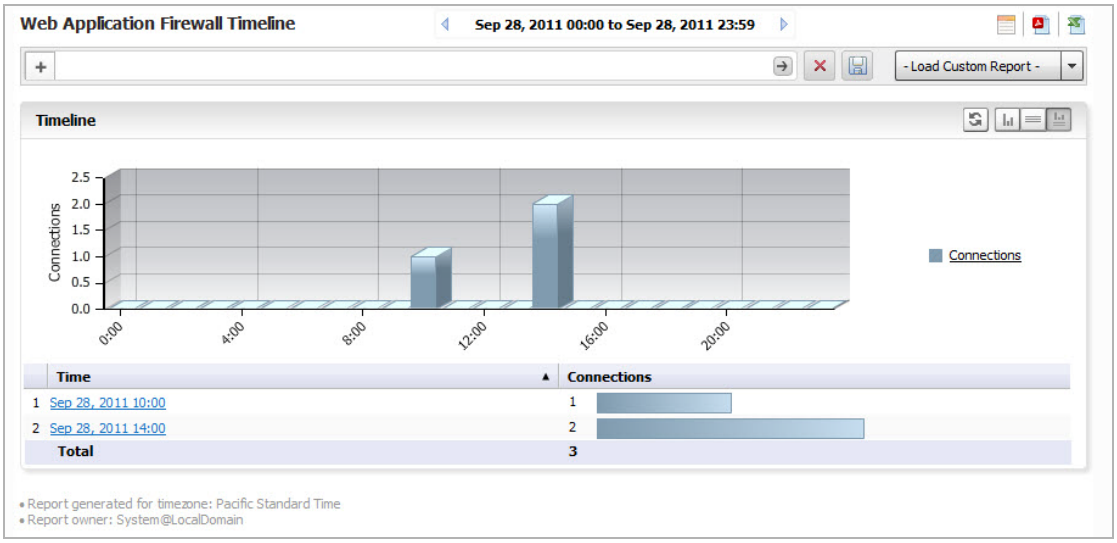
Viewing Unit-Level Data Usage Reports

Step 1 Click the **SRA** tab.

Step 2 Select the desired Unit.

Step 3 Expand the **Data Usage** entry and click **Timeline** to display the Report.

Step 4 The graph displays the number of connections to the selected SRA appliance during the desired interval. The current 24 hours is displayed by default.



The timeline contains the following information:

- **Hour**—when the sample was taken.
- **Connections**—number of connections to the SRA appliance

Step 5 To change the interval of the report, use the left arrow to click back a day at a time, or click on the **Time Bar** to access the Interval menu pull-down calendar.

Step 6 After selecting a date, click **Search.** The Analyzer 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 SRA Top Users Reports

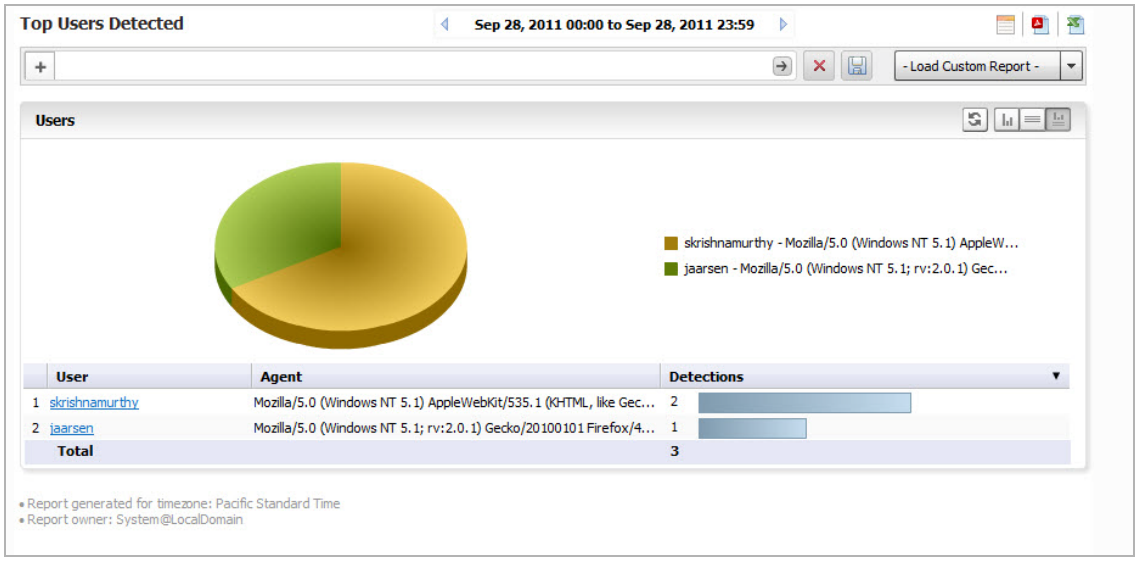
The Top Users report displays the users who used the most connections on the specified date.

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

Step 1 Click the **SRA** tab.

Step 2 Select the SRA appliance.

Step 3 Expand the **Data Usage** tree and click **Users**. The Top Users page displays.



Step 4 The pie chart displays the percentage of connections used by each user.

The table contains the following information for all users:

- **Users**—the user name
- **Connections**—number of connection events or “hits”

By default, the Analyzer 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 pull-down calendar.

Step 5 To display a limited number of users, use the Search Bar fields.

Note This report allows you to drill down by user. Clicking on a user in either the chart or grid view will take you to the Log Analyzer.

Viewing User Activity Logs

Web User Activity logs allow you to filter results to view only the activity of a specific use**r.**

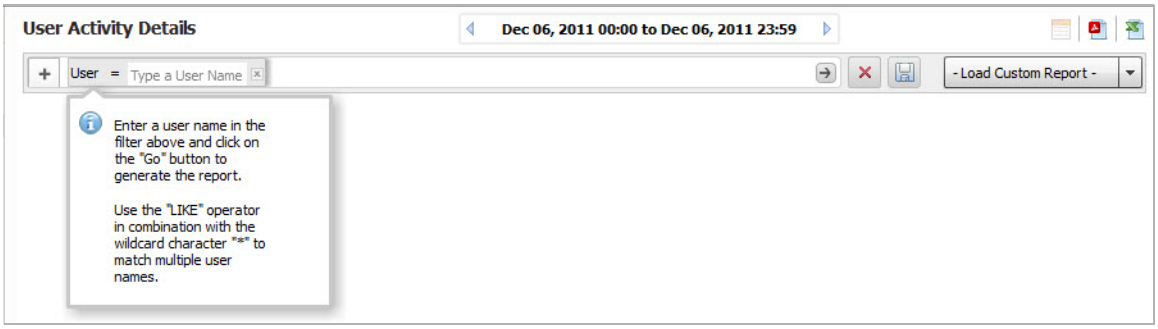
The User Activity Analyzer provides a detailed report listing activity filtered by user. If a user report has been saved previously, bringing up the User Activity Analyzer will display a list of saved reports under the Filter Bar.

If you wish to create a new report, use the Filter Bar to create a new report.

Step 1 Click the **Firewall** tab.

Step 2 Select a SonicWALL appliance.

Step 3 Click on **User Activity** > **Details** to bring up the **User Activity Analyzer**. The User Activity Analyzer generates a Detail report based on the user name.



If no user activity reports were saved, only the Filter Bar will display, with the User filter pre-selected. You can enter a specific user name, or use the LIKE operator wildcards (*) to match multiple names.

Step 4 Enter the name of the user into the field and click the Go (arrow) button to generate the report

The customized User Activity Details report will display a timeline of events, Initiators, Responders, Services, Applications, Sites visited, Blocked site access attempted, VPN access policy in use, user authentication, Intrusions, Initiator Countries, and Responder Countries associated with that particular user.

Data for a particular user may not be available for all of these categories.

Viewing Access Method Reports

Access Methods provide an overview of the protocols used to access the net. They are available as a summary pie chart or in a Top User report, both of which provide additional information on the access protocol of the specified user through the Log Analyzer.

Viewing the Access Summary Report

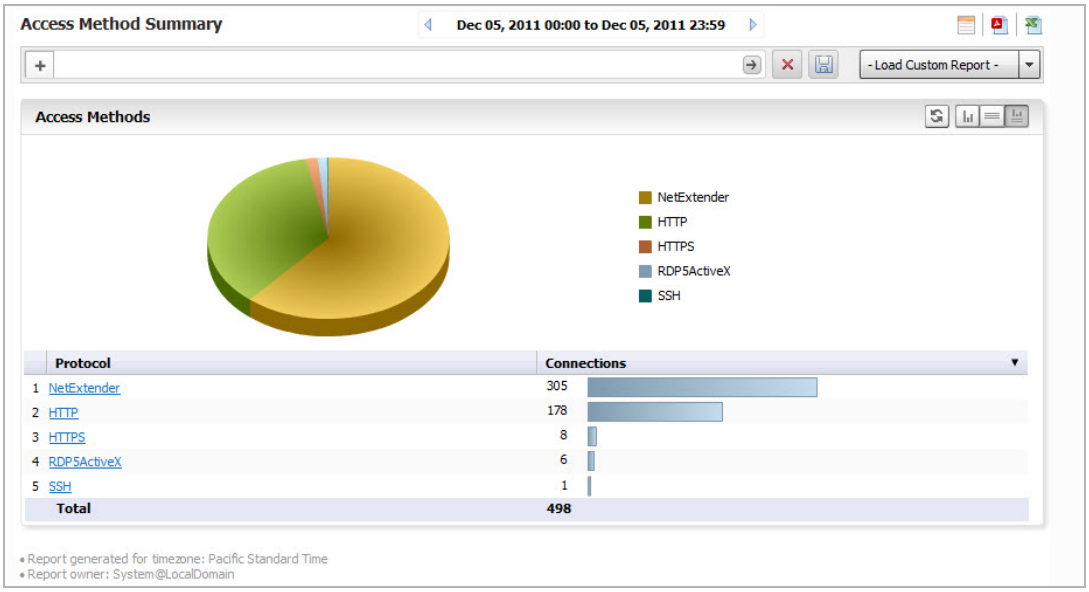
The Access Summary report provides an overview of the types of access protocols used. Clicking on a hyperlinked protocol entry will take you to the Log Analyzer view for more details.

To view the Summary Report:

Step 1 Click the **SRA** tab.

Step 2 Select a SRA appliance.

Step 3 Expand the **Access Method** tree and click **Summary**. The Access Method Summary page appears.



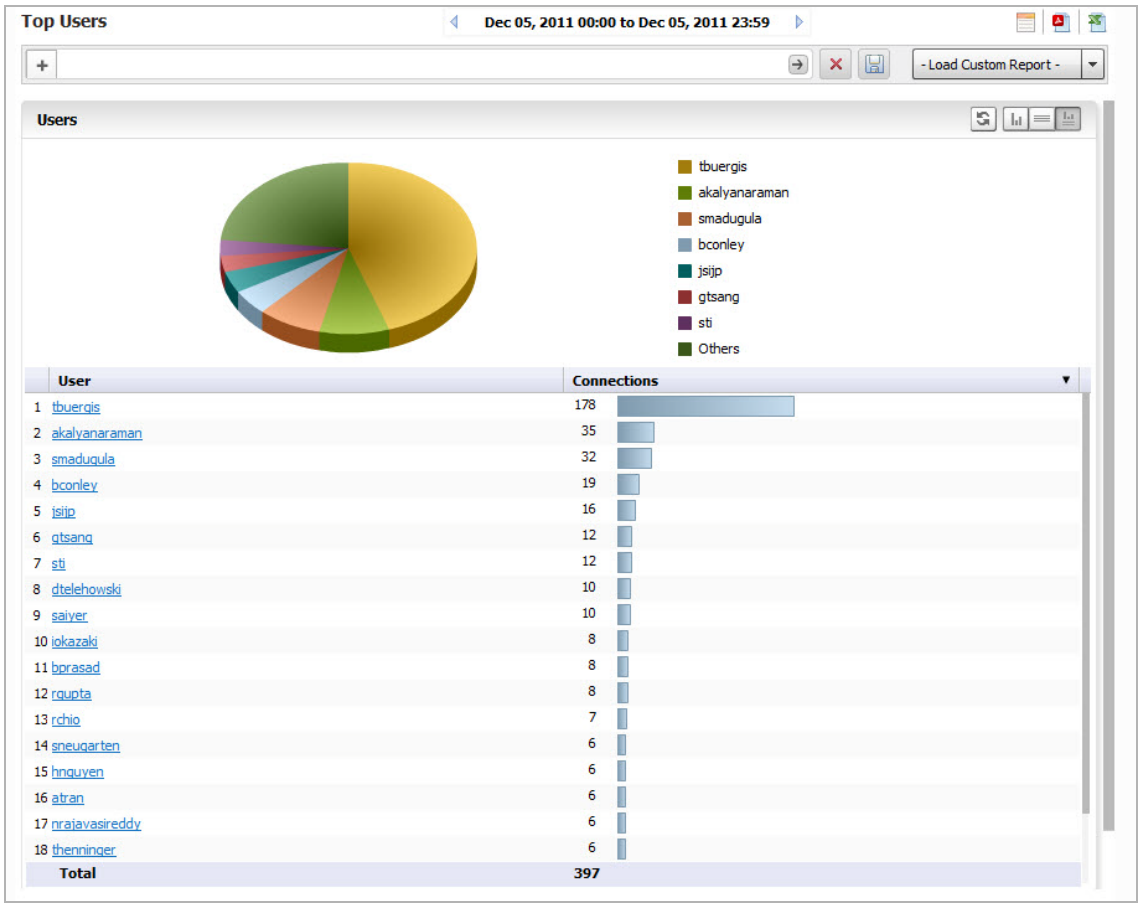
Step 4 Click on a section of the pie chart to obtain more details, or hover the mouse over an item on the Protocol column and right click **Add Filter** to narrow the results to a particular access protocol. The results will display in the Log Analyzer report.

Viewing the Top Users Access Report

Step 1 Click the **SRA** tab.

Step 2 Select a SRA appliance.

Step 3 Expand the **Access Method** tree and click **Users**. The Top Users report appears.



In the chart view, you can click on either the pie chart or user list to obtain more information from the Log Analyzer. Results will be filtered by user, and the setting added to the filter bar.

Alternatively, you can hover your mouse over a user in the User column of the grid view, then right click to filter results. For full details on that user, drill down by clicking on the user name in the column.

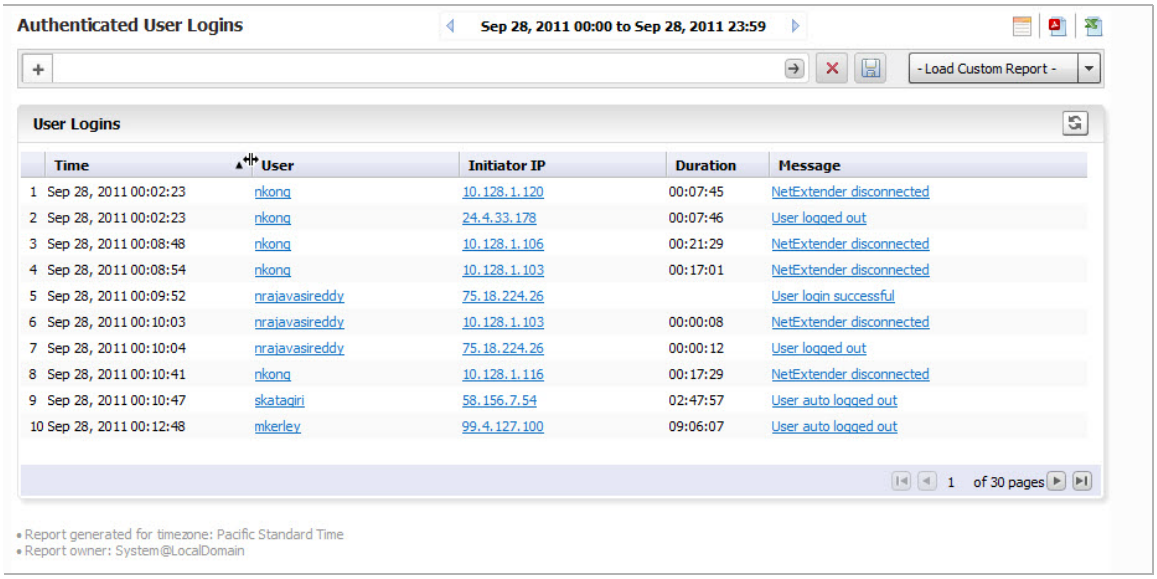
Viewing SRA Authentication User Login Report

The Authentication Summary report shows an overview of user logins and login attempts and disconnections by time, user, IP address, type of connection/disconnection, and amount of time the connection was established. Authentication reports are only available at the unit level.

Step 1 Click the **SRA** tab.

Step 2 Select a SRA appliance.

Step 3 Expand the **Authentication** tree and click **User Login**. The Authenticated User Login report appears.



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

The user login report shows the login for users that logged on to the SRA appliance during the specified day.

The Report contains the following information:

- **Time**—the time that the user logged in
- **User**—the user name
- **Initiator IP**—the IP address of the user's computer
- **Message**—the type of connection/disconnect
- **Duration**—the duration of the user login session

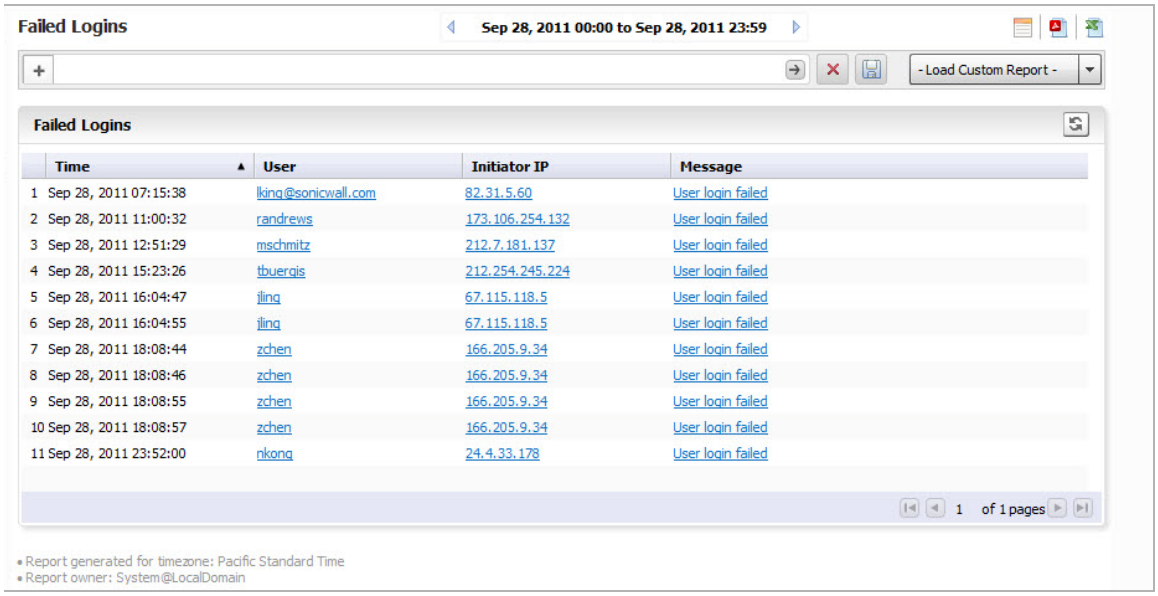
Viewing SRA Authentication Failed Login Report

The Authentication Failed Login report shows an overview of user logins and login attempts and disconnections by time, user, IP address, type of connection/disconnection, and amount of time the connection was established. Authentication reports are only available at the unit level.

Step 1 Click the **SRA** tab.

Step 2 Select a SRA appliance.

Step 3 Expand the **Authentication** tree and click **User Login**. The Authenticated User Login report appears.



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

The failed login report shows the login attempts for users that attempted to log on to the SRA appliance during the specified day.

The Report contains the following information:

- **Time**—the time that the user logged in
- **User**—the user name
- **Initiator IP**—the IP address of the user's computer
- Message—about the type of failed attempt

Viewing Web Application Firewall (WAF) Reports

The Web Application Firewall (WAF) Summary report contains information on the number of connections incurring Application Firewall activity logged by a SonicWALL appliance during each hour of the specified day, or at the global level, for all SonicWALL appliances for the day.

The Web Application Firewall provides the following Reports:

- Timeline
- Threats Detected
- Threats Prevented
- Apps Detected
- Apps Prevented
- Users Detected
- Users Prevented

Clicking on hyperlinks in these reports take you to the Log Analyzer view, for more details.

To view reports:

Step 1 Click on the SRA tab and either GlobalView for the group or by individual appliance in the TreeControl view on the left tab of the interface.

Step 2 Click **Reports** on the middle tab.

Step 3 Select the WAF entry to expand it and click on the Report you want to view.

Viewing Connections Timeline

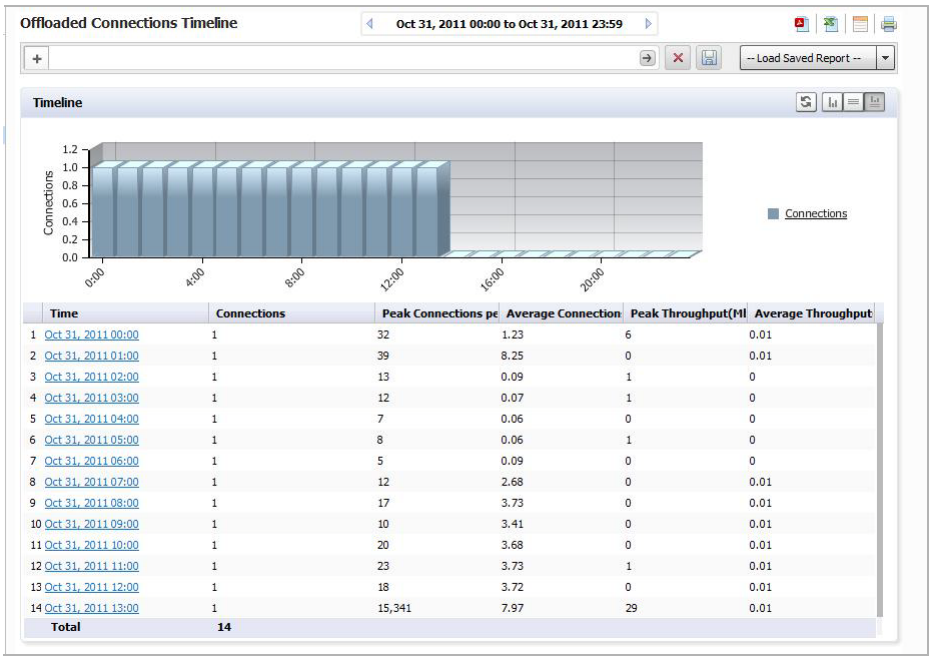
The WAF Connections timeline displays connections to the web firewall over time.To view the Web Application Firewall Summary report, perform the following steps:

Step 1 Click the **SRA** tab.

Step 2 Select a SonicWALL appliance.

Step 3 Click **Connections** > **Timeline**

The Timeline displays the unit level summary report containing Offloaded Connections information for an individual SRA system.



	Time	Connections	Peak Connections pe	Average Connection	Peak Throughput(Ml	Average Throughput
1	Oct 31, 2011 00:00	1	32	1.23	6	0.01
2	Oct 31, 2011 01:00	1	39	8.25	0	0.01
3	Oct 31, 2011 02:00	1	13	0.09	1	0
4	Oct 31, 2011 03:00	1	12	0.07	1	0
5	Oct 31, 2011 04:00	1	7	0.06	0	0
6	Oct 31, 2011 05:00	1	8	0.06	1	0
7	Oct 31, 2011 06:00	1	5	0.09	0	0
8	Oct 31, 2011 07:00	1	12	2.68	0	0.01
9	Oct 31, 2011 08:00	1	17	3.73	0	0.01
10	Oct 31, 2011 09:00	1	10	3.41	0	0.01
11	Oct 31, 2011 10:00	1	20	3.68	0	0.01
12	Oct 31, 2011 11:00	1	23	3.73	1	0.01
13	Oct 31, 2011 12:00	1	18	3.72	0	0.01
14	Oct 31, 2011 13:00	1	15,341	7.97	29	0.01
	Total	14				

Click on the hyperlinks available in this report to go to the Log Analyzer.

Viewing WAF Top Threats Detected

The Threats Detected report displays the threats detected, according to signature, classification, and severity. To view the Web Application Firewall Top Threats Detected report, perform the following steps:

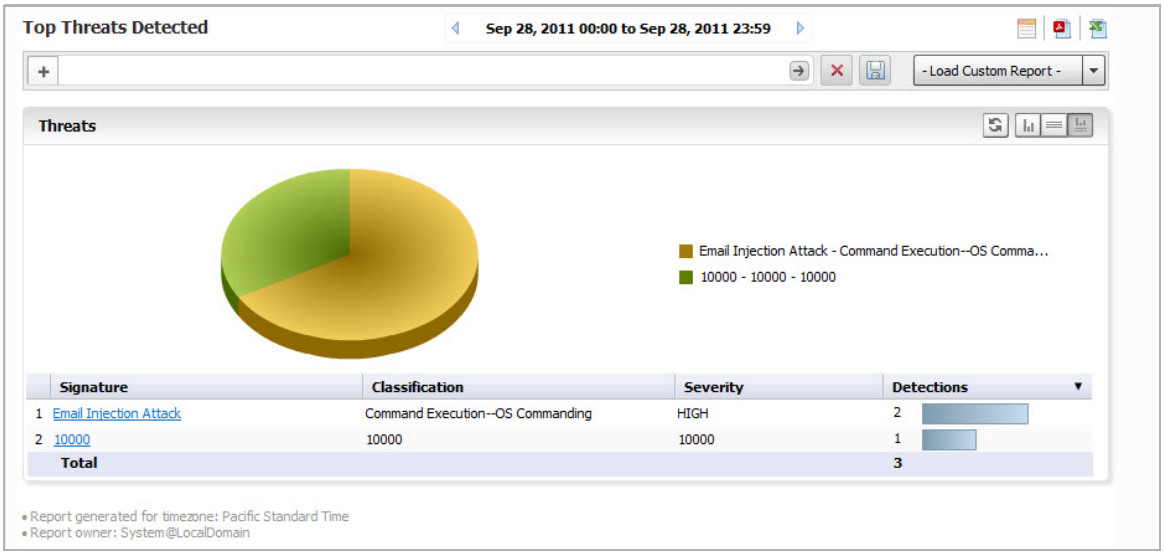
Step 1 Click the **SRA** tab.

Step 2 Select a SonicWALL appliance.

Step 3 Click on the **Reports** tab.

Step 4 Click **WAF** > **Threats Detected**.

The Top Threats Detected screen shows the top threats detected by the firewall, and gives details on the Threat Signature, Threat Classification, Threat Severity, in addition to total threats detected.



Click on the hyperlinks available in this report to go to the Log Analyzer.

Viewing WAF Top Threats Prevented

To view the Web Application Firewall Top Threats Prevented report, perform the following steps:

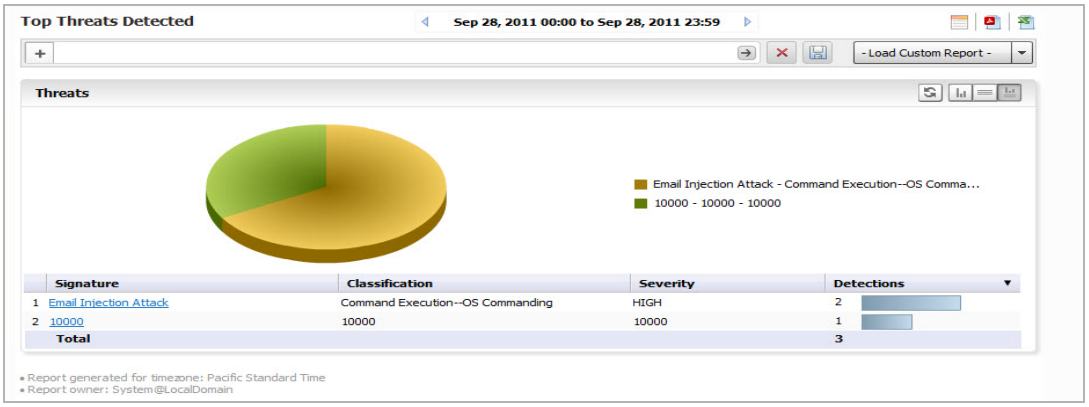
Step 1 Click the **SRA** tab.

Step 2 Select a SonicWALL appliance.

Step 3 Click on the **Reports** tab.

Step 4 Click **WAF** > **Threats Prevented**.

The Top Threats Prevented view shows Top Threats detected and prevented by the web firewall, with details on the Threat Signature, Threat Classification, Threat Severity, in addition to total threats detected.



Viewing WAF Top Applications Detected

To view the Web Application Firewall Top Applications Detected report, perform the following steps:

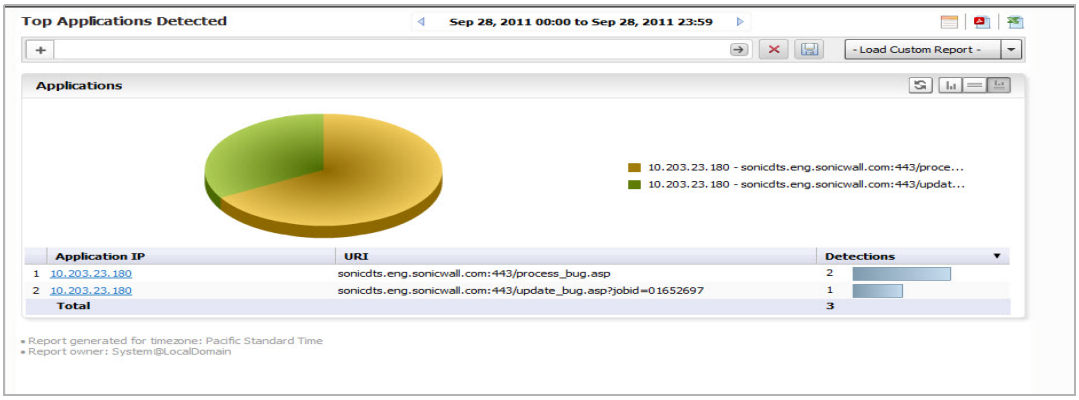
Step 1 Click the **SRA** tab.

Step 2 Select a SonicWALL appliance.

Step 3 Click on the **Reports** tab.

Step 4 Click **WAF** > **Applications Detected**.

The Top Applications Detected report will list applications with the most number of threats detected by the WAF process. It will display the Application IP, URI and the Detections in order of the number of detections.



Click on the hyperlinks available in this report to go to the Log Analyzer.

Viewing WAF Top Applications Prevented

To view the Web Application Firewall Top Applications Detected report, perform the following steps:

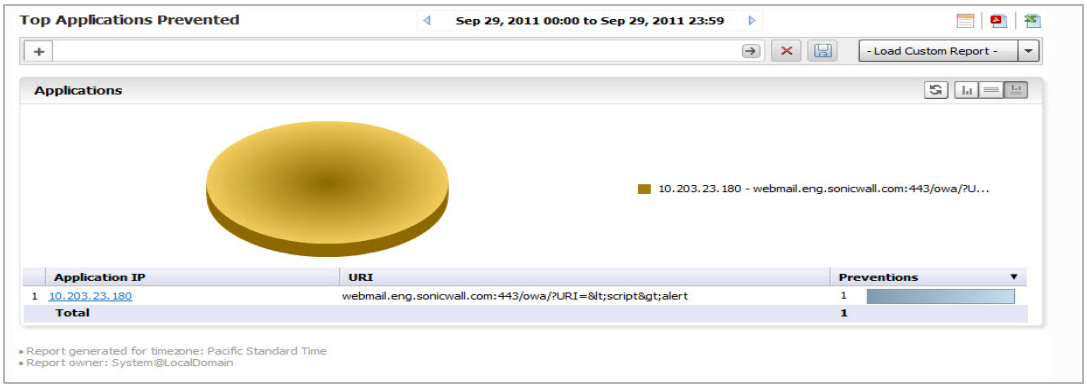
Step 1 Click the **SRA** tab.

Step 2 Select a SonicWALL appliance.

Step 3 Click on the **Reports** tab.

Step 4 Click **WAF** > **Applications Detected**.

The Top Applications Prevented report will list applications with the most number of threats prevented by the Web Application Firewall. It will display the Application IP, URI and the preventions in order of the number of threats prevented by the firewall



Click on the hyperlinks available in this report to go to the Log Analyzer.

Viewing WAF Top Users Detected

The Top Users Detected report will list the top authenticated users from whom threats have been detected by the Web firewall. It will display the User Name, User Agent and the Detections in order of the number of detections.

The Top Users report displays the users who made the most VPN connections on the specified date.

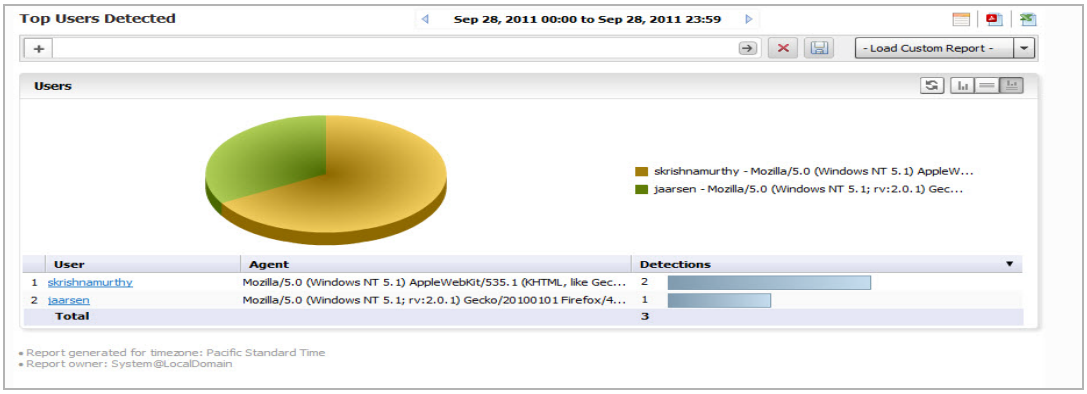
To view the Top Users report, perform the following steps:

Step 1 Click the **SRA** tab.

Step 2 Select a SonicWALL appliance.

Step 3 Click on the **Reports** tab.

Step 4 Click **WAF** > **Users Detected**. The Top Users page displays.



Step 5 The pie chart displays the VPN connections for the top VPN users.

Step 6 The table contains the following information by default:

- **Users**—the user's login. You can drill down to learn the IP address of the user.
- **Agent** - the User agent and version being used.

- **Detections**—the number of VPN connections in order of number of detections.
- **MBytes**—the number of megabytes transferred.

Step 7 By default, the Analyzer Reporting Module shows yesterday's report, a pie chart, and the ten top users. To change the date of the report, use the Search Bar and click the **Start** or **End** field to access the pull-down calendar, or click **More Options** for report display settings.

Viewing WAF Top Users Prevented

To view the Web Application Firewall Top Users Prevented report, perform the following steps:

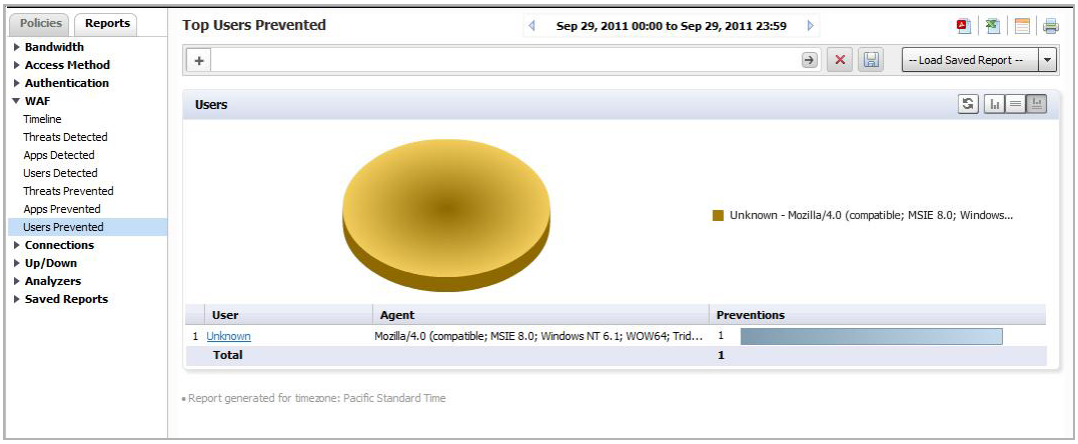
Step 1 Click the **SRA** tab.

Step 2 Select a SonicWALL appliance.

Step 3 Click on the **Reports** tab.

Step 4 Click **WAF** > **Users Prevented**.

The Top Users Prevented report lists the top authenticated users from whom threats have been prevented by the SonicWALL web firewall. It displays their user name, user agent, and preventions, in order of the number of preventions.



Click on the hyperlinks available in this report to go to the Log Analyzer.

Viewing Connection Reports

Connection reports show the number of connections, as well as throughput data, application and user data.

Viewing the Offloaded Connection Timeline

The Offloaded Connection Summary report lists the total connections made for all offloaded applications for one day, displayed per hour per day. The grid section displays peak connections per second, peak throughput, average connections per second, and average throughput per hour.

To view the Offloaded Connections Timeline report, perform the following steps:

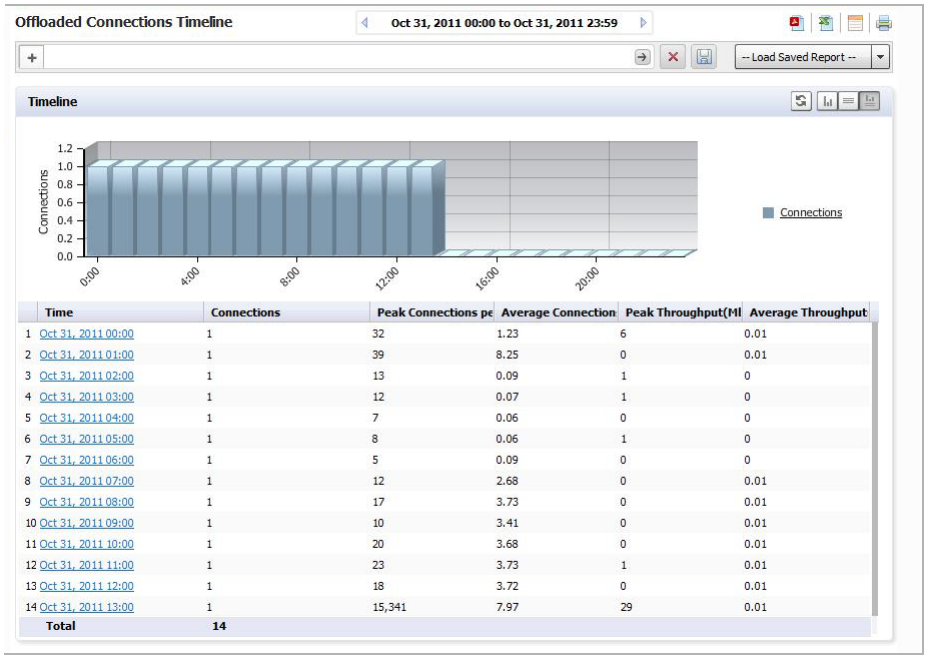
Step 1 Click the **SRA** tab.

Step 2 Select a SonicWALL appliance.

Step 3 Click on the **Reports** tab.

Step 4 Click **Connections** > **Timeline**.

The Offloaded Connections Summary report displays.



Viewing the Offloaded Connections Top Applications Report

The Top Applications report lists those applications having the most offloaded connections, as well as information about the application and throughput.

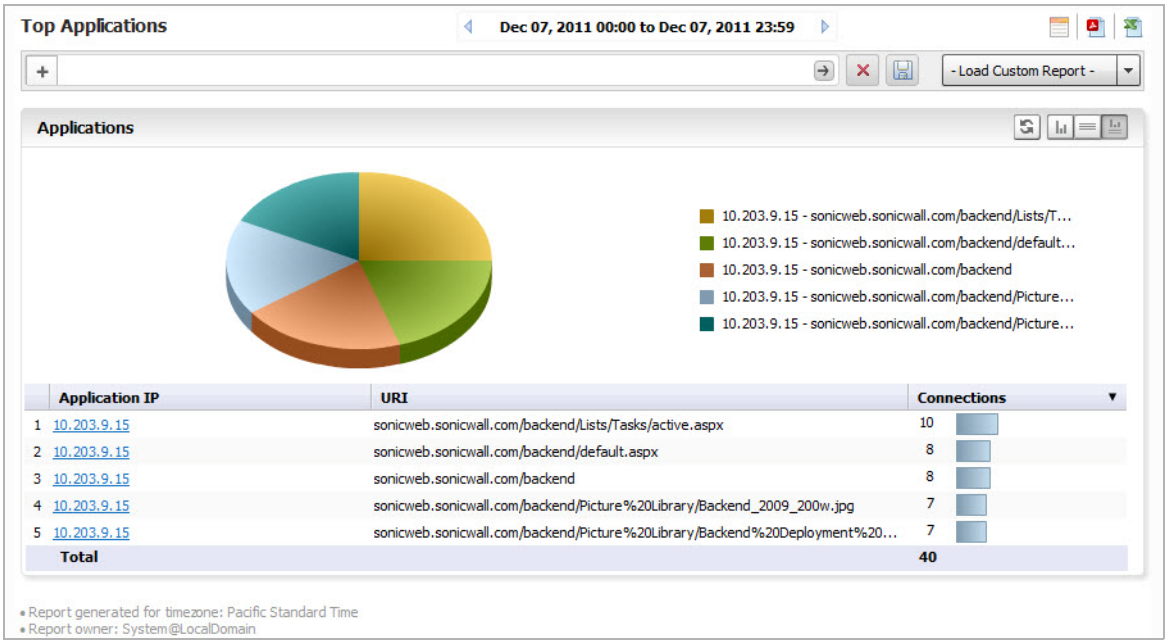
To view the report:

Step 1 Click the **SRA** tab.

Step 2 Select a SonicWALL appliance.

Step 3 Click on the **Reports** tab.

Step 4 Click **Connections** > **Applications**.



The report displays the IP address of the application, the URI, and how many connections were established. The report is drillable on the application IP address to obtain the Log Analyzer report.

Viewing the Offloaded Connections Top Users Report

The Top Users report lists the users who have the most offloaded connections It displays the User Name, User agent, and connections, in order of number of offloaded connections. The report will drill down to the Top Applications, filtered by User Name.

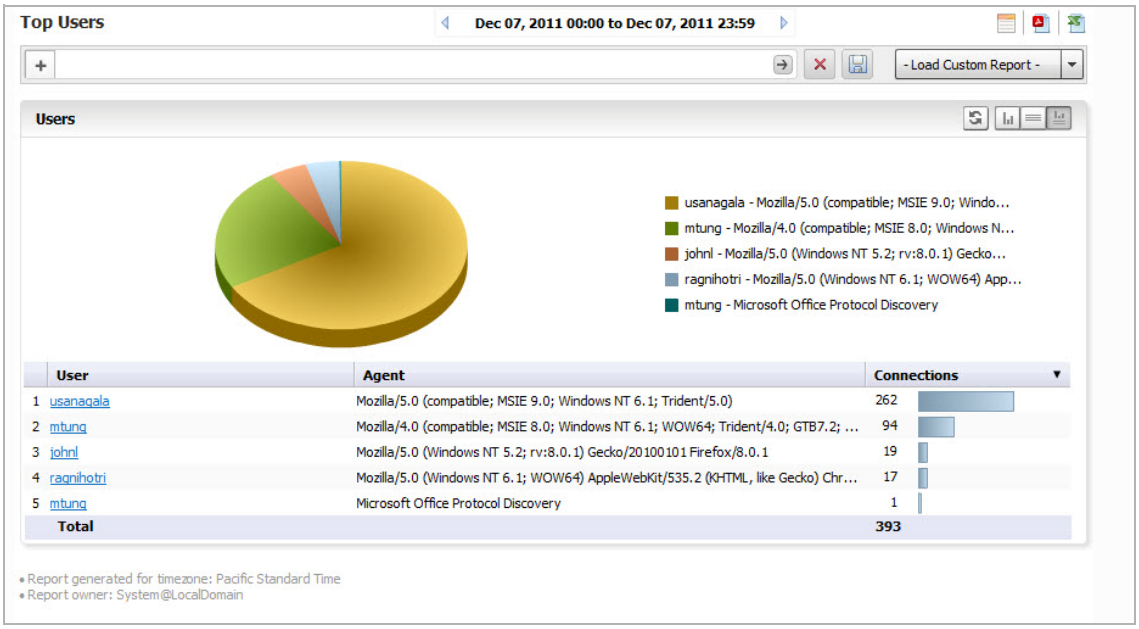
To view the report:

Step 1 Click the **SRA** tab.

Step 2 Select a SonicWALL appliance.

Step 3 Click on the **Reports** tab.

Step 4 Click **Connections** > **Users**.



The report will drill down to the Top Applications, filtered by User Name.

Viewing SRA Analyzer Logs

Analyzer logs contain detailed information from the system logs on each transaction that occurred on the SRA appliance.

The Log Analyzer allows advanced users to examine raw data for status and troubleshooting information. The Analyzer logs contain detailed information from the system logs on each transaction that occurred on the specified SonicWALL appliance. These logs can be filtered or drilled down to further narrow the focus of the information, allowing analysis of data about alerts, traffic, bandwidth consumption, etc. The Log Analyzer is only available at the individual unit level.

The SRA Log Analyzer contains information about Initiator and Responder IP addresses, Status Messages, User and Services used, as well as the time and duration of the session.

You can filter the log on IP address, Message, User, or Service.

Clicking hyperlinks on SRA Reports takes you the Analyzer Log view of the information. Log information can be saved by using the Save icon on the Filter Bar for a specific report. This report will then Appear in the list of Custom Reports.

For more information on the Log Analyzer, refer to “Using the Log Analyzer” section on page 126.

Saving System Log Reports

To load the report for later viewing, either:

- Click Load Custom Report and select from the pull-down list of saved Custom reports.
- Click on **Analyzers** > **Log Analyzer**

Note The Log Analyzer entries display 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 “**Configuring SRA Scheduled Reports**” on page 136 and Universal Scheduled Reports.

You can also click on the print icon to save a log to PDF of Excel format.

Note Saved system logs are limited in the number of rows that will be saved. If saving to PDF, a maximum of 2500 rows will be saved. If saving to Excel, a maximum of 10,000 rows will be saved.

Viewing the Analyzer Log for a SRA Appliance

To view the Log, perform the following steps:

Step 1 Click the **SRA** tab.

Step 2 Select a SRA appliance.

Step 3 Expand the **Analyzer** tree and click on Log Analyzer. The saved Log report page displays.

Syslog Exclusion Filter

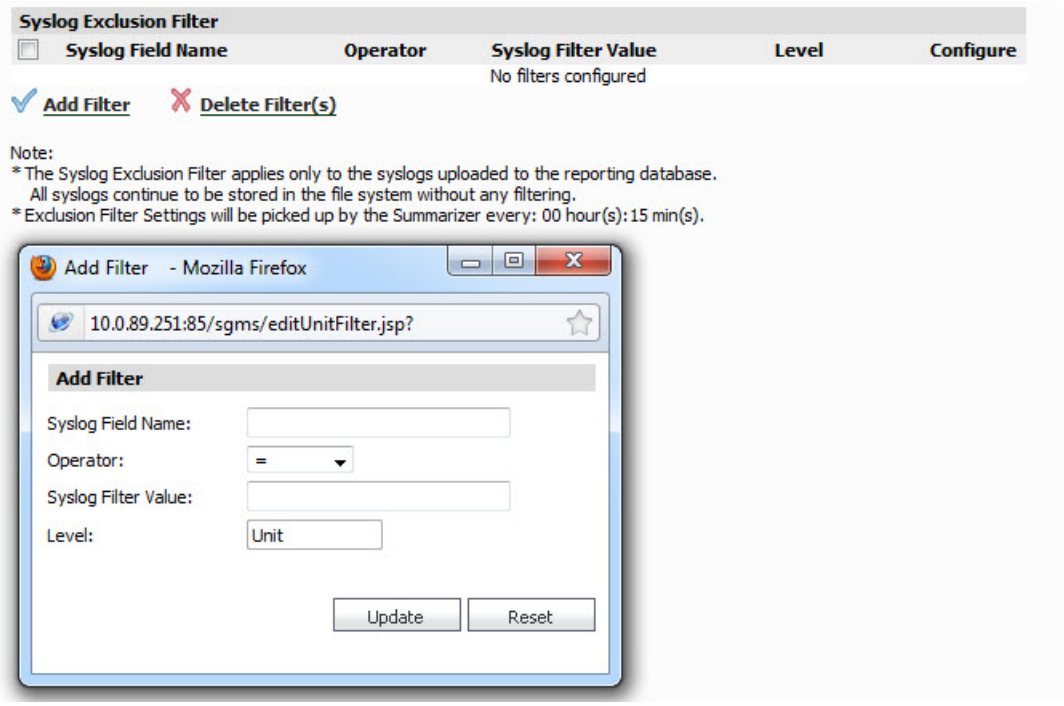
Filters allow you to fine-tune what information is displayed in Reports. Filters allow you to narrow search results and view subsets of report data.

Use this screen to manage the volume of syslog uploaded to the reporting database. The factory default filters are configured to upload only the syslog needed to generate the reports. This can be fine tuned further, but it required advanced knowledge of the syslog and consequently should be performed by experts only. Adding a wrong filter could lead to receiving a **Report Could Not Be Generated** message.

Step 1 To add a filter, click on **Configuration** > **Filters**.

The Syslog Exclusion Filter page comes up. This page allows you to view filters currently applied, add filters, or remove filters.

Step 2 To configure and add a filter, click **Add Filter**. The Add Filter menu comes up.



Step 3 Specify the field you want to modify, and select an operator and value. Click **Update**.

Custom Reports

You can configure a report with customized filters, then save it for later viewing and analysis. Saving a Report allows you to view it later, by loading it through the Custom Reports interface. Custom Reports can either be saved directly, or configured through the Universal Scheduled Reports. You can either load the report through the Custom Report pull-down on the Search Bar, or click **Reports** > **Custom** and choose from the list of saved Custom reports.

Custom Reports are available at the unit level for all appliances visible on the SRA tab. The Log Analyzer must be enabled for the appliance.

The Manage Reports screen (**Custom Reports** > **Manage Reports**) allows you to view what Custom Reports are available and delete reports from the system.

For more information on Custom Reports, refer to the “Custom Reports” section on page 132.

CHAPTER 8

Viewing CDP Reports

This chapter describes how to generate and view Continuous Data Protection (CDP) Reports on the SonicWALL Analyzer. CDP is a secure backup solution that runs continuously, backing up data from assigned agents, such as servers, laptops, and PCs.

This chapter contains the following sections:

CDP Reporting Overview

This section provides an introduction to the CDP reporting feature. This section contains the following subsections:

After reading the Analyzer CDP Reporting Overview section, you will understand the main steps to be taken in order to create and customize reports successfully.

For a general introduction to reporting, see the "Dell SonicWALL Analyzer Reporting Overview" section on page 85.

CDP Reports Tab

The CDP tab gives you access to the Continuous Data Protection (CDP) Reports section of the Dell SonicWALL Analyzer management interface. Reporting supports both graph and non-graph reports, and allows you to filter data according to what you wish to view. It supports multiple product-licensing models.

What is CDP Reporting?

Reports on SonicWALL Continuous Data Protection (CDP) appliances allows administrators to monitor online status and disk space usage, either globally within a network, or by appliance. CDP reporting also provides detailed backup reports for individual appliances.

The Filter Bar provides an intuitive, responsive interface for customizing the CDP report layout and configuring content filtering to focus on specific times and/or details. Hyperlinks allow access to additional reports data, by clicking on column entries to drill down to the desired detail view. By using these functions, you can:

- Track events to the minute or second of the day for forensics and troubleshooting

- Drill-down to find specific details
- Track appliance activity

How to View CDP Reports

To view the available types of reports for CDP, perform the following steps:

1. Log into your Dell SonicWALL Analyzer management console.
2. Click the **CDP** tab.

   The following types of reports are available:

   Global **Level Reports**:

   – Capacity
     - Summary: disk capacity listed by appliance for one day (default)

   Unit Level Reports

   – Backup Activity
     - Top Agents: total connections listed by hour
     - Top File Extensions: connections listed by user
     - Backup Details
     - User Backup Activity

Drilling down through the Group Level **Capacity Summary** report by appliance takes you to the Unit Level **Summary Report**. By drilling down through hypertext links in the Summary, you access the Detail-level reports.

Click **Backup Activity** > **Backup Details** to go directly to the Detail report.

For more information on how to navigate through the Reports, refer to “Navigating Dell SonicWALL Analyzer Reporting” on page 89.

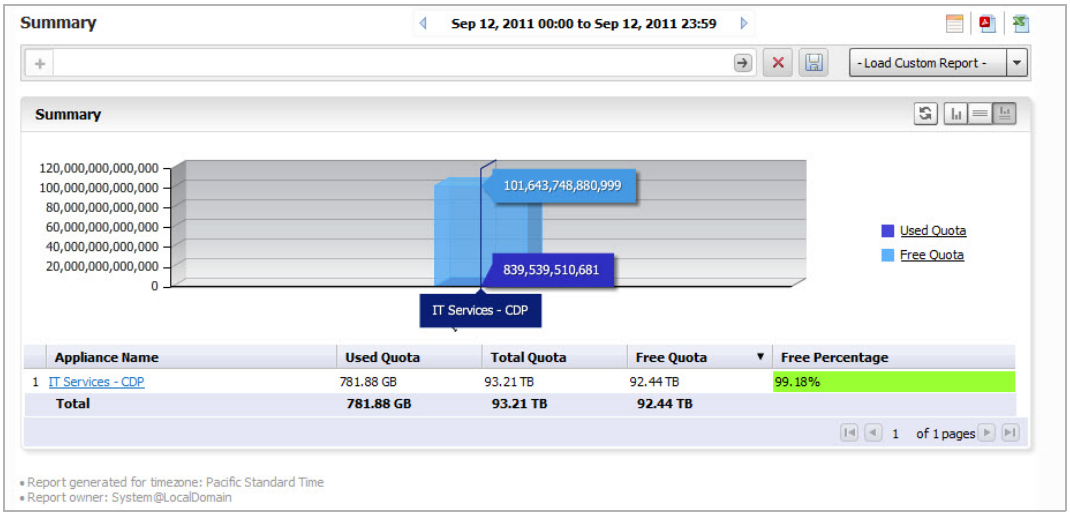
Viewing the Capacity Summary Report

The Capacity report provides an overview of disk usage, either for multiple devices via the Global View, or by individual unit, broken down by appliance or agent. Clicking on an appliance link in the global summary will take you to a Summary report for the agents of that appliance.

To view the Capacity report:

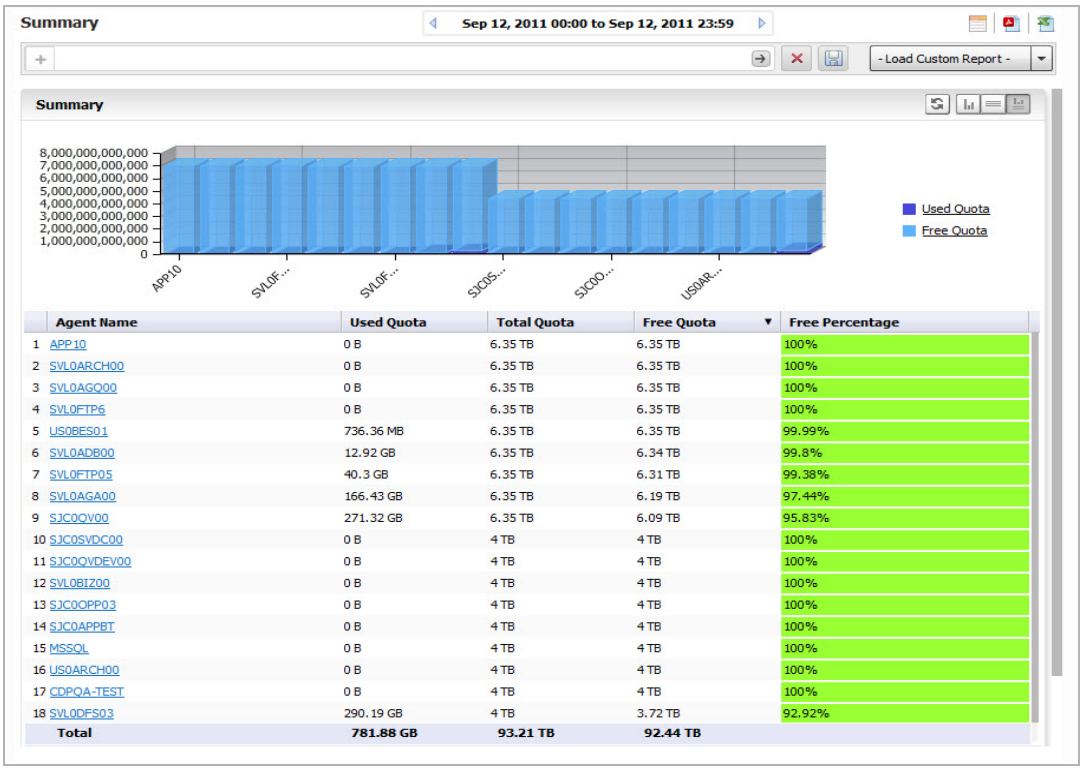
Step 1 Click the **CDP** tab.

The report includes the used and free quotas of the capacity for each appliance, as well as what percentage of that capacity is free.



Step 2 To view the Capacity Summary for an individual unit, click on the unit in the TreeControl panel.

A detailed view of the agents and quotas for the unit comes up.



	Agent Name	Used Quota	Total Quota	Free Quota	Free Percentage
1	APP10	0 B	6.35 TB	6.35 TB	100%
2	SVL0ARCH00	0 B	6.35 TB	6.35 TB	100%
3	SVL0AGQ00	0 B	6.35 TB	6.35 TB	100%
4	SVL0FTP6	0 B	6.35 TB	6.35 TB	100%
5	US0BES01	736.36 MB	6.35 TB	6.35 TB	99.99%
6	SVL0ADB00	12.92 GB	6.35 TB	6.34 TB	99.8%
7	SVL0FTP05	40.3 GB	6.35 TB	6.31 TB	99.38%
8	SVL0AGA00	166.43 GB	6.35 TB	6.19 TB	97.44%
9	SJC0QV00	271.32 GB	6.35 TB	6.09 TB	95.83%
10	SJC0SVDC00	0 B	4 TB	4 TB	100%
11	SJC0QVDEV00	0 B	4 TB	4 TB	100%
12	SVL0BIZ00	0 B	4 TB	4 TB	100%
13	SJC0OPP03	0 B	4 TB	4 TB	100%
14	SJC0APPBT	0 B	4 TB	4 TB	100%
15	MSSQL	0 B	4 TB	4 TB	100%
16	US0ARCH00	0 B	4 TB	4 TB	100%
17	CDPQA-TEST	0 B	4 TB	4 TB	100%
18	SVL0DFS03	290.19 GB	4 TB	3.72 TB	92.92%
	Total	**781.88 GB**	**93.21 TB**	**92.44 TB**	

Click the agent name to add a filter and obtain a Detail view of backup information.

Viewing Unit Backup Activity

You can view backups for Top Agents and Top File Extensions for a system. These files are drillable. You can also Click Backup Details to go directly to a Detail report.

Viewing the Top Agents Report

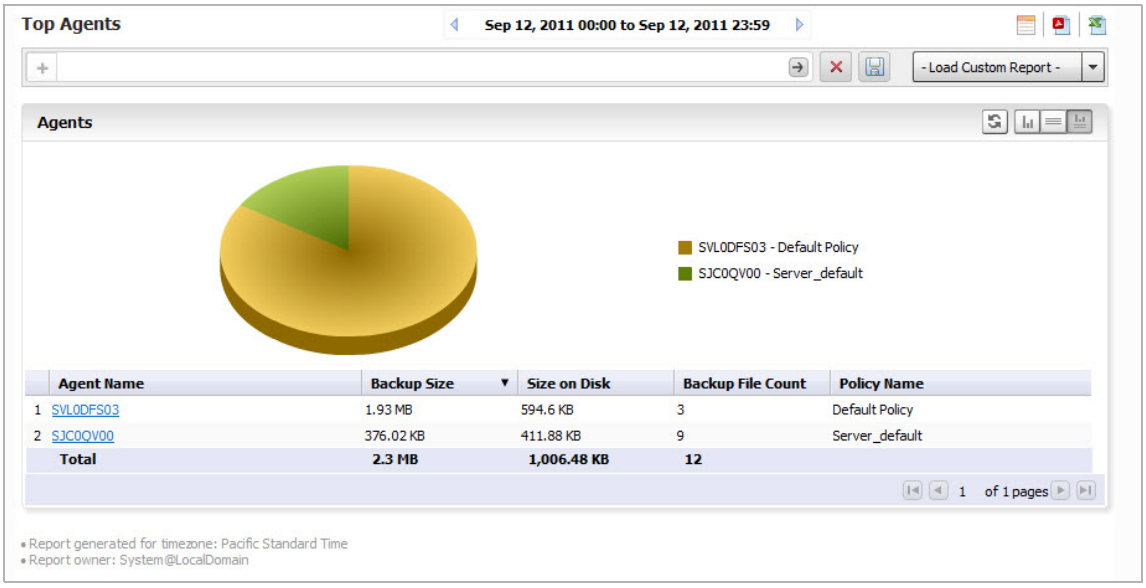
The Top Agents report lists the name of the agent, backup size, size of the compressed disk file in KB, and policy. The agents are displayed on a pie chart.

To view the Top Agents report, perform the following steps:

Step 1 Click the **CDP** tab.

Step 2 Click on the entry for the desired SonicwALL appliance.

Step 3 Click on **Backup Activity** > **Top Agents**.



Drilling down takes you to the Detail level report, listing the backed up appliance and listing its backed up files and folders. The Detail report also provides status on whether the backup operation was successful. You can shortcut to an unfiltered version of the Detail report by clicking **Backup Details**.

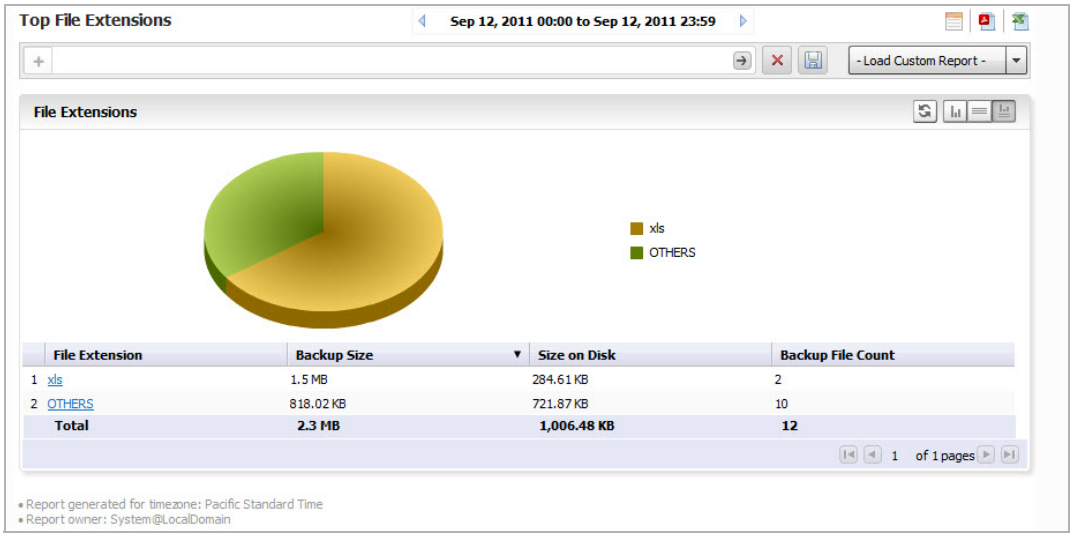
Top File Extensions

The Top File Extensions report lists the extension, backup size, size of the compressed disk file in KB, and number of backed up files.

Step 1 Click the **CDP** tab.

Step 2 Click on the entry for the desired SonicWALL appliance.

Step 3 Click on **Top File Extensions** on the Reports tab.



Drilling down takes you to the Detail level report, listing the backed up appliance and its files and folders

Viewing the Detail View Report

SonicWALL GMS provides a shortcut to the Detail view of CDP reports. The Detail view includes: what appliances were backed up and when, whether the operation was successful, the agent for the appliance, and the file and folder names backed up, with respective sizes of both original files and folders and backed up files and folders.

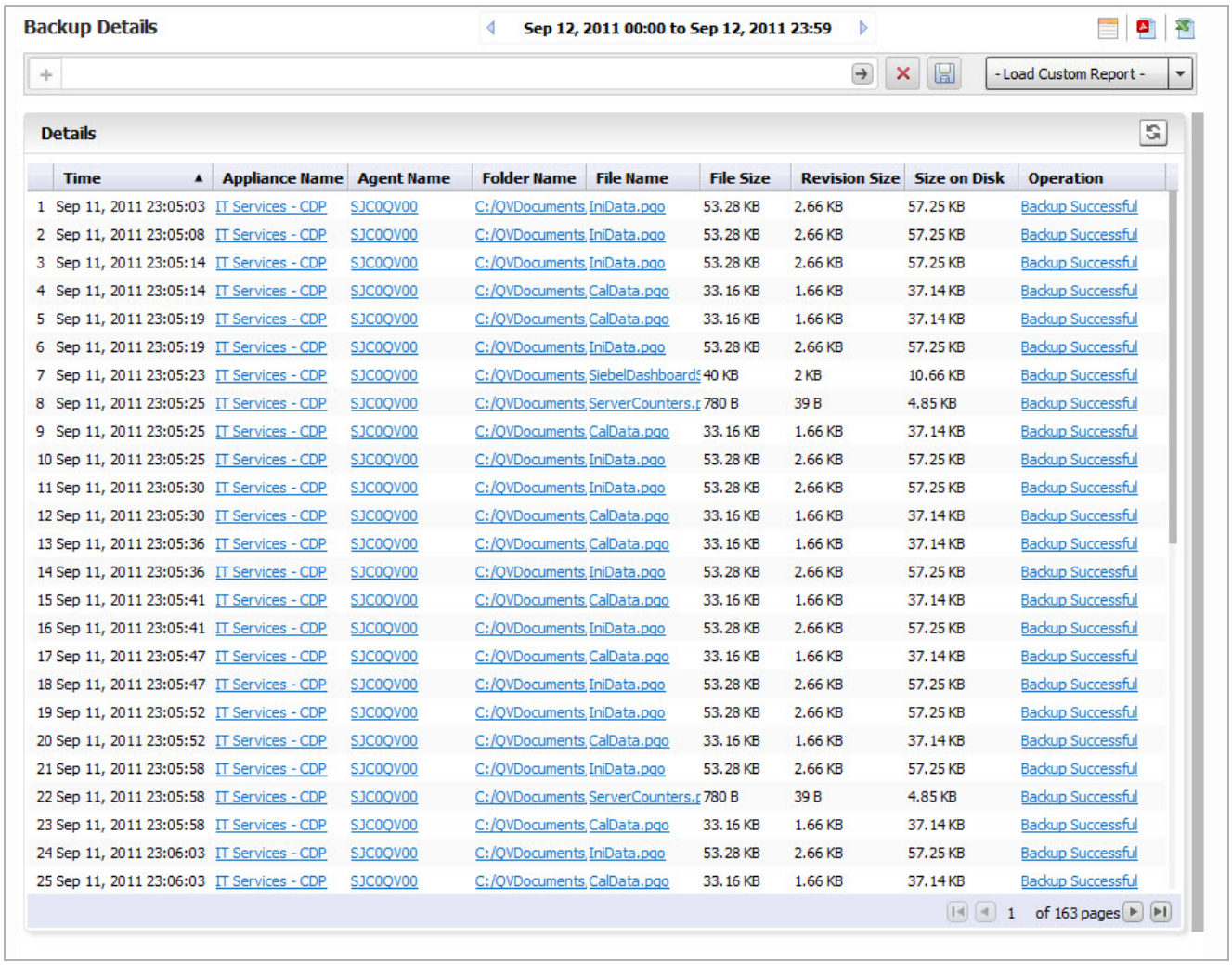
To see the Detail view:

Step 1 Click the **CDP** tab.

Step 2 Click on the entry for the desired SonicwALL appliance.

Step 3 Click on **Backup Details** on the Reports tab.

A detail view, similar to what you might see in the Log Analyzer, comes up. The CDP detail view is not organized into graph and grid view sections like the Firewall and SRA views. However, by clicking on links, you can filter results.



If desired, the Detail view of backup activity can be saved. It will then appear under Custom Reports, and in the Manage Reports list.

For more information on Custom reports, refer to "Custom Reports" section on page 109.

Viewing the User Backup Report

Viewing User Backup Reports takes you to the Detail view of the Backup report. The Detail view includes: what appliances were backed up and when, whether the operation was successful, the agent for the appliance, and the file and folder names backed up, with respective sizes of both original files and folders and backed up files and folders.

To see the Detail view:

Step 1 Click the **CDP** tab.

Step 2 Click on the entry for the desired SonicwALL appliance.

Step 3 Click on **Backup > User Backups** on the Reports tab.

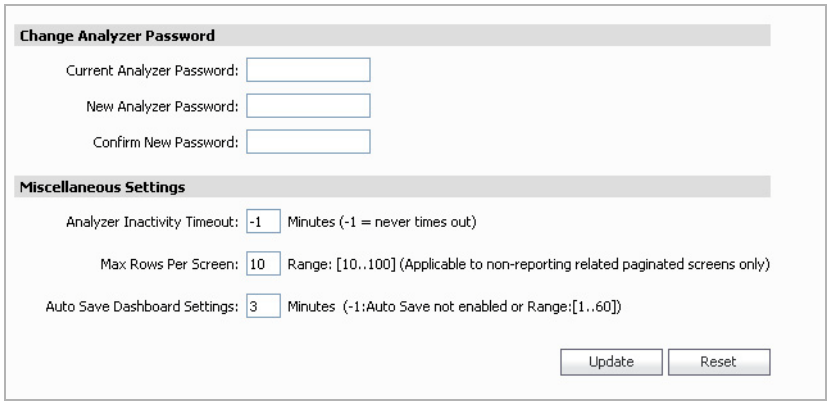
You can save the User Backup Report as a Custom report, for later viewing. For more information on Custom reports, refer to the “Custom Reports” section on page 109.

CHAPTER 9

Configuring User Settings

Configuring User Settings

This chapter describes how to configure the user settings that are available in the Console panel on the **User Settings > General** page, which provides a way to change the Analyzer administrator password, the Analyzer inactivity Timeout, and pagination settings.



Perform the following steps to configure the user settings that are available in the Console panel on the **User Settings > General** page:

Step 1 Enter the existing Dell SonicWALL Analyzer password in the **Current** Analyzer **Password** field.

Step 2 Enter the new Dell SonicWALL Analyzer password in the **New** Analyzer **Password** field.

Step 3 Reenter the new password in the **Confirm New Password** field.

Note Password fields will be grayed out for users on a Remote Domain.

Step 4 The Analyzer Inactivity Timeout period specifies how long Dell SonicWALL Analyzer waits before logging out an inactive user. To prevent someone from accessing the Dell SonicWALL Analyzer UI when Dell SonicWALL Analyzer users are away from their desks, enter an appropriate value in the Analyzer **Inactivity Timeout** field. You can disable automatic logout completely by entering a “-1” in this field. The minimum is 5 minutes and the maximum is 120 minutes.

Step 5 Select a value between 10 and 100 in the **Max Rows Per Screen** field. This value applies only to non-reporting related paginated screens.

Step 6 When you are finished, click **Update**. The settings are changed. To clear all screen settings and start over, click **Reset**.

Note The maximum size of the Dell SonicWALL Analyzer User ID is 24 alphanumeric characters. The password is one-way hashed and any password of any length can be hashed into a fixed 32 character long internal password.

CHAPTER 10

Configuring Log Settings

This section describes how to configure Log Settings. This includes adjusting settings on deleting log messages after a certain period of time, and setting criteria for viewing logs.

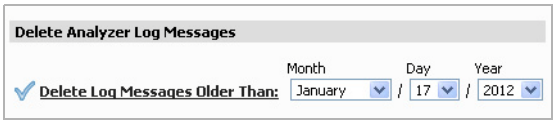
This chapter includes the following sections:

Configuring Log Settings

The Log > Configuration screen provides a way to delete log messages older than a specific date.

To delete Analyzer log messages, perform the following steps:

1. Click the **Console** tab, expand the **Log** tree, and click **Configuration**. The Configuration page displays.

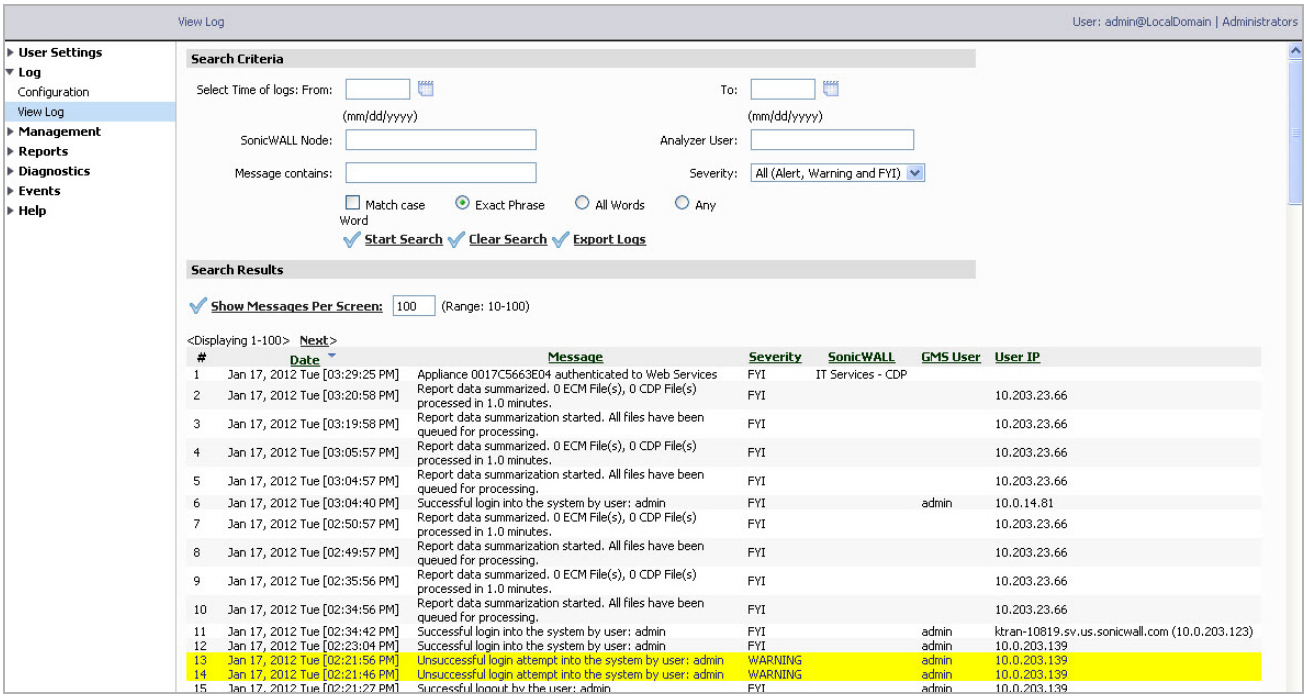


2. Select the month, day, and year from the drop down menu.
3. Click **Delete Log Messages Older Than**.

Configuring Log View Search Criteria

The Dell SonicWALL Analyzer log keeps track of changes made within the Dell SonicWALL Analyzer UI, logins, failed logins, logouts, password changes, scheduled tasks, failed tasks, completed tasks, raw syslog database size, syslog message uploads, and time spent summarizing syslog data. To view the Dell SonicWALL Analyzer log, perform the following steps:

1. Click the Console tab, expand the Log tree, and click **View Log**. The View Log page displays.



2. Each log entry contains the following fields:
   - #—specifies the number of the log entry.
   - **Date**—specifies the date of the log entry.
   - **Message**—contains a description of the event.
   - **Severity**—displays the severity of the event (Alert, Warning, or FYI).
   - **SonicWALL**—specifies the name of the SonicWALL appliance that generated the event (if applicable).
   - **User@IP**—specifies the user name and IP address.
3. To narrow the search, configure some of the following criteria:

Tip You can press Enter to navigate from one form element to the next in this section.

   - **Select Time of logs**—displays all log entries for a specified range of dates.
   - **SonicWALL Node**—displays all log entries associated with the specified SonicWALL appliance.
   - Analyzer **User**—displays all log entries with the specified user.

- **Message contains**—displays all log entries that contain the specified text. This input field provides an auto-suggest functionality that uses existing log message text to predict what you want to type. It fills in the field with the suggested text and you can either press **Tab** to accept it or keep typing. Different suggestions will appear as you continue to type if log messages match your input.
- **Severity**—displays log entries with the matching severity level:
  - All (Alert, Warning, and FYI)–where FYI mean “For Your Information”
  - Alert and Warning
  - Alert
- Select the **Match case** checkbox to make the **SonicWALL Node**, Analyzer **User**, and **Message contains** search fields case sensitive.
- Select one of **Exact Phrase**, **All Words**, or **Any Word**.
  - **Exact Phrase** matches a log entry that contains exactly what you typed in the **Message contains** field
  - **All Words** matches a log entry that contains all the words you typed in the **Message contains** field, but the words can be non-consecutive or in any order
  - **Any Word** matches a log entry that contains any of the words you typed in the **Message contains** field

4. To view the results of your search criteria, click **Start Search**. To clear all values from the input fields and start over, click **Clear Search**. To save the results as an HTML file on your system, click **Export Logs** and follow the on-screen instructions.
5. To configure how many messages are shown per screen, enter a new value between 10 and 100 in the **Show Messages Per Screen** field. (default: 10). Click **Next** to display the next page, or click **Previous** to display the preceding page.

CHAPTER 11

Configuring Console Management Settings

This chapter describes the settings available on the Console panel in the Management section. The following sections are found in this chapter:

Configuring Management Settings

On the Console > Management >Settings page, you canconfigure email settings, set the system debug level, synchronize model codes information, and configure password security settings.

This section describes the following Settings topics:

Configuring Email Settings

An SMTP server and an email address are required for sending Analyzer reports.

If the Mail Server settings are not configured correctly, you will not receive important email notifications, such as:

- System alerts for your Dell SonicWALL Analyzer deployment performance
- Availability of product updates, hot fixes, or patches
- Scheduled Reports

To configure these email settings:

Step 1 Click the **Console** tab.

Step 2 Expand the **Management** tree and click **Settings**. The Settings page displays.

Step 3 Type the IP address of the Simple Mail Transfer Protocol (SMTP) server into the **SMTP Server** field. This server can be the same one that is normally used for email in your network. Type in the SMTP Port number to use for email service.

Step 4 Enter the email account name and domain that will appear in messages sent from the Dell SonicWALL Analyzer into the Analyzer **Sender e-Mail Address** field.

Step 5 Enter the email account name and domain that will appear in messages sent from the Dell SonicWALL Analyzer into the Analyzer **Administrator e-Mail Address** field. You can use User Authentication for this user by checking the box.

Step 6 When finished in the Settings page, click **Update**. To clear the screen settings and start over, click **Reset**.

Configuring System Debug Level

Dell SonicWALL Analyzer provides the **System Debug level** option to control the debug messages sent to the log file.

To configure this setting:

1. Select a debug level from the **System Debug level** drop-down list. The range is 0-3 where a level of 0 provides no debug log messages and a level of 3 provides the maximum number of debug messages.
2. When finished in the Settings page, click **Update**. To clear the screen settings and start over, click **Reset**.

Enforcing Password Security

Dell SonicWALL Analyzer supports enforced password rotation for enhanced security compliance.

To enable and configure enforced password rotation:

1. Select the **Enforce Password Security** checkbox.
2. In the **Number of days to force password change** field, enter a value. The default is 90. Dell SonicWALL Analyzer will prompt the administrator to change the admin account password after the specified number of days.
3. When finished in the Settings page, click **Update**. To clear the screen settings and start over, click **Reset**.

Show Legacy (pre Analyzer 7.1) Reports

After the upgrade to Analyzer 7.1 new reports can only be generated using the new Analyzer reporting infrastructure. Old Viewpoint reports can be viewed under legacy reports session (it is not possible to view both 7.1 and pre-7.1 reports in the same session). Reports generated by pre 7.1 releases of SonicWALL Analyzer are still available for viewing. Analyzer 7.1 Reporting is not compatible with earlier versions, but reports generated by earlier versions are still accessible under the Analyzer reporting Infrastructure.

To view legacy reports, perform the following steps:

Step 1 Select the Show Legacy (pre Analyzer 7.1) Reports checkbox.

Step 2 Log out of SonicWALL Analyzer.

Step 3 Log back into SonicWALL Analyzer using administrator credentials.

Synchronizing Model Codes

The Sync Model Codes feature accommodates new SonicWALL product introductions without the need for Analyzer update. When SonicWALL updates the the corporate server (MySonicWALL) with a new product code, it then becomes available to Analyzer. The task is scheduled to run every 24 hours and is also available manually.

To synchronize model codes immediately:

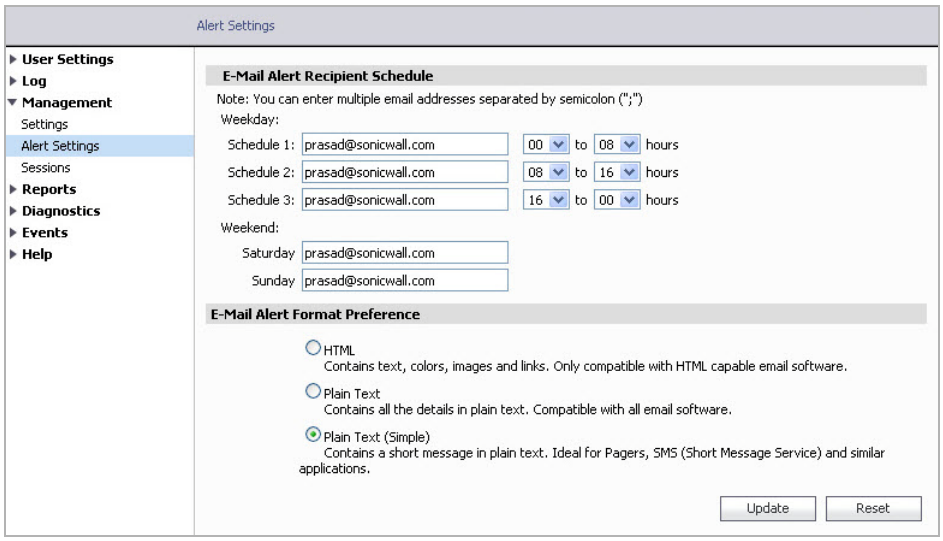
1. On the Console > Management > Settings page, click **Sync Model Codes information now**.
2. A short time later the page is updated to display the synchronization status at the top.

Configuring Management Alert Settings

The Alert Settings page specifies which email addresses receive email alerts and notifications during specific times.

To configure the alert notification settings, perform the following steps:

1. Click the **Console** tab, expand the **Management** tree and click **Alert Settings**. The Alert Settings page displays.



2. Configure the email address(es) that will receive notifications and the times that they will receive them:
   - **Schedule 1**—Specifies who will receive notifications during the first weekday schedule. Enter one or more email addresses (separated by commas) and specify the start and end time for the shift.
   - **Schedule 2**—Specifies who will receive notifications during the second weekday schedule. Enter one or more email addresses (separated by commas) and specify the start and end time for the shift.
   - **Schedule 3**—Specifies who will receive notifications during the third weekday schedule. Enter one or more email addresses (separated by commas) and specify the start and end time for the shift.
   - **Saturday**—Specifies who will receive notifications on Saturday. Enter one or more email addresses (separated by commas) and specify the start and end time for the shift.
   - **Sunday**—Specifies who will receive notifications on Sunday. Enter one or more email addresses (separated by commas) and specify the start and end time for the shift.
3. Select whether the email alert will be sent as **HTML**, **Plain Text**, or **Plain Text (Pager**). The Pager setting sends a very short email to ensure that the email is not cut off by the character limits of some pagers.
4. When you are finished, click **Update**. The settings are saved.

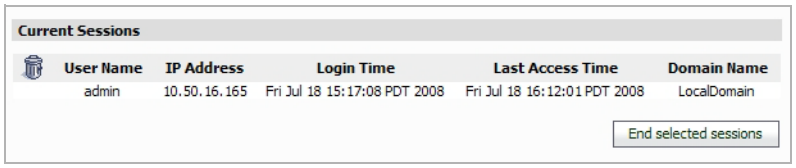
Configuring Management Sessions

The Sessions page of the Management section of the Analyzer Console allows you to view session statistics for currently logged in Analyzer users and to end selected sessions.

Managing Sessions

On occasion, it may be necessary to log off other user sessions. To do this, perform the following steps:

1. Click the **Console** tab, expand the **Management** tree and click **Sessions**. The Sessions page displays.



2. When more than one session is active, a checkbox is displayed next to each row. Select the check box of each user to log off and click **End selected sessions**.

   The selected users are logged off.

CHAPTER 12

Managing Reports in the Console Panel

This section describes how to configure reporting settings on the Console panel. These include how often the summary information is updated, the number of days that summary information is stored, and the number of days that raw data is stored.

The following sections are included in this chapter:

Summarizer

This section contains the following subsections:

About Summary Data in Reports

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

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

Additionally, you can select the number of days that raw syslog data is stored. The raw data is made up of information for every connection. Depending on the amount of traffic, this can quickly consume an enormous amount of space in the database. Analyzer creates a new 2 GB database for raw syslog data everyday. Be very careful when selecting how much raw information to store.

Summarizer Settings and Summarization Interval for CDP

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

See the following sections:

- "Setting the Reports Data Summarization Interval" section on page 178
- "Using Summarize Now" section on page 180

Enabling Report Summarization for CDP Appliances

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

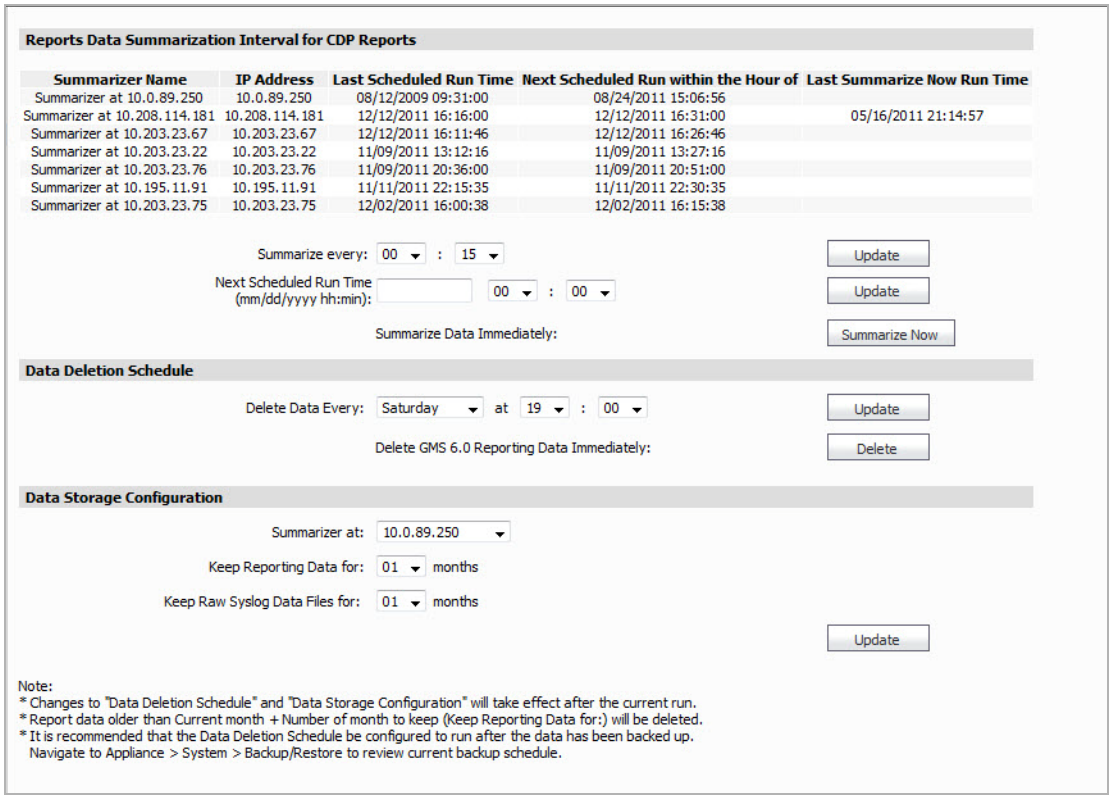
1. On the **Console** panel, navigate to **Reports > Summarizer**.
2. Under **Summarizer Settings**, select the **Enable Report Summarization** checkbox.
3. Click **Update**.

Setting the Reports Data Summarization Interval

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

To configure the summarization interval, perform the following steps:

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



2. Under Reports Data Summarization Interval, important information about the Summarizer is displayed. Use the **Summarize every** pull-down lists to specify how often in hours and minutes the Analyzer Reporting Module should process syslog data and update summary information.

3. Click the **Update** button to the right of this field.
4. To specify the next summarization time, enter a date in the form mm/dd/yyyy in the **Next Scheduled Run Time** field, and select the hour and minute values from the pull-down lists.
5. Click the **Update** button to the right of this field.
6. To update the summary information now, click the **Summarize Now** button. Dell SonicWALL Analyzer will automatically process the latest information and make it available for immediate viewing.

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

For more information about using and verifying the Summarize Now option, see the "Using Summarize Now" section on page 180.

Using Summarize Now

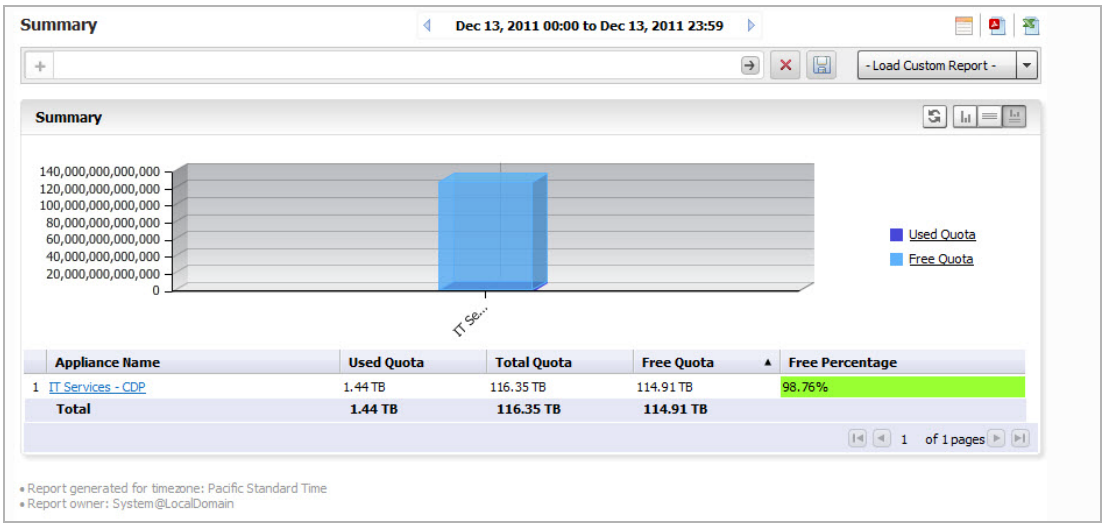
The Summarize Now feature allows the administrator to create instant summary reports without affecting the regularly scheduled summary reports. You can use Summarize Now to test that the Summarizer is gathering data for a managed unit. The SonicWALL Analyzer Summarize Now feature is located in the **Console**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

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

1. Click the **Console** tab, expand the **Reports** tree and click **Summarizer**. Click the **Summarize Now** button to summarize data immediately.
2. You will see a pop-up window verifying that you want to summarize the data now. Summarizing data using **Summarize Now** is a one-time action and will not affect the scheduled summary. Click **OK** to continue.
3. To verify summarization, navigate to **Log > View Log** in the left pane. Search for the message **Report Data Summarized** to verify that the Summarize Now action has completed.
4. When Summarize Now has completed, click the Firewall tab at the top of the screen. In the left-most pane, click GlobalView or click an appliance.

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

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



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

Configuring the Data Deletion Schedule Settings

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

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

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

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

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

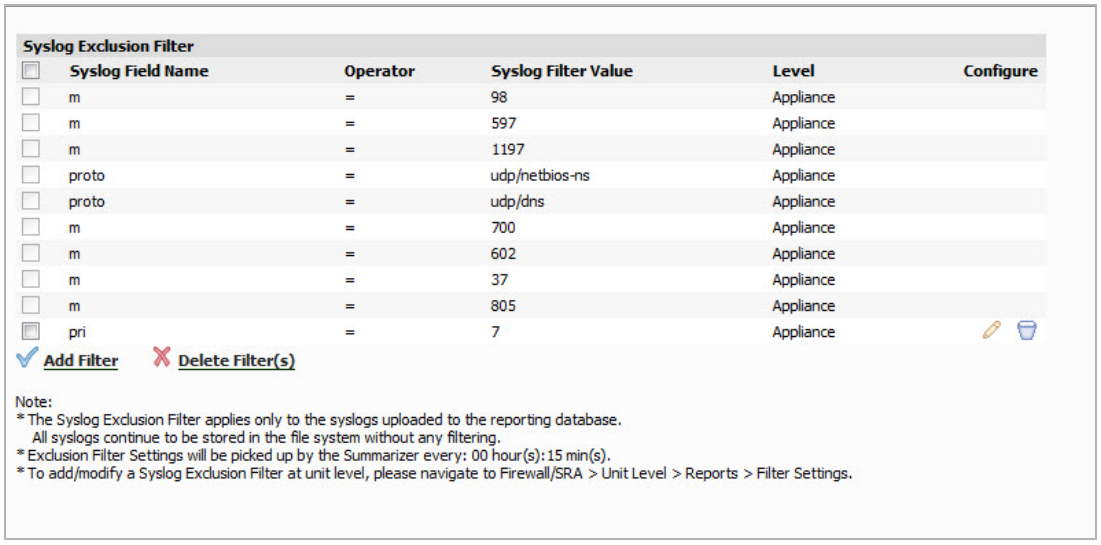
1. On the **Console** panel, navigate to **Reports > Summarizer**.
2. Under **Data Deletion Schedule**, select the day and time for deletion in the hour and minute **widget**. Syslog data will be deleted at this time only after being stored for the number of days configured. You specify how long to keep the date in **Data Storage Configuration**.This field allows you to specify the data address of the Summarizer, how long to keep reporting data (in months), and how long to keep the raw syslog data (in months)
3. Click the **Update** button to the right of this field.

Syslog Exclusion Filter

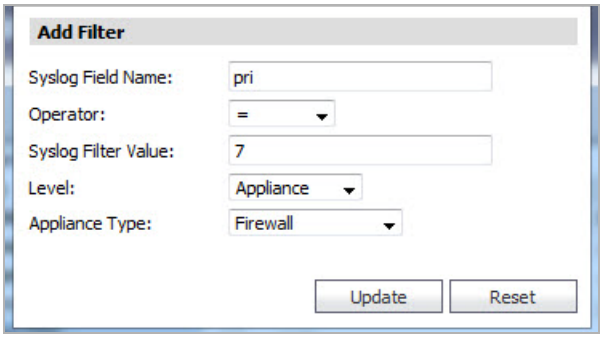
The Syslog Exclusion Filter allows you to select what fields and operators to use for filtering the syslog database. It is picked up by the Summarizer every 15 minutes and applied to the global syslog settings.

The Syslog Exclusion Filters function in a manner similar to applying an exclusion filter to a single Firewall or SRA appliance, but are applied to all GMS appliances, or all appliances in a Firewall or SRA group.

1. To add a filter, click **Reports** > **Syslog Filter**.



2. Click **Add a Filter**. The Add Filter menu comes up.



3. Select the syslog field name, and an operator and value, for the field you wish to exclude. Then select the level of Deployment: Appliance, Agent, or full Deployment.

   If you select Appliance, you will be prompted for the type of appliance: Firewall, SRA, or CDP. If you select Agent, you will be prompted to select from a list of SGMS agents.

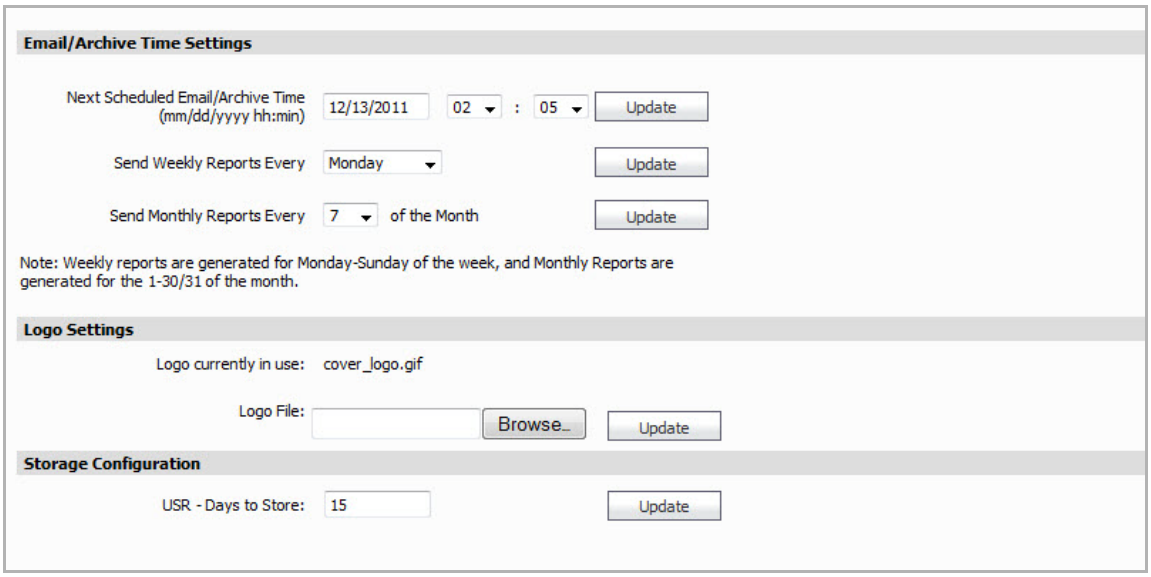
4. Click **Update**.

   You can also click on the pencil in the Configure column to edit an existing filter setting. If no values appear in the Configure column, the filter is a default system filter. These defaults cannot be configured or deleted.

   Syslogs are stored in the database without filtering, so the filters in the Syslog Exclusion Filter apply only to values displayed in Reports.

Email/Archive

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



Configuring Email/Archive Settings

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

1. Click the **Console** tab, expand the **Reports** tree and click **Email/Archive**. The Email/Archive page displays.
2. To set the next archive time, enter the date and time in the **Next Scheduled Email/Archive Time** fields and click **Update**.
3. To specify the day to send weekly reports, select the day from the **Send Weekly Reports Every** list box and click **Update**.
4. To specify the date to send monthly reports, select the date from the **Send Monthly Reports Every** list box and click **Update**.
5. If the Web server address, port, or protocol has changed since SonicWALL Analyzer was installed, the new values will automatically appear in the **Email/Archive Configuration** section. These settings can be modified on the System Interface, and cannot be modified here.
6. Under Logo Settings, you can select a logo to be used on reports. By default, the SonicWALL logo is used. To select another logo, click **Browse** next to the **Logo File** field or type the path and filename into the field, and then click **Update**.
7. Under Storage Configuration, select how many days to store Universal Scheduled Reports (USR) then click **Update**.

USR schedules are managed under the Dashboard Tab. For more information on USR scheduling, refer to the "Using the Universal Scheduled Reports Application" section on page 60.

Note High-traffic systems can generate reports that consume large amounts of memory, disk space and CPU time. Set your **Number of Days to Archive** and **Scheduled Archive Time** accordingly.

Managing Legacy Reports

Reports generated by pre 7.1 releases of Dell SonicWALL Analyzer are still available for viewing, but require careful management. Dell SonicWALL Analyzer 7.1 Reporting is not compatible with earlier versions, but reports generated by earlier versions are still accessible under the current reporting structure.

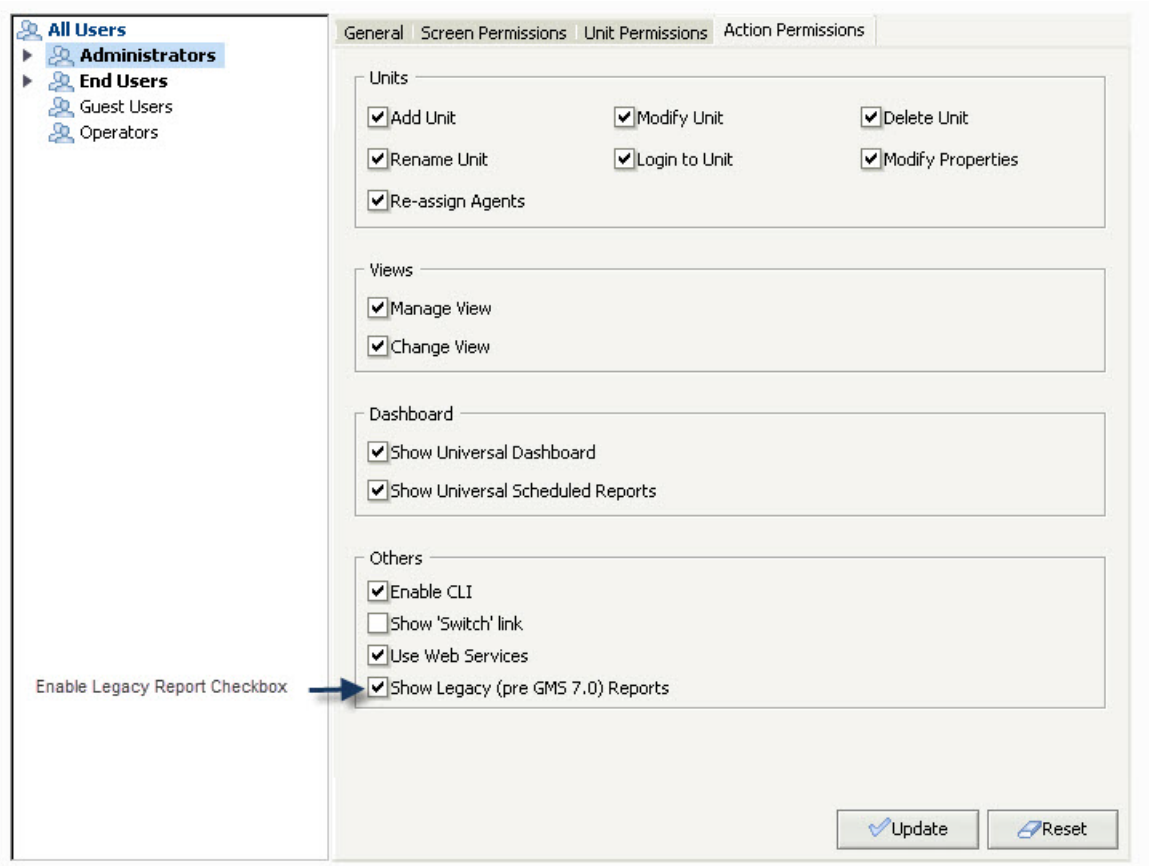
Because it is not possible to view both 7.1 and pre-7.1 reports in the same session, we advise creating a separate Login for accessing Legacy reports. This allows switching back and forth, as you can only view 7.1 or pre 7.1 reports in a session. By creating a separate login, you can switch between viewing modes.

Step 1 Create a new User or Administrator login. An Administrator login (with a name like Admin_Legacy) is recommended, as this login will have full privileges. For more information on configuring Legacy reports for new user, refer to the Console Management section.

Step 2 Log into the Management > Users > Action Permissions tab.

Step 3 Set flag in the checkbox for **Show Legacy (pre GMS 7.1) Reports**.

Note This check box is only available if SonicWALL Analyzer 7.0 Reports exist in the system.

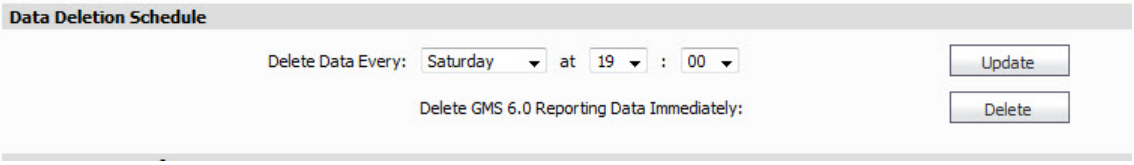


Step 4 Log out, log back in using the new Login created in Step 1.

If Legacy Reports are no longer needed, you can delete them.

Step 1 Go to **Reports > Summarizer**.

Step 2 Under the **Data Deletion Schedule**, you will see a box for **Delete 7.0 Reporting Data Immediately**. Click **Delete** to delete the Legacy reports.



Note If you delete pre-7.1 reporting data, the Legacy data checkboxes under the Action Permissions and Summarizer tabs will no longer be available, going forward.

CHAPTER 13

Using Diagnostics

This chapter describes the diagnostic information that SonicWALL Analyzer provides and summarizer status information.

This chapter includes the following sections:

Debug Log Settings

Debug Log Settings are included with Analyzer to help you diagnose issues you may encounter with your log data.

Warning **The Debug Log Settings are intended for use only under the direction of SonicWALL Tech Support.**

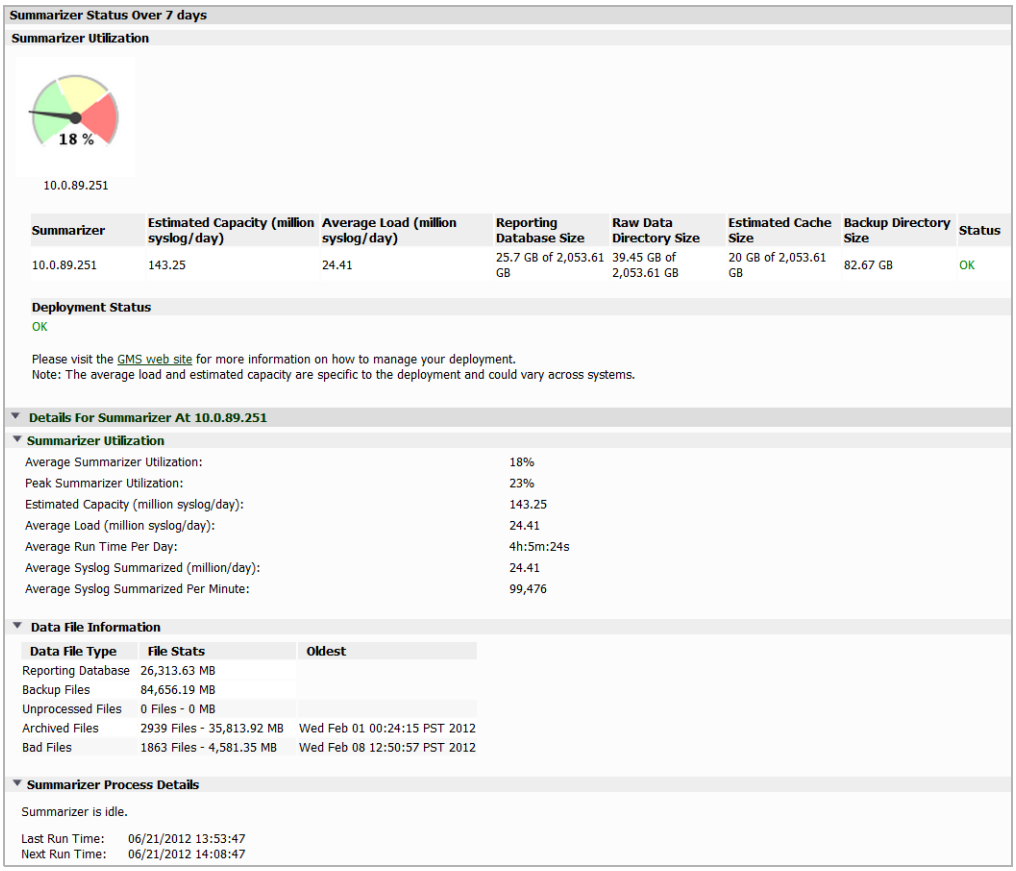
Configuring Debug Log Settings

When instructed by SonicWALL Technical Support, perform the following steps to set the debug level:

1. Click the **Console** tab, expand the **Diagnostics** tree and click **Debug Log Settings**. The Debug Log Settings page displays.
2. Select the amount of debug information that is stored from the **System Debug Level** field. For no debugging, enter 0. For verbose debugging, enter 3.

Summarizer Status

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



The Summarizer Status screen provides performance metrics for your network administrator to plan, design, and expand your Analyzer server deployment. This feature has information on the Syslog Collector and Summarizer metrics. The metrics displayed are daily averages collected over the last 7 days.

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

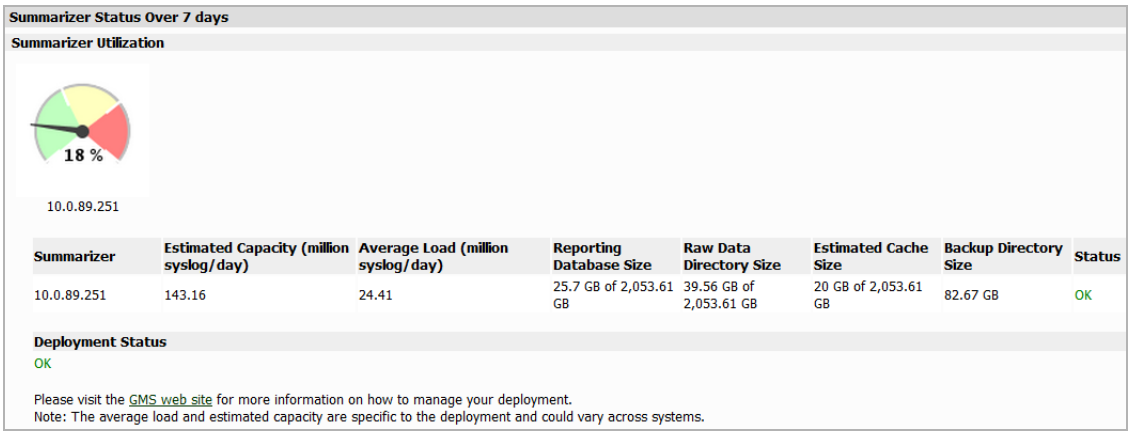
To reach the Summarizer Status screen, navigate to the **Console** panel of Analyzer and then to **Diagnostics > Summarizer Status**.

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

- Summarizer Status Over 7 Days, page 189
- Details for Summarizer at <IP Address>, page 190

Summarizer Status Over 7 Days

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



Summarizer Utilization

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

- **Summarizer**: Displays the IP address of the Summarizer.
- **Estimated Capacity (million syslog/day)**: The estimated capacity of the system. This is calculated by taking the (average load per day) and dividing it by the (time spent), assuming that the Summarizer was to constantly summarize 24 hours (as in the case of a dedicated Summarizer).
- **Average Load (million syslog/day)**: The number of incoming syslogs per day.
- **Reporting Database Size**: Displays the size of the reporting database in gigabytes.
- **Raw Data Directory Size**: Displays the size of the raw syslog directory in gigabytes.
- **Estimated Cache Size**: Displays the estimated size of the cache in gigabytes.
- **Backup Directory Size**: Displays the size of the backup directory in gigabytes.
- **Status**: Displays the status of the Summarizer. There are three different status notifications:
  - **OK**: The system is operating normally.
  - **High Capacity**: The average load is greater than 90% of capacity.
  - **Low Disk Space**: There is less that 5GB of space left on the disk.

Deployment Status

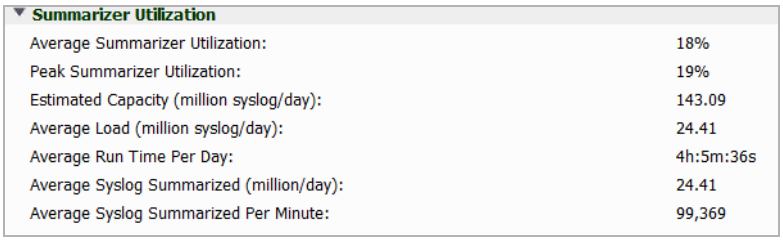
The Deployment Status tells the user how the deployment should be sized if it is not performing well. The user may need to reassign some units to a different agent, add another agent, or add more disk space

Details for Summarizer at <IP Address>

This sections details the Summarizer Utilization for the applicable IP address.

Summarizer Utilization

The Summarizer Utilization section for a specific summarizer shows not only the information at deployment level, but also provides granular details of the summarizer's operation and current status for each individual summarizer.

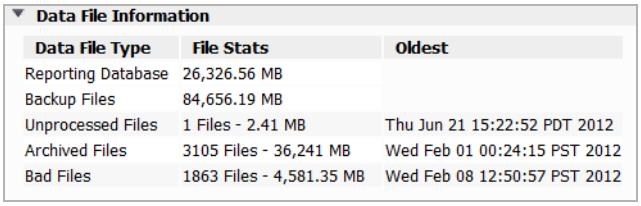


- **Average Summarizer Utilization**: The average percentage of Summarizer utilization.
- **Peak Summarizer Utilization**: The percentage of peak Summarizer utilization.
- **Estimated Capacity (million syslog/day)**: The estimated capacity of the system. This is calculated by taking the (average load per day) and dividing it by the (time spent), assuming that the Summarizer was to constantly summarize 24 hours (as in the case of a dedicated Summarizer).
- **Average Load (million syslog/day)**: The number of incoming syslogs per day.
- **Average Run Time Per Day**: The total amount of time spent generating summarization statistical data and results over the time period of one day.
- **Average Syslog Summarized (million/day)**: The total number of syslogs summarized, displayed in millions per day.
- **Average Syslog Summarized per minute**: The average number of syslogs summarized per minute over the applicable time period.

Note Not all syslogs are summarized. Some syslogs are discarded based on criteria defined at the **Console > Reports > Syslog Filter** and **Unit > Reports > Configuration > Syslog Filter** pages.

Data File Information

This section displays syslog file details for the selected summarizer.



The Data File Information table is divided into three columns:

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

  There are five main data file types:

  – Reporting Database Files: The files in the reporting database.

  – Backup Files: The backup snapshot.

  – Unprocessed Files: The data files in the summarizer's processing queue.

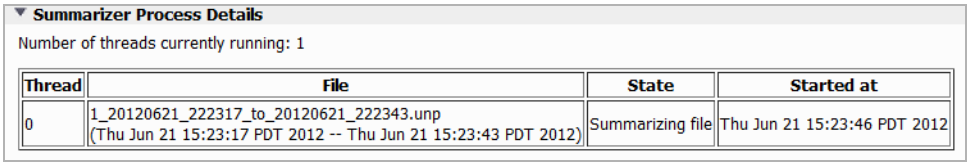
  – Archived Files: The processed data files.

  – Bad Files: Data files with processing errors.
- **File Stats**: The number of syslog files in the category and their size in Megabytes.
- **Oldest**: The date and time on the oldest file in the category.

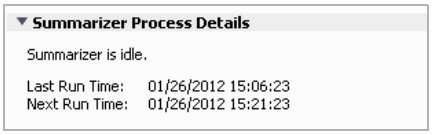
Summarizer Process Details

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

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



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



CHAPTER 14

Granular Event Management

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

This chapter contains the following sections:

Granular Event Management Overview

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

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

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

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

What is Granular Event Management?

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

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

How Does Granular Event Management Work?

The Granular Event Management framework provides customized event handling for specific alerts about database and database log size, and security service subscription licenses. For a list of the predefined alerts, see "**Using Granular Event Management**" on page 194.

Using Granular Event Management

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

Table 5 GEM Predefined Default Objects

Panel	Screens	Predefined Default Objects
Console	Events > Schedule	Schedule Groups:
		• 24x7
		• Weekdays 24 hours
		• 8x5
		• Weekend
		Schedules:
		• Schedule: admin
		• Database Backup
		• Monday 24 hours
		• Monday business hours
		• Tuesday 24 hours
		• Tuesday business hours
		• Wednesday 24 hours
		• Wednesday business hours
		• Thursday 24 hours
		• Thursday business hours
Console	Events > Alert Settings	Database Info
		• Database Size Status

Panel	Screens	Predefined Default Objects
		• System Files Backed-Up Status
		• Disk Space Utilization Status

About Alerts

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

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

- Firewall panel: Alert settings for Reporting
- Console panel: Alert settings for the Analyzer application

Table 6 GEM Alert Types

Panel location	Available Alert Types
Console	Backed up Syslog Files
	New Firmware Availability
	Bandwidth Usage (Billing Cycle)
	Bandwidth Usage (Daily)
Firewall	Anti Virus License
	CFS License
	Warranty License
	Anti Spyware License
	Intrusion License
	VPN Tunnel Status
	Agent Quota Reached
	Agent Unsuccessful Backups
	Appliance Capacity Status
	CPU Status

Configuring Granular Event Management

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

See the following sections:

- “Configuring Events on the Console Panel” section on page 196

Configuring Events on the Console Panel

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

See the following sections:

- “Configuring Event Thresholds” section on page 196
- “Configuring Event Schedules” section on page 198
- “Enabling or Disabling Alerts on the Console Panel” section on page 201

Configuring Event Thresholds

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

The following tasks are described in this section:

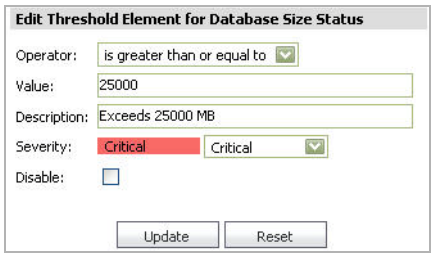
- “Editing an Threshold Element” section on page 197
- “Enabling/Disabling Thresholds and Threshold Elements” section on page 197

Editing an Threshold Element

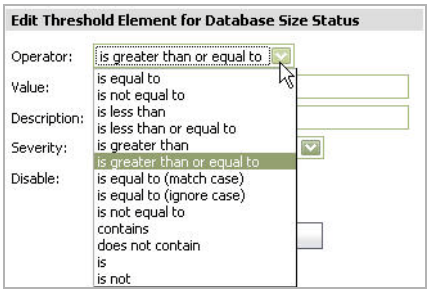
To edit an existing element of a Threshold, perform the following steps:

1. On the **Events > Threshold** screen, click the **Edit** icon located in the Configure column in the element row.

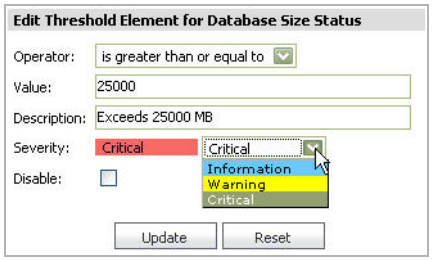
   The Edit Threshold pop-up window displays:



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



3. In the **Value** field, enter the value for your threshold element.
4. In the **Description** field, enter the description for your threshold element.
5. In the **Severity** field, select the severity priority from the drop down menu. These are color coded for your easy reference on the Events > Threshold screen.



6. To disable the threshold element, click the **Disable** check box. See "Enabling/Disabling Thresholds and Threshold Elements" section on page 197.
7. Click **Update**.

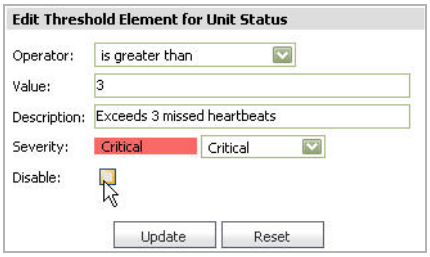
Enabling/Disabling Thresholds and Threshold Elements

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

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

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

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



4. Click **Update**.

Configuring Event Schedules

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

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

The following tasks are described in this section:

- "Adding an Event Schedule" section on page 198
- "Editing an Event Schedule" section on page 199
- "Adding an Event Schedule Group" section on page 200
- "Deleting a Schedule or Schedule Group" section on page 200

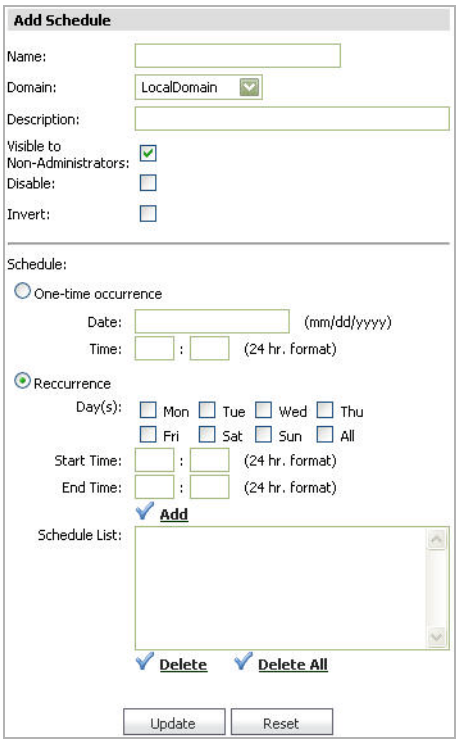
Adding an Event Schedule

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

To add an event schedule, perform the following steps:

1. On the **Events > Schedules** screen, click **Add Schedule**.
2. In the **Name** field, enter a name for the schedule.
3. In the **Domain** filed, click the pull-down list and select a name. This function is for Super Admins only.

4. In the **Description** filed, add a description for the schedule.
5. Select the **Visible to Non-Administrators** check box if you want the schedule to be visible and usable by non-administrators.
6. To temporarily disable a schedule, select the **Disable** checkbox.
7. Click **Invert** to create a schedule that is “off” during the dates and times that you specify.
8. In the Schedule field, you can create one or more schedules. For each schedule, configure either:
   - One Time Occurrence
     - Fill in the **Date** and **Time** fields.
   - Recurrence
     - Fill in **Days**, **Start Time**, and **End Time** fields.
9. Click **Add** to add this schedule to the **Schedule List** text box.



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

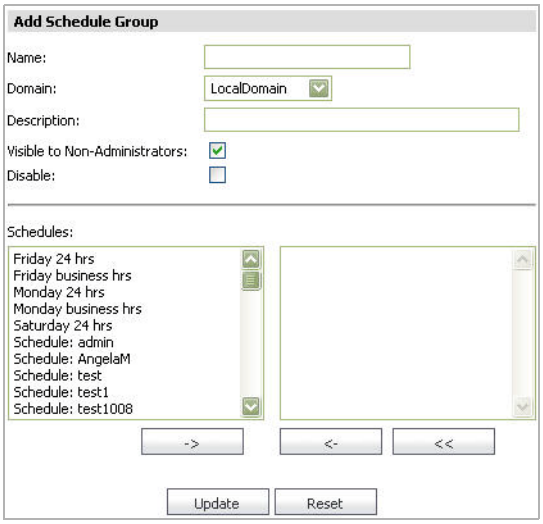
Editing an Event Schedule

To edit an existing schedule, click the **Edit** icon on the right side of the **Events > Schedule** screen. The screen and procedure for editing are the same as those for adding a schedule. See “Adding an Event Schedule” section on page 198.

Adding an Event Schedule Group

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

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



7. Click **Update**.

Editing an Event Schedule Group

To edit an existing schedule group, click the **Edit** icon on the right side of the **Events > Schedule** screen. The screen and procedure for editing are the same as those for adding a event schedule group. See "Adding an Event Schedule Group" section on page 200.

Deleting a Schedule or Schedule Group

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

Note Deleting a Schedule or Schedule Group that is in use is not permitted. A warning message displays when this action is performed.

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

1. Navigate to the **Events > Schedule** screen.

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

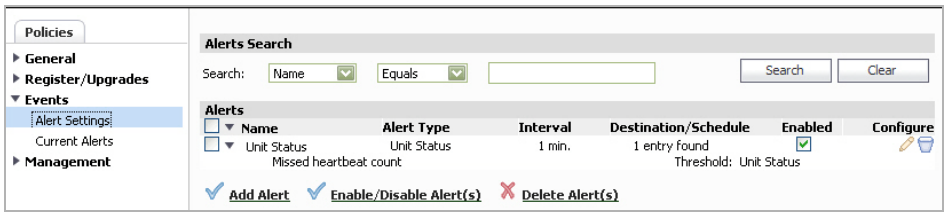
Enabling or Disabling Alerts on the Console Panel

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

Add Alert

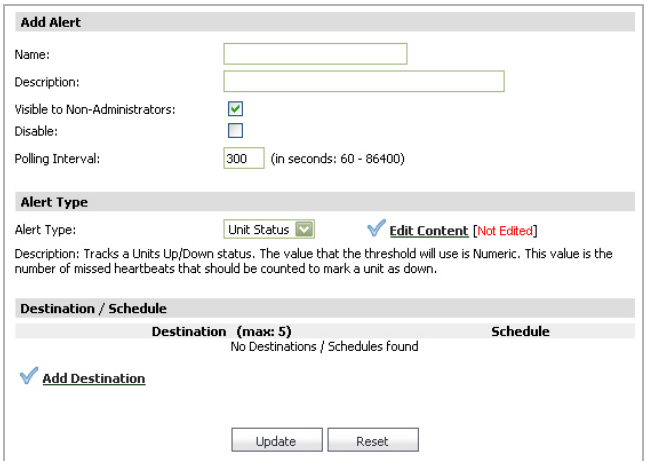
In the Add Alert panel you can enter an alert name and description, select the options for visible to non-administrators and disable, and enter the polling interval. Perform the following steps to add an alert:

1. Navigate to the **Events** > **Alert Settings page**.



2. Click the **Add Alert** link.

The Add Alert screen displays.



3. Enter a name and description for your alert.
4. Enable the **Visible to Non-Administrators** checkbox if you want your Alert to be visible to non-administrators.
5. Enable the **Disable** checkbox to disable this Alert.

6. Enter a **Polling Interval** value (in seconds: 60-86400)

Alert Type

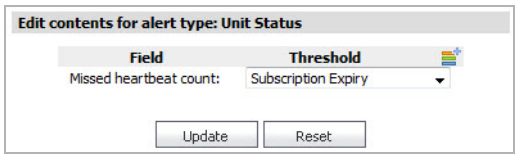
In the Alert Type panel you can select an alert type from the provided list and view the definitions of each alert type. Perform the following steps to configure an Alert Type:

1. Click the **Alert Type** pull-down list and select an alert type.

Note When an alert type is selected, a description for that alert is displayed in the Alert Type panel.

Most of the Alert Types require you to edit content. Editing Contents allows the user to pick additional info, in a granular fashion, on which the alerting has to be performed.

2. Click the **Edit Content** link. The Edit Contents for Alert Type Unit Status pop-up window displays.



3. Click the **Threshold** pull-down list and select a threshold.

Note You can create a new threshold on-the-fly by clicking the icon. Only one new threshold can be created in this feature.

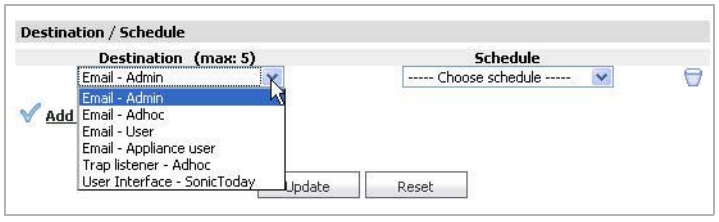
4. Click the **Update** button. To reset the settings, click the **Reset** button.

Destination / Schedule

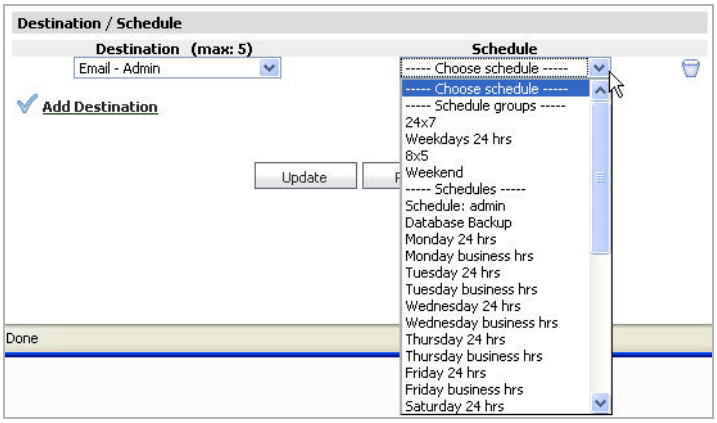
In the Destination / Schedule panel you can add up to 5 destinations and set a schedule for each. Perform the following steps to add a destination and set a schedule:

Note Every selected destination is required to have a schedule set.

1. Click the **Add Destination** link under the Destination/Schedule section. The Destination field designates where you want alerts to be sent. You have a maximum number of five destinations.



2. Click the **Schedule** pull-down list, then select a schedule type. The Schedule field designates the frequency of when you want alerts to be sent to the destination(s).



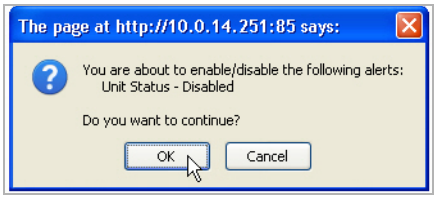
3. Click **Update** to finish adding an alert.

Enabling/Disabling Alerts

Perform the following steps to enable and disable an alert:

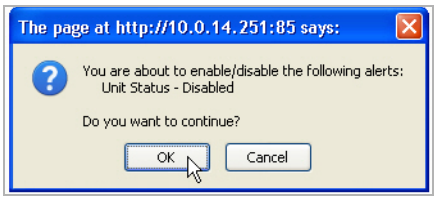
Enabling a Alert

1. Select the **Enabled** checkbox of the alert(s) you wish to enable.
2. Click the **Enable/Disable Alert(s)** link. A confirmation window will display. Click **OK** to enable/disable.



Disabling an Alert

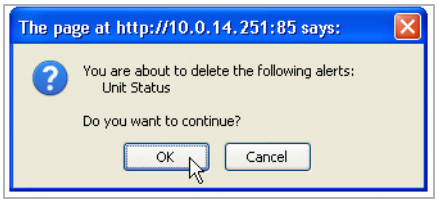
1. Deselect the **Enabled** checkbox of the alert(s) you wish to disable.
2. Click the **Enable/Disable Alert(s)** link. A confirmation window will display. Click **OK** to enable/disable.



Deleting Alerts

Perform the following steps to delete an alert:

1. Select the checkbox(s) of the Alert(s) you wish to delete.
2. Click the **Delete Alert** link. A confirmation window will display.



3. Click **OK** to delete.

Note

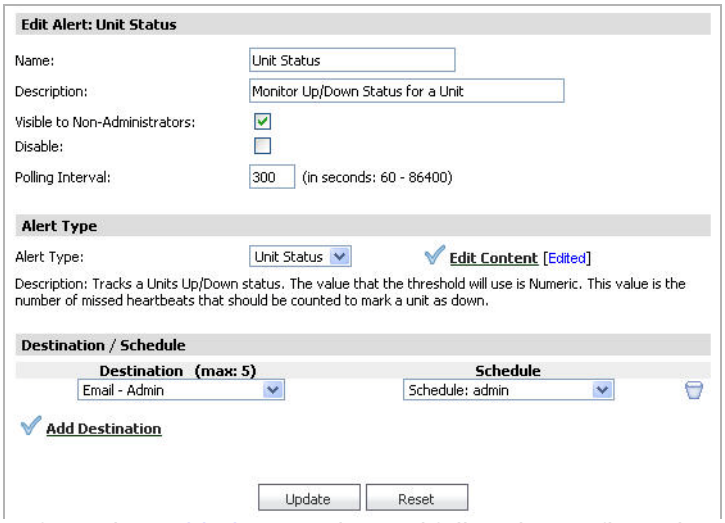
You can also delete an alert by clicking the **Delete** icon under the **Configure** section of the alert you wish the delete.

Editing Alerts

Once an alert is created, you can go back and edit it at any time. Perform the following steps to edit an alert:

1. Click the **Configure** icon of the alert you wish to edit.

The **Edit Alert** page will display.



2. Refer to the "Add Alert" section and follow the configuration procedures to edit your existing Alert.

Viewing Current Alerts

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

CHAPTER 15

Using Analyzer Help

To access the Analyzer online help, click the **Help** button in the top-right corner of the Analyzer user interface.

The Dell SonicWALL Analyzer online help provides context-sensitive conceptual overviews, configuration examples, and trouble shooting tips.

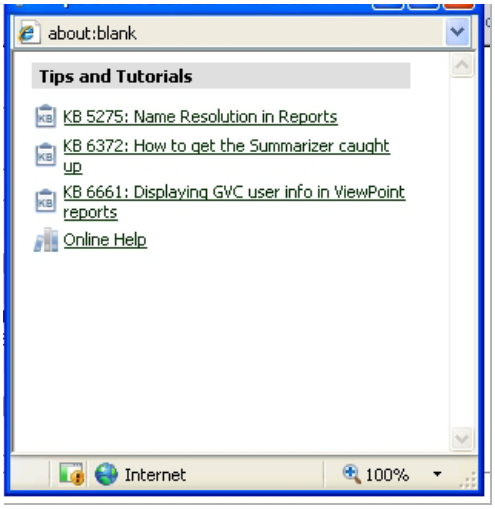
About Analyzer

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

To access the Analyzer online help, click the blue **Help** button in the top-right corner of the Analyzer user interface.

Tips and Tutorials

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



To access tips and tutorials:

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

Appendix A: Upgrading

This appendix is designed to help you upgrade Dell SonicWALL Analyzer. If you have not used Dell SonicWALL Analyzer before, you might want to familiarize yourself with Dell SonicWALL Analyzer concepts and features.

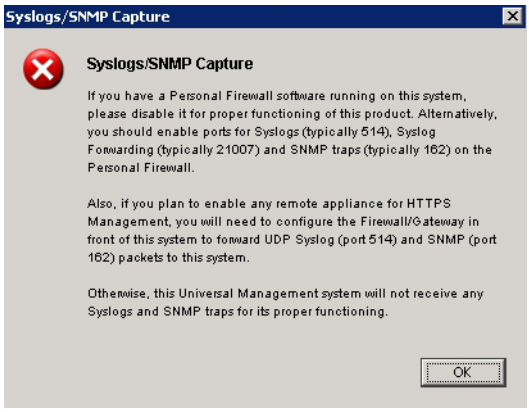
This appendix contains the following sections:

Upgrading SonicWALL ViewPoint 6.0 to Analyzer 7.1

The Dell SonicWALL Analyzer cannot be directly upgraded from ViewPoint 6.0 to Analyzer 7.1, but it can be upgraded from Analyzer 7.0. To upgrade the Dell SonicWALL Analyzer from a version earlier than 7.0, you need to upgrade to major versions of Analyzer until you reach 7.0, then you can upgrade to 7.1. To upgrade major versions of Dell SonicWALL Analyzer, use the Universal Management Suite installer and perform the following:

1. Log on to your Dell SonicWALL Analyzer management computer as **administrator** (Windows). Launch the SonicWALL Universal Management Suite installer, by double-clicking the file **sw_gmsvp_win_eng_x.x.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 a previous version of Analyzer/ViewPoint 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 Dell 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 Dell SonicWALL Analyzer 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 Dell SonicWALL Analyzer installation, enter the word **Analyzer** 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**.

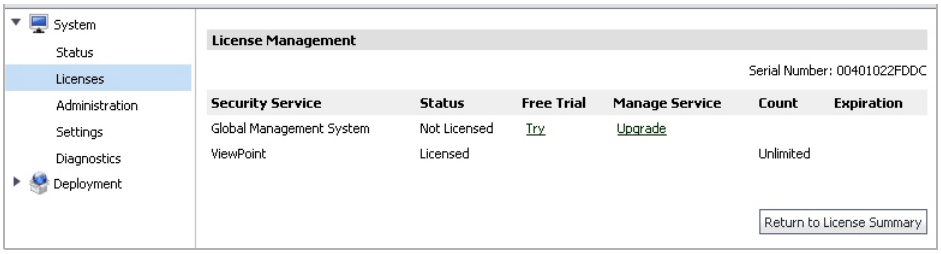
   In the Dell SonicWALL Analyzer login page, enter the same credentials for **User** and **Password** that you had in your earlier version prior to the upgrade.

Upgrading from Analyzer to GMS

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

When five or more registered devices are connected to Dell SonicWALL Analyzer reporting, the **Try GMS Free - 30 Days** button appears next to the tabs at the top of the Analyzer 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 Dell SonicWALL GMS Free Trial and purchasing the Dell SonicWALL GMS upgrade license, see the following sections:

- “Enabling the GMS Free Trial from Analyzer” section on page 211
- “Enabling the GMS Free Trial from the UMH Interface” section on page 213
- “Completing the Free Trial Upgrade” section on page 214
- “Configuring Appliances for GMS Management” section on page 217
- “Purchasing a SonicWALL GMS Upgrade” section on page 218

Enabling the GMS Free Trial from Analyzer

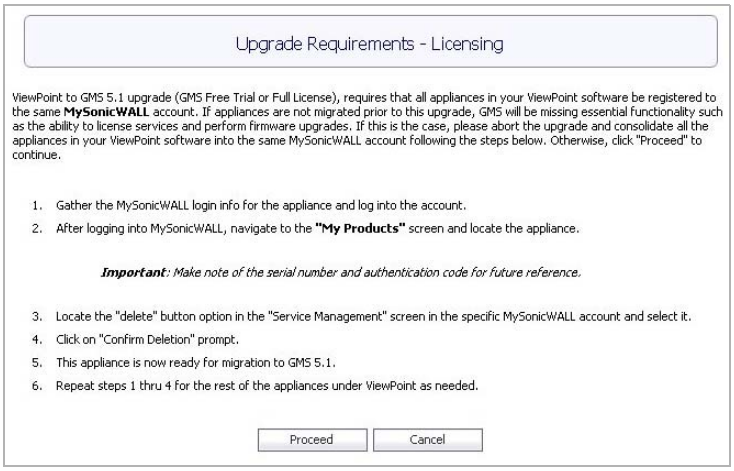
When five or more devices are connected to Dell SonicWALL Analyzer reporting, the **Try GMS Free - 30 Days** button appears next to the tabs at the top of the Analyzer management interface.

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

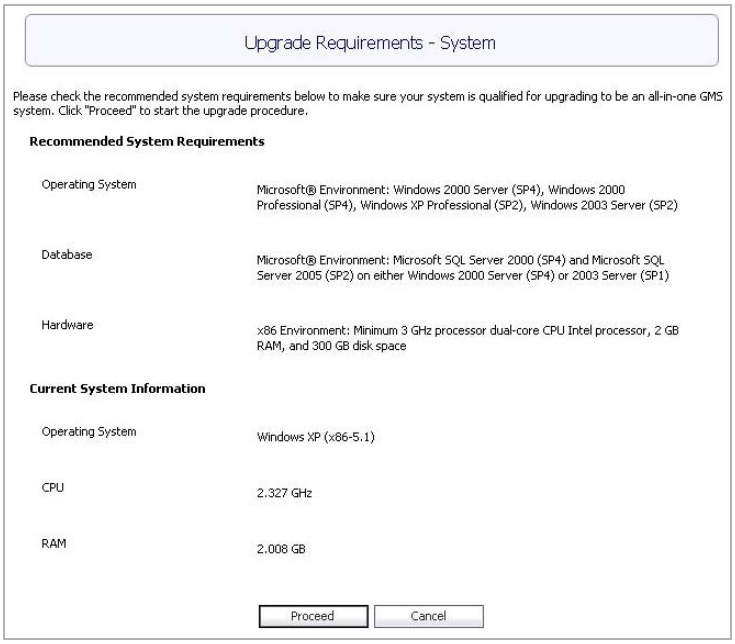
To enable the 30-day Dell SonicWALL GMS Free Trial from the Analyzer management interface, perform the following steps:

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

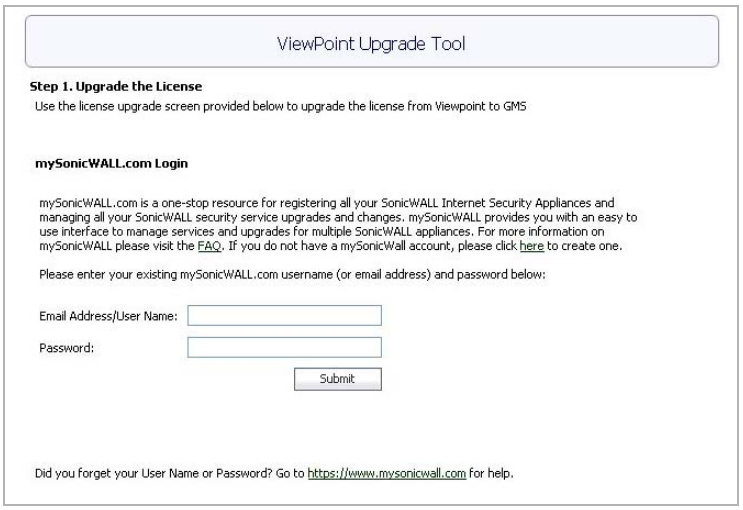
2. The Analyzer Upgrade Tool launches and guides you through the process of installing the Free Trial or Upgrade. The tool displays the **Upgrade Requirements – Licensing** screen. Before migrating to GMS, ensure that all appliances under Analyzer reporting are registered to the same MySonicWALL account.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



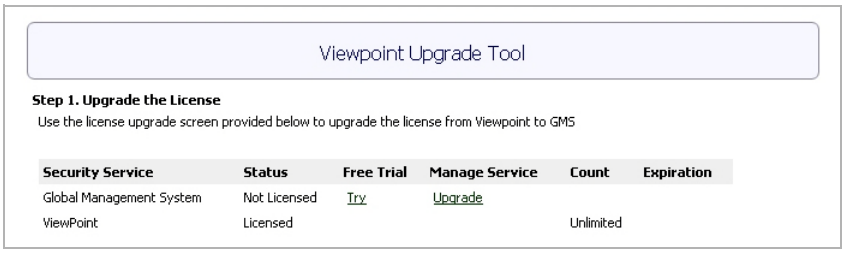
3. The **Upgrade Requirements – System** screen displays the recommended operating system, database, and hardware system requirements. Click **Proceed**.



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



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

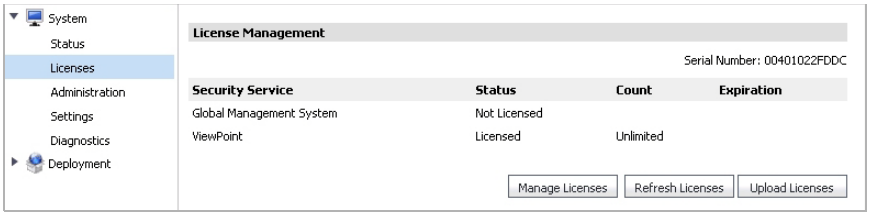


6. From this point, the upgrade process continues with the same steps for access from either the Analyzer interface or the Universal Management Host interface. To continue the procedure, perform the steps in the “Completing the Free Trial Upgrade” section on page 214.

Enabling the GMS Free Trial from the UMH Interface

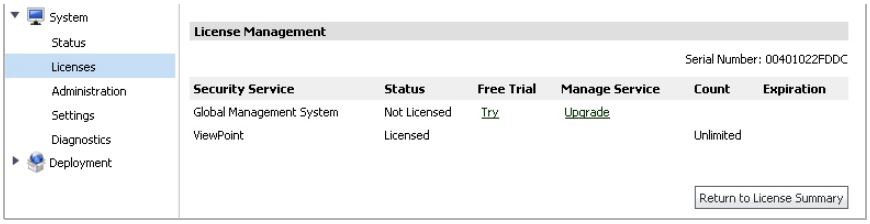
To enable the 30-day Free Trial of Dell SonicWALL GMS from the Universal Management Host interface on your Dell SonicWALL Analyzer system, perform the following steps:

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.

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



4. From this point, the upgrade process continues with the same steps for access from either the Analyzer interface or the Universal Management Host interface. To continue the procedure, perform the steps in the “Completing the Free Trial Upgrade” section on page 214.

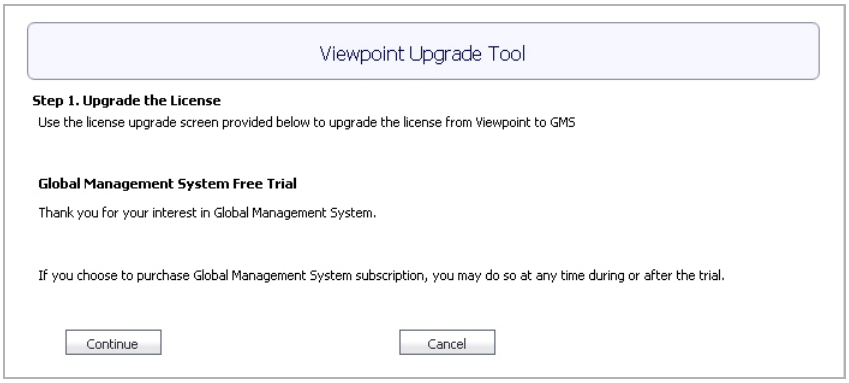
Completing the Free Trial Upgrade

This procedure provides the common upgrading steps for access from either the SDell SonicWALL Analyzer 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:

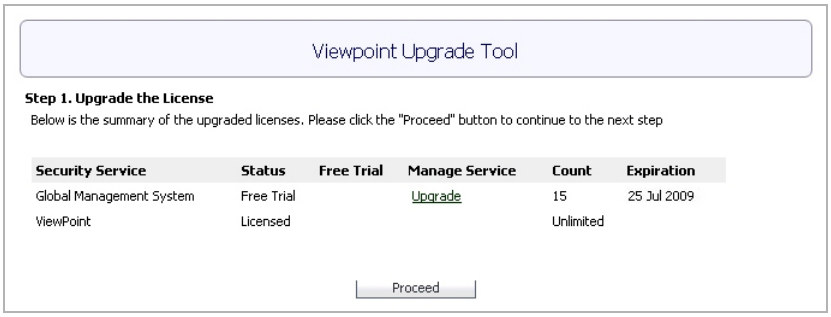
- “Enabling the GMS Free Trial from Analyzer” section on page 211
- “Enabling the GMS Free Trial from the UMH Interface” section on page 213

To continue the upgrade, perform the following steps:

1. In the Analyzer Upgrade Tool page, click the **Continue** button.



2. The next screen provides a summary of GMS and Analyzer 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 Dell SonicWALL GMS upgrade. Click **Proceed**.

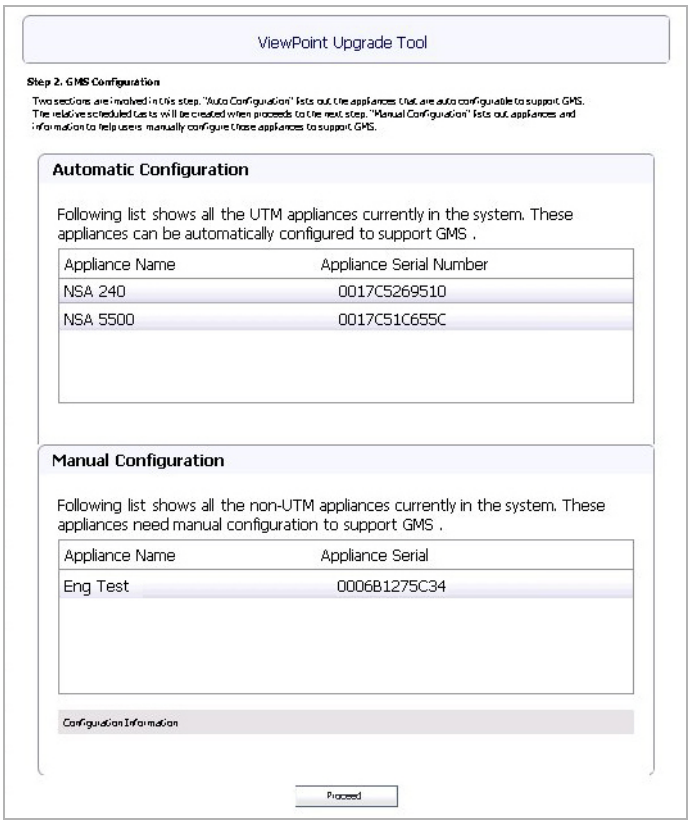


3. In the next Analyzer Upgrade Tool page, you begin the configuration for GMS in step 2 of the upgrade process. This page displays two sections:

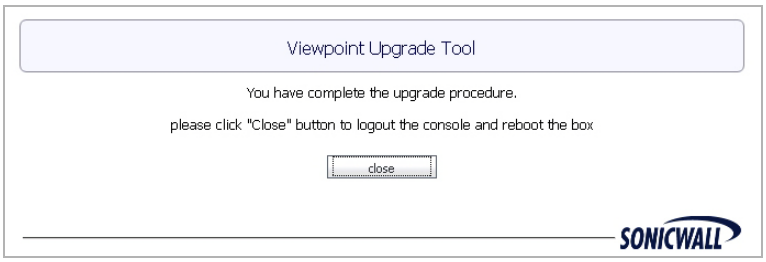
   Automatic Configuration – Contains a list of Dell SonicWALL firewall or CSM appliances in your Analyzer installation. These appliances will be automatically configured for GMS management.

   Manual Configuration – Contains a list of Dell SonicWALL Aventail, SSL-VPN, or CDP appliances in your Analyzer installation. You must manually configure these appliances for GMS management. See the "Configuring Appliances for GMS Management" section on page 217 for detailed instructions on enabling GMS management on these appliances.

   When ready, click **Proceed**.



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

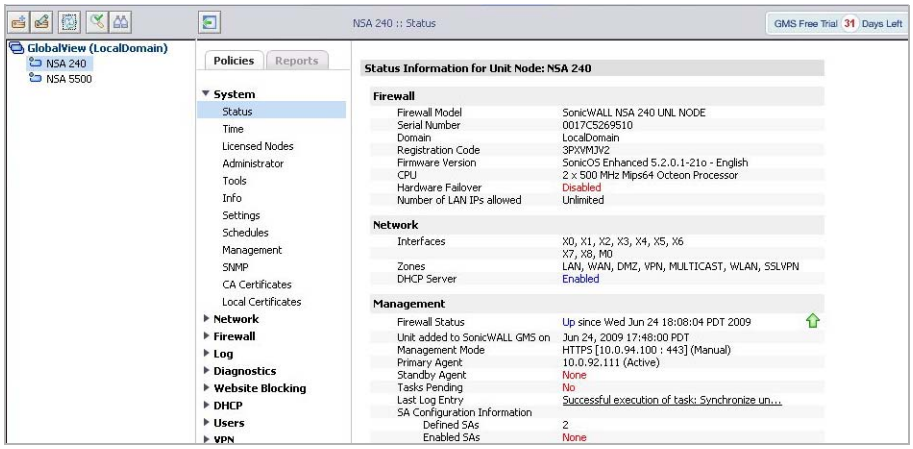


5. The GMS login page appears and requests that you reboot the system. Reboot the system. If a reboot is not performed, you may encounter problems with the correct IP Address appearing.

6. After rebooting, log in with your Analyzer 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.

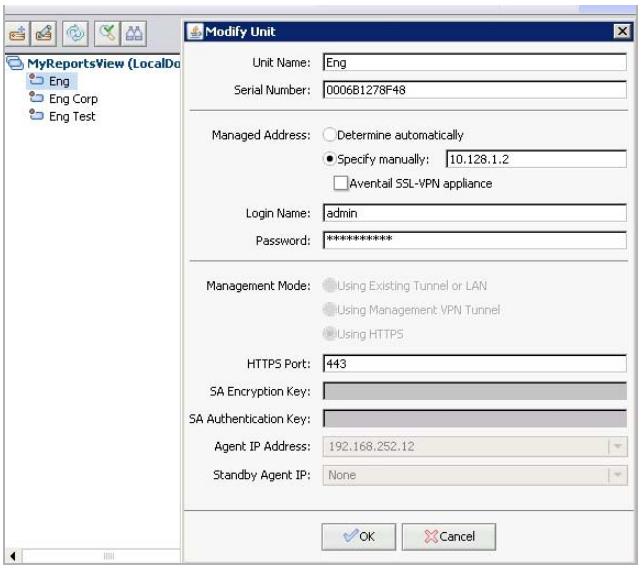
7. On the **System > Status** page for connected appliances, you can view the log entries for task synchronization and automatic addressing mode, related to the GMS configuration.



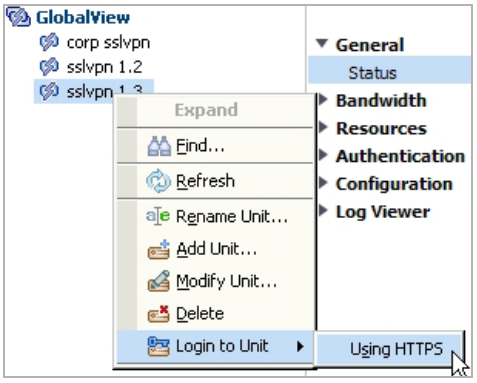
Configuring Appliances for GMS Management

To manually configure the appliances listed in the Manual Configuration section of the Analyzer Upgrade Tool page (see Step 3. on page 215), perform the following steps for each appliance:

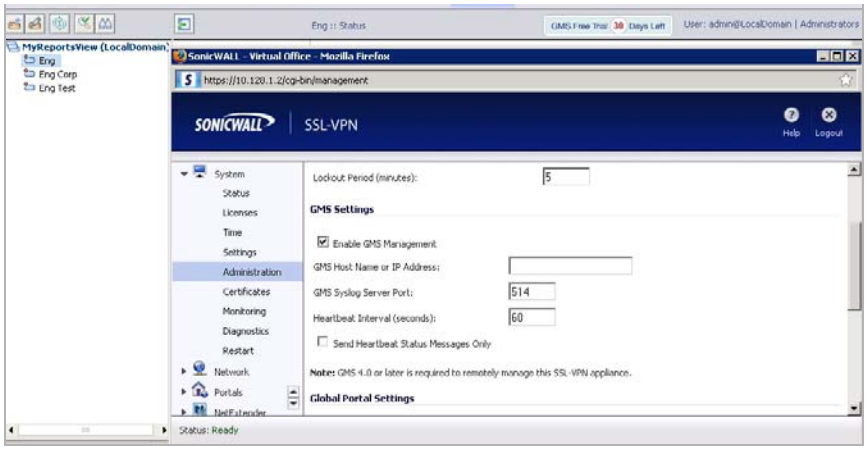
1. In the GMS management interface, click the tab at the top of the page that corresponds to the type of appliance, such as **SSL-VPN** or **CDP**.
2. In the left pane, right-click one of the listed appliances and select **Modify Unit**.
3. In the Modify Unit screen in the right pane, copy the appliance 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 Analyzer Upgrade Tool page.

Purchasing a SonicWALL GMS Upgrade

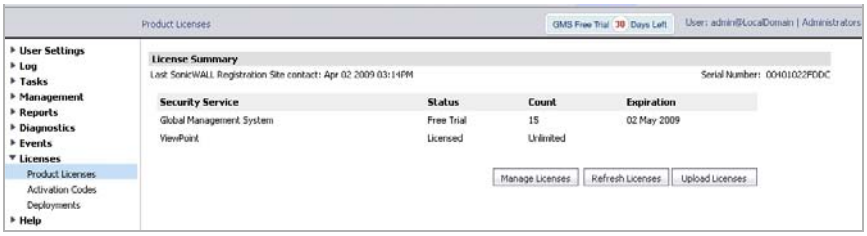
You can purchase an upgrade to Dell SonicWALL GMS at any time during the 30-day Free Trial.

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

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

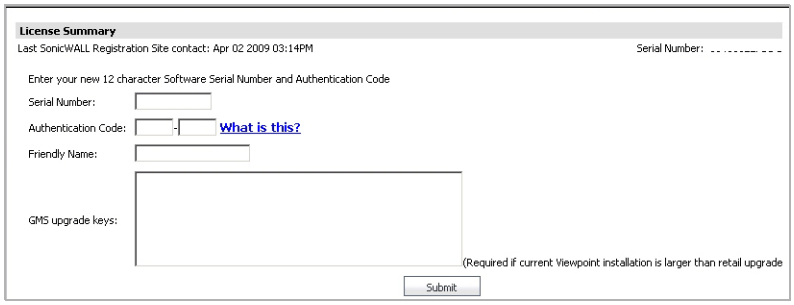
2. In the **Buy GMS** page, click **I want to upgrade to GMS now**.

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 GMS. You must contact your Dell 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.



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

Miscellaneous Procedures and Tips

This section contains miscellaneous Global Management System 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 Dell SonicWALL Analyzer data. For more information, see “Backing up Dell SonicWALL Analyzer Data” on page 220.
- Dell SonicWALL Analyzer requires Mixed Mode authentication when using SQL Server 2000. To change the authentication mode, see “Changing the SQL Server Authentication Mode” on page 220.
- If you are reinstalling Dell SonicWALL Analyzer, preserving the previous configuration settings can save a lot of time. To reinstall Dell SonicWALL Analyzer using an existing Dell SonicWALL Analyzer database, see “Reinstalling Dell SonicWALL Analyzer Using an Existing Database” on page 221.
- If you need to uninstall Dell SonicWALL Analyzer from a server, it is important to do it correctly. To uninstall Dell SonicWALL Analyzer, see “Uninstalling SonicWALL Universal Management Suite and Its Database” on page 221.

Backing up Dell SonicWALL Analyzer Data

Dell SonicWALL Analyzer stores its configuration data in the SGMSDB database. It is important to back up this database and the individual Dell SonicWALL Analyzer 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.

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 Dell SonicWALL Analyzer services for database backup. However, make sure that the backup occurs when Dell SonicWALL Analyzer activity is the lowest and that the backup operation schedule does not clash with the Dell SonicWALL Analyzer scheduler.

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

Changing the SQL Server Authentication Mode

Dell SonicWALL Analyzer 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 Dell SonicWALL Analyzer Using an Existing Database

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

1. Install a new database, using the same username and password that you used for the existing Dell SonicWALL Analyzer database.
2. Install Dell SonicWALL Analyzer using this new database.
3. Stop all Dell SonicWALL Analyzer 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 Dell SonicWALL Analyzer database.
5. Restart the Dell SonicWALL Analyzer 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 221.
- To uninstall SonicWALL Universal Management Suite databases from Microsoft SQL Server 2000, see “MS SQL Server 2000” on page 221.

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.