SonicWall™ Analyzer 8.3

Administration Guide

SONICWALL™

Legend

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

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

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Analyzer Administration Guide
Updated — March 2017
Software Version — 8.3
232-003848-00 Rev A

Contents

Part 1. Introduction

Part 2. Dashboard

Part 3. Reporting

Part 4. Console

Part 5. UMH

Part 6. Appendices

Part 1

Introduction

- Introduction to Analyzer
- Provisioning and Adding SonicWall Appliances

1

Introduction to Analyzer

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

About this Guide

This guide provides the information you need to configure and use SonicWall Analyzer for monitoring SonicWall network security and other appliances. SonicWall Analyzer creates dynamic, Web-based network reports showing all activity on monitored appliances.

Overview of Analyzer

This section contains the following subsections:

What is Analyzer?

Monitoring critical network events and activity, such as security threats, inappropriate Web use, and bandwidth levels, is an essential component of network security. 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.

Key Features in Analyzer 8.3

This section describes the SonicOS enhancements included in the Analyzer 8.3 release:

- **Provides SonicOS 6.2.7 support** — SonicOS Enhanced versions 6.2.7 and above are supported.

Key Features in Analyzer 8.2

This section describes the SonicOS enhancements included in the Analyzer 8.2 release:

- **Provides SonicOS 6.2.6 support** — SonicOS Enhanced versions 6.2.6 and above are supported, including SonicPoint enhancements like Capture ATP policy configuration.

  SonicOS 6.2.6.0 includes an important new feature that are supported by Analyzer 8.2:

  - Capture Advanced Threat Protection (Capture ATP)

- **About Capture ATP** — Capture Advanced Threat Protection (ATP) is an add-on security service to the firewall, similar to Gateway Anti-Virus (GAV). Capture ATP helps a firewall identify whether a file contains a zero-day virus by transmitting a suspicious file to the Cloud where the Capture ATP service analyzes the file to determine if it contains a virus. Capture ATP then sends the results to the firewall. This is done in real time while the file is being processed by the firewall.

  The **Capture ATP > Status** page displays a graph chart that shows the percentages of benign and malicious files discovered, as well as the total number of files analyzed. It also displays a log table that shows the results of individual files submitted for analysis.

  Capture ATP can also analyze files that you upload for analysis from the **Capture ATP > Status** page. After the files are analyzed they are listed in the table on the Status page. You can click on any file in the log table on the Status page and see the results from the detailed analysis of that file.

Note that Capture ATP is only supported on the following appliances. The smaller TZ appliances and the SOHO wireless appliance do not support Capture ATP.

Table 1.

- SuperMassive 9600
- SuperMassive 9400
- SuperMassive 9200
- NSA 6600
- NSA 5600
- NSA 4600
- NSA 3600
- NSA 2600
- TZ600
- TZ500 and TZ500 Wireless

Key Features in Analyzer 8.1

This section describes the SonicOS enhancements included in the Analyzer 8.1 release:

- **Provides SonicOS 6.2.4 and 6.2.4.3 and above support** — New features in SonicOS 6.2.4, 6.2.4.3 and above are supported.
    - **Log > Settings enhancements** — New fields added including: “Syslog ID,” “E-mail Format,” and “Include All Log Information.”
        - In the Syslog ID box, enter the Syslog ID that you want. A Syslog ID field is included in all generated Syslog messages, prefixed by “id=”. Thus, for the default value, firewall, all Syslog messages include “id=firewall.” The ID can be set to a string consisting of 0 to 32 alphanumeric and underscore characters.

        NOTE: The Syslog ID field is fixed to firewall when the Override Syslog Settings with Reporting Software Settings option is enabled, and therefore, cannot be modified.

        - **Email Format** — Select whether log emails will be sent in Plain Text, CSV Attachment, or HTML format from the drop-down menu.
        - **Include All Log Information** — Select to have all information included in the log report.
        - **Solera Capture Stack** — Solera Networks makes a series of appliances of varying capacities and speeds designed to capture, archive, and regenerate network traffic. The Solera Networks Network Packet Capture System (NPCS) provides utilities that allow the captured data to be accessed in time sequenced playback, that is, analysis of captured data can be performed on a live network via NPCS while the device is actively capturing and archiving data.
- **Firewall Action** — Changes to the report database, table structure, and associated reports in the UI. Report can now include the firewall action for all events relating to the traffic that is traversing or being blocked by the firewall.
- **Reporting Database** — Infobright with Postgres — The Analyzer 8.1 upgrade replaces the Infobright with MySQL database formerly used in earlier versions with Infobright with Postgres. The installer will ask if you want to perform the data migration to the new database.
- **Analyzer 8.1 Installation and Deployment Requirements** — The license to distribute Infobright with MySQL, the reporting database used in Analyzer 8.0, expires on Dec 31, 2015. Infobright is replacing it with Infobright running the PostgresSQL engine instead. The basic premise for the changes is the restrictions and difficulties in negotiating the licensing agreements with Oracle MySQL.

  Support for InfoBright with MySQL will continue and customers who have deployments as of Dec 31, 2015 will continue to receive upgrades, patches, and hot fixes until Dec 31, 2018. They will also be able to add new Agents to the existing deployments.
- **Backup and Restore Performance enhancements** — Added two new fields to the UMH S**ystem > Backup/Restore** screen to include “Free disk space required,” and “Auto disk space management.”

- **“Free disk space required”** — Indicates the space required to perform the backup, and how much space is available for use on the resource. If available disk space is less than the estimated free disk space required, the backup process will not start. However, if the auto disk space management feature is enabled, the backup process deletes the previous backup files to free the disk space required for the backup process to begin.
- **“Auto disk space management”** — Select to allow Analyzer to manage the disk space and backup requirements. Auto disk space management is a configurable option provided for you to automate recovering disk space by deleting previous backup files in case of a disk space shortage for the backup process. If there is sufficient disk space for the backup process to run, this feature does not have any impact.

Key Features in Analyzer 8.0

This section describes the SonicOS enhancements included in the Analyzer 8.0 release:

- **Provides SonicOS 6.2.4 support** — Analyzer 8.0 supports the following SonicWall network security platforms for reporting:
  - TZ300 and TZ300 Wireless
  - TZ400 and TZ400 Wireless
  - TZ500 and TZ500 Wireless
  - TZ600 and TZ600 Wireless
  - SOHO and SOHO Wireless*

  * The TZ appliances run SonicOS 6.2.3.1 or higher, while the SOHO runs SonicOS 5.9.1.3 or higher. Appliances running firmware newer than the SonicOS 6.2.3.1 or 5.9.1.3 releases can still have reports generated by Analyzer 7.2.
- **Java Applet Replacement** — The TreeControl application (that displays all managed appliances) and the User Management application (Console > Management > Users) have now been replaced with non-Java versions. All Java applets in the front-end have been removed, except for NetMonitor and the “Login to Unit” feature from TreeControl.
- **SonicOS Support** — New features in SonicOS 6.2 are supported.
- **Portuguese Support** — The Login screen now includes version information and indicates Brazilian Portuguese support.
- Reporting
  - **Report Database Rebuild Utility** — The Reporting Database Rebuild Utility allows you to submit a request to rebuild any specific month's report table if it were to become corrupt.
  - **Report Data Optimization** — In previous versions, report data optimization exported sorted report data into a file and reloaded that data back to the report database. In Analyzer 8.0, instead of using a file to upload the data, a temporary table is created that exports and reimports that data, leading to better performance.
  - **Botnet Reports** — Botnet reporting is added to the Reports panel and includes four report types: Attempts, Targets, Initiators, and Timeline.
  - **Geo-IP Reports** — Geo-IP reports contain information on blocked traffic that is based on the traffic's country of origin or destination. Geo-IP Reporting is added to the Reports panel and includes four report types: Attempts, Targets, Initiators, and Timeline.
  - **MAC Address in Reporting** — This feature shows the Media Access Control (MAC) address on the report page. This adds detail to the current device-specific information in the report panel and

the PDF report. New columns “Initiator MAC” and “Responder MAC” are added to the following reports:

- Data Usage > Initiators
- Data Usage > Responders
- Data Usage > Details
- User Activity > Details
- Web Activity > Initiators

- **Enhanced Reporting Database** — The Reporting Database has been upgraded to a newer version that offers better performance and higher reliability.
- **Distributed Universal Scheduled Report** — PDF report generation and uses an engine that can make better use of your CPU and RAM resources, resulting in faster delivery of scheduled reports with larger volumes and more rows of data.

- **Enhanced USR Template Manager** — In addition to the PCI Report template, HIPAA and SOX templates are added to Universal Scheduled Reports as an aid for compliance audits.
- **USR-Customizing Sorting Option in PDF** — Provides additional sorting options for Scheduled PDF reports
- **Log** Analyzer — The **Firewall > Reports > Analyzers > Log** Analyzer page has been updated with an out-of-the-box default view.
- **Packet Data View for Signature Alerts**
- The disabling of default Syslog filters is allowed
- **Comments Possible for Syslog Filters**
- Number of Syslog messages per file configurable through UI
- **All Windows Modules of Analyzer 8.0 are now 64-bit** — Provides better usage of system resources and better performance.
- High-level User Interface Changes
  - Secure Remote Access (SRA) has been renamed to Secure Mobile Access (SMA).
  - The CDP tab is removed.
  - SMA (formally SRA) tabs are no longer shown by default, but can be activated on **Console > Management > Settings**.

Key Features in Analyzer 7.2

The following features were key to Analyzer 7.2:

- **IPv6 Support** — IPv6 is supported in Analyzer 7.2, allowing you to:
  - Install Analyzer in an IPv6 network environment. Analyzer can now access various Network Elements using IPv6 addresses, such as: Firewalls, SMTP servers, RADIUS/LDAP Authentication Servers, SNMP Managers, WebServices, and so on.
  - Access Analyzer web interfaces on an IPv6 network.
  - Generate IPv6 based reports.
- **Scheduled Reports Permission Management** — In 7.1, scheduled reports created by an end user can only be viewed and configured by the creator and Administrator. 7.2 gives the scheduled report creator the ability to manage permissions of the scheduled reports so other users in the deployment can view and configure the report.

- **Intrusion Reporting Enhancements** — Two new reports are added at root level to the Intrusion reports:
  - Reports > Intrusions > Details
  - Reports > Intrusions > Alerts
- **Syslogs Sent by Appliances that are not under Reporting or Management** — Some of the units which are no longer managed by Analyzer send syslogs that create NMM files which impact performance. In 7.2, you are notified if this occurs and they can make the unit stop sending syslog messages.
- **Application Level Data Archiving and Aging** — In 7.1 data was not deleted from the application table such as logs and meta data tables, causing the number of rows to grow quickly in the tables, affecting overall performance of the application. In 7.2 the console logs and application meta data tables are aged and archived to fix this issue.
- **Localization** — Support for the Korean language is included in 7.2.
- **Disable Archiving of Syslogs to File System** — Added the option to disable storing of archived syslogs.
- **Reverse DNS Support** — This feature enhances the quality of data by performing a reverse lookup on the private IP addresses (LAN Side) with a missing hostname sent by the firewall. The reverse lookup is performed by logging into the DNS server on the LAN side of the firewall. This functionality requires the Analyzer to be installed on the LAN side of the firewall, to be able to access the DNS Server.
- **Log** Analyzer **Enhancements** — The Log Analyzer interface is customizable to allow expansion and easy distribution of columns for ease of navigation.

Deployment Requirements

SonicWall Analyzer does not require any additional node licenses.

NOTE: Analyzer is not supported on laptops or tablets.

Topics:

Operating System Requirements

SonicWall Analyzer supports the following Microsoft Windows operating systems:

- Windows Server 2012 Standard 64-bit
- Windows Server 2012 R2 Standard 64-bit (English and Japanese language versions)
- Windows Server 2012 R2 Datacenter
- Windows 8.1 64-bit

- Windows 7 64-bit

These Windows systems can either run in physical standalone hardware platforms, or as a virtual machine under Windows Server 2012 Hyper-V or VMware ESXi.

TIP: For best performance and scalability, it is recommended to use a 64-bit Windows operating system. 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 environments. In a Hyper-V virtualized environment, Windows Server is a guest operating system running on Hyper-V. Analyzer is then installed on the Windows Server virtual machine that is layered over Hyper-V.

NOTE: Analyzer is not supported on MS-Windows Server virtual machines running in cloud services, such as Microsoft Azure and Amazon Web Services EC2.

Hardware Requirements for Windows Server

Use the Capacity Calculator 2 to determine the hardware requirements for your deployment.

NOTE: A Windows 64-bit operating system with a RAM of at least 16GB of RAM is highly recommended for better performance of reporting modules.

SonicWall Analyzer Virtual Appliance Requirements

The elements of basic VMware structure must be implemented prior to deploying the SonicWall Analyzer Virtual Appliance. SonicWall Analyzer Virtual Appliance runs on the following VMware platforms:

- ESXi 6.0 and 5.5

Use the following client applications to import the image and configure the virtual settings:

- **VMware vSphere** – Provides infrastructure and application services in a graphical user interface for ESXi, included with ESXi. Allows you to specify Thin or Thick (Flat) provisioning when deploying the Virtual Appliance.
- **VMware vCenter Server** – Centrally manages multiple VMware ESXi environments. Provides Thick provisioning when deploying the Virtual Appliance.

Virtual Appliance Deployment Considerations

Consider the following before deploying the SonicWall Analyzer Virtual Appliance:

- SonicWall Analyzer management is not supported on Apple MacOS.
- All modules are 64-bit.

Use the Capacity Calculator 2 to determine the hardware requirements for your deployment.

- The performance of SonicWall Analyzer Virtual Appliance depends on the underlying hardware. It is highly recommended to dedicate all the resources that are allocated to the Virtual Appliance, especially the hard-disk (datastore). In environments with high volumes of syslogs, you need to dedicate local datastores to the Analyzer Virtual Appliance.
- The 64-bit Virtual Appliances take advantage of the additional RAM available to it. A minimum of 8GB RAM is required. However, at least 16GB of RAM is highly recommended for better performance of reporting modules.
- When using Thick or Flat provisioning as the storage type option, the entire amount of disk space is allocated when you import and deploy the SonicWall Analyzer Virtual Appliance file. When using Thin

provisioning, the initial size is very small and grows dynamically as more disk space is needed by the SonicWall Analyzer Virtual Appliance application, until the maximum size is reached. After being allocated, the size does not shrink if the application space requirements are subsequently reduced.

Additional disk space provided to the SonicWall Analyzer Virtual Appliance in the virtual environment, beyond the respective limits of 250 GB or 950 GB, is not utilized.

MySQL Requirements

Previously, SonicWall Analyzer automatically installed MySQL as part of the base installation package. The SonicWall Analyzer 8.1 upgrade replaces the Infobright with MySQL database formerly used in earlier versions with Infobright with Postgres (IB-PG). The installer will ask if you want to perform the data migration to the new database. Separately installed instances of MySQL are not supported with the SonicWall Analyzer Virtual Appliance.

Browser Requirements

SonicWall Analyzer uses advanced browser technologies such as HTML5, which are supported in most recent browsers. SonicWall recommends using the latest Chrome, Firefox, Internet Explorer, or Safari browsers for administration of the SonicWall Analyzer.

This release supports the following Web browsers:

- Chrome 42.0 and higher (recommended browser for dashboard real-time graphics display)
- Firefox 37.0 and higher
- Internet Explorer 10.0 and higher (do not use compatibility mode)

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

NOTE: Turn off Compatibility Mode when accessing Analyzer sites with Internet Explorer. For more information, see the Knowledge Base article located at:
https://support.sonicwall.com/sonicwall-gms/kb/sw14003

Network Requirements

To complete the Analyzer deployment process documented in this guide, the following network requirements must be met:

- The SonicWall Analyzer server must have access to the Internet
- The SonicWall Analyzer server must have a static IP address
- The 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.

NOTE: Depending on the configuration of 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 could vary.

SonicWall Appliance and Firmware Support

SonicWall Analyzer supports the following SonicWall appliances and firmware versions:

Component requirements

SonicWall Platforms	SonicWall Firmware Version
Network Security Appliance	
SuperMassive 10000 Series	SonicOS 6.0 or newer • **NOTE**: Only partial reporting support is currently available. Contact your SonicWall Sales representative through https://support.software.dell.com/ for more information.
SuperMassive 9000 Series	SonicOS 6.1 or newer
NSA Series	SonicOS 5.0 or newer
TZ and TZ Wireless Series	SonicOS 5.0 or newer
SonicWall SOHO and SOHO Wireless	SonicOS 6.2.5 or newer
Secure Mobile Access	
SMA 100 Series (SMA 200/400)	SMA 8.1 or newer
SRA/SSL-VPN Series	SSL-VPN 2.0 or newer (management) SSL-VPN 2.1 or newer (management and reporting)
E-Class SRA Series	E-Class SRA 9.0 or newer
SMA 1000 Series (SMA 6200/7200)	SMA 10.7.2 or newer
Email Security/Anti-Spam	
Email Security Series	Email Security 7.2 or newer (management only)

NOTE: Appliances running firmware newer than this SonicWall Analyzer release can still generate reports. However, the new features in the firmware release will be supported in an upcoming release of Analyzer.

NOTE: Legacy SonicWall XPRS/XPRS2, SonicWall SOHO2, SonicWall Tele2, and SonicWall Pro/Pro-VX models are not supported for SonicWall Analyzer reporting. Appliances running SonicWall legacy firmware including SonicOS Standard 1.x and SonicWall legacy firmware 6.x.x.x are not supported for SonicWall Analyzer reporting.

NOTE: SonicWall Analyzer can be connected to SSL-VPN 2000 and 4000 appliances. Use the **Log > View Log** page to set up the Analyzer connection (in addition to the configuration changes made on the Analyzer). In SonicWall SRA SSL-VPN 5.5 or later firmware versions, a **Log > Analyzer** page is provided for configuration of Analyzer settings.

SonicWall Analyzer Installation

Analyzer 8.3 can be installed as a fresh install or as an upgrade from Analyzer 8.2. If you wish to perform a fresh install of Analyzer 8.3, refer to the *SonicWall Analyzer Getting Started Guide* that relates to your Analyzer deployment.

Previously, Analyzer automatically installed MySQL as part of the base installation package. The Analyzer 8.3 upgrade replaces the Infobright with MySQL database formerly used in earlier versions with Infobright with Postgres (IB-PG). The installer will ask if you want to perform the data migration to the new database. Separately installed instances of MySQL are not supported with Analyzer.

All software components related to SonicWall Analyzer and SonicWall Global Management System (GMS), including the 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 *SonicWall Analyzer Getting Started Guide*.

License and Registration Requirements

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

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

On SonicWall appliances that send reporting data to the Analyzer, SonicWall Analyzer is licensed and activated separately from the SonicWall appliances. MySonicWall provides a way to associate SonicWall appliances with the Analyzer instance installed on the Windows system. Licensing your SonicWall Analyzer application on a 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. After 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. After 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

SonicWall Analyzer includes two separate management interfaces:

- **SonicWall Universal Management Host (UMH) System Management Interface** – Used for system management of the host server, 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/`

- **SonicWall Analyzer Management Interface** – Used to access the SonicWall Analyzer application that runs on the system. This interface is used to configure and view SonicWall Analyzer reporting on SonicWall

appliances and for configuring Analyzer administrative settings. Access the 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 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 **Switch** 

in the top right corner of the page.

Log In to Analyzer

After registering your SonicWall Analyzer product, to log in 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 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, Traditional Chinese, Korean, and Portuguese.

To login to Analyzer,

1 Enter the SonicWall user ID (default: admin) and password (default: password). Select **Local Domain** as the domain (default).

2 Click **Submit**. The SonicWall Analyzer management interface displays.

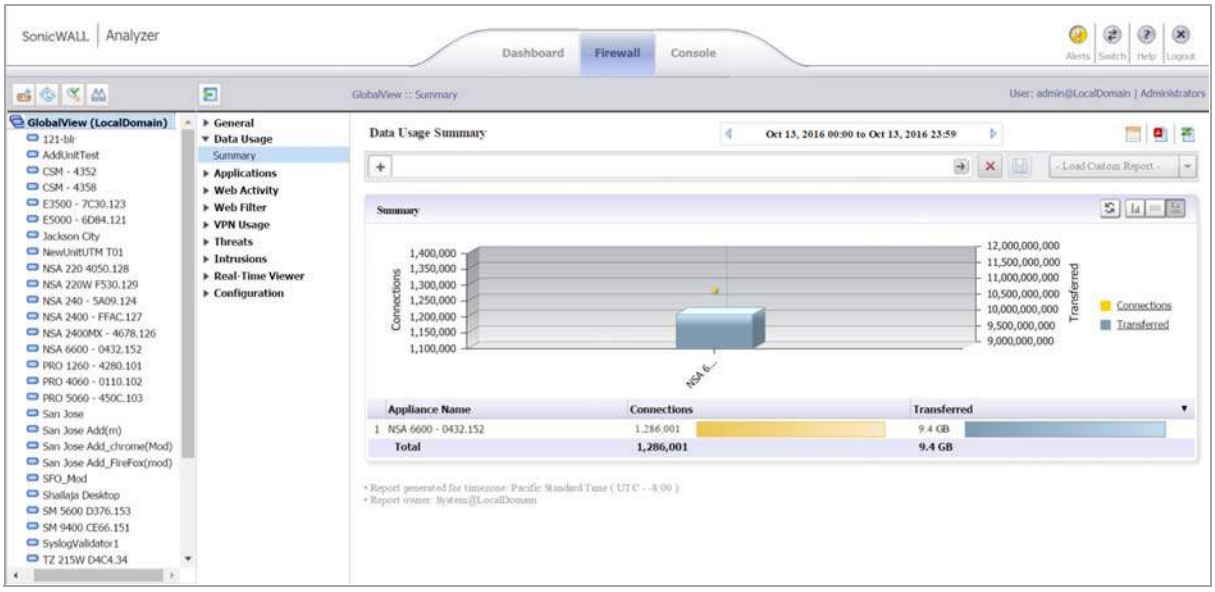
> **NOTE:** For more information on installation, login procedures, and registration of your SonicWall Analyzer installation, refer to the appropriate Getting Started Guide, available at: https://support.sonicwall.com/sonicwall-analyzer/analyzer/technical-documents

Navigating the Analyzer User Interface

This section describes the Firewall, SMA, and Console panels in the SonicWall Analyzer user interface. For information about the Dashboard panel, see the Using the Universal Scheduled Reports Application on page 31.

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.



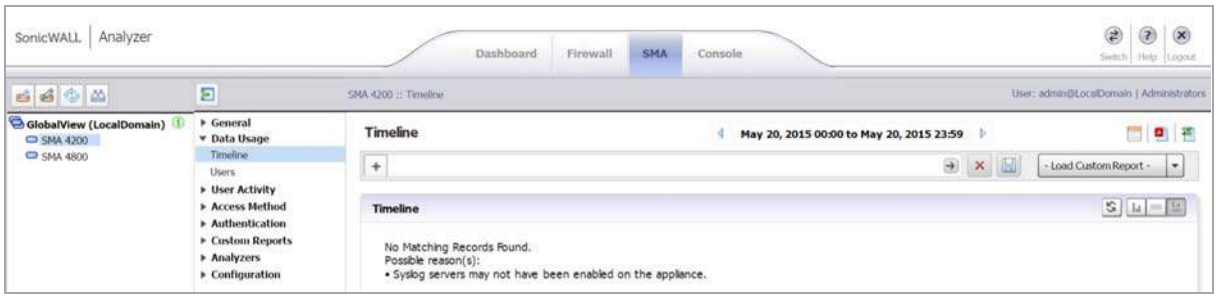
From the Firewall Panel, you can view the following for connected SonicWall appliances:

- 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.

SMA Panel

The SMA 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 SMA Panel, click the **SMA** tab at the top of the Analyzer user interface.

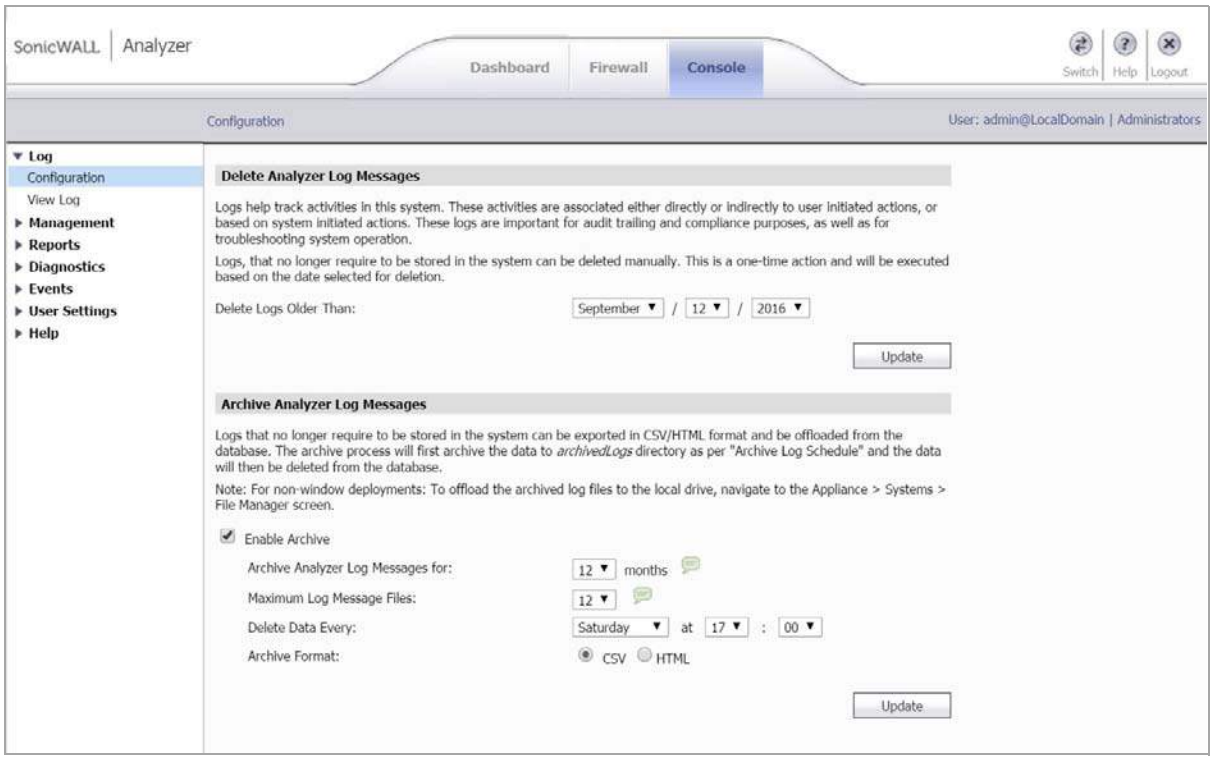


From the SMA Panel, you can view the following for connected SonicWall SSL VPN appliances:

- 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.

Console Panel

The Console Panel is used to configure 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 SonicWall Analyzer user interface.



From the Console Panel, you can do the following:

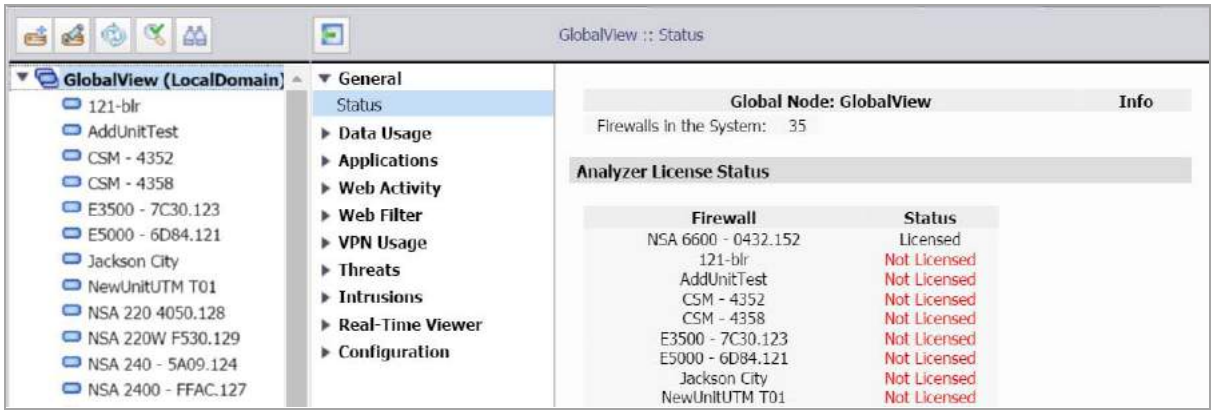
- Change the Analyzer password, adjust the amount of inactive time before you are automatically logged out of Analyzer, and set the maximum number of rows displayed on paginated screens.
- Configure Web sites and Web users that are excluded from Web usage reports.
- View the Analyzer log and delete old log messages. The Analyzer log contains information on alert notifications, failed Analyzer login attempts, and other events that apply to 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

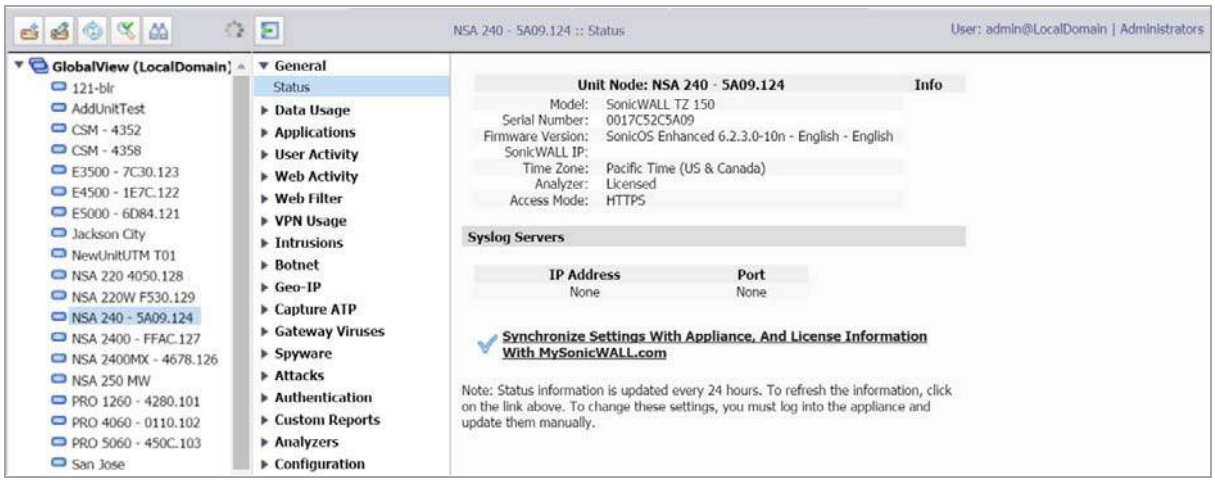
SonicWall Analyzer allows you to view status and reports for all appliances at once using **GlobalView**, or for a single unit at a time with the **Unit** view. Analyzer provides status information on the **General > Status** page of the Firewall or SMA panel.

GlobalView is a grouping of all the appliances you are monitoring with Analyzer. From the GlobalView of the Firewall or SMA 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** or **SMA** 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.

Icon meaning

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

Using the Analyzer TreeControl Menu

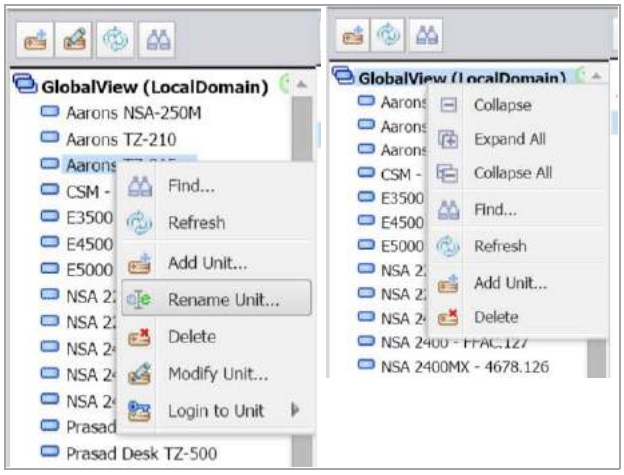
This section describes the content of the TreeControl menu within the SonicWall Analyzer user interface.

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
- SMA and EX-Series SMA 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.
- **Add Unit** – Add a new unit to the Analyzer view. Requires unit IP and login information.
- **Rename Unit** – (unit view only) Renames the selected SonicWall appliance.
- **Delete** – Delete the selected unit
- **Modify Unit** – (unit view only) Change basic settings for the selected unit, including unit name, IP and login information, and serial number.
- **Login to Unit** – (unit view only) Log in to the selected unit using HTTPS protocols.

2

Provisioning and Adding SonicWall Appliances

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

This chapter contains the following sections:

Provisioning SonicWall Appliances

This section describes how to configure SonicWall appliances to support SonicWall Analyzer.

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

Provisioning a SonicWall Firewall Appliance

To provision a SonicWall firewall appliance for SonicWall Analyzer, complete the following steps:

1. Log in to the firewall appliance. Navigate to the **Log > Syslog** page.
2. In Syslog Servers, click **Add**.
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.
4. Navigate to the **System > Time** page, and enable **Display UTC in logs** (instead of local time).

Provisioning a SonicWall SMA SMB Appliance

To provision a SonicWall SMA SMB appliance for SonicWall Analyzer, complete the following steps:

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

2 In Analyzer Settings, click **Enable** Analyzer.

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

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

Provisioning a 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 > Configure Centralized Management** screen, and enter the Analyzer IP address and port number to start sending syslog.

Adding SonicWall Appliances to Analyzer

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

SonicWall Analyzer communicates with SonicWall appliances using HTTPS protocol.

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 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 to the following sections:

- Adding SonicWall Appliances on page 26
- Modifying SonicWall Appliance Settings on page 28
- Deleting SonicWall Appliances from Analyzer on page 28

Adding SonicWall Appliances

To add a SonicWall appliance using the SonicWall Analyzer management interface, complete the following steps:

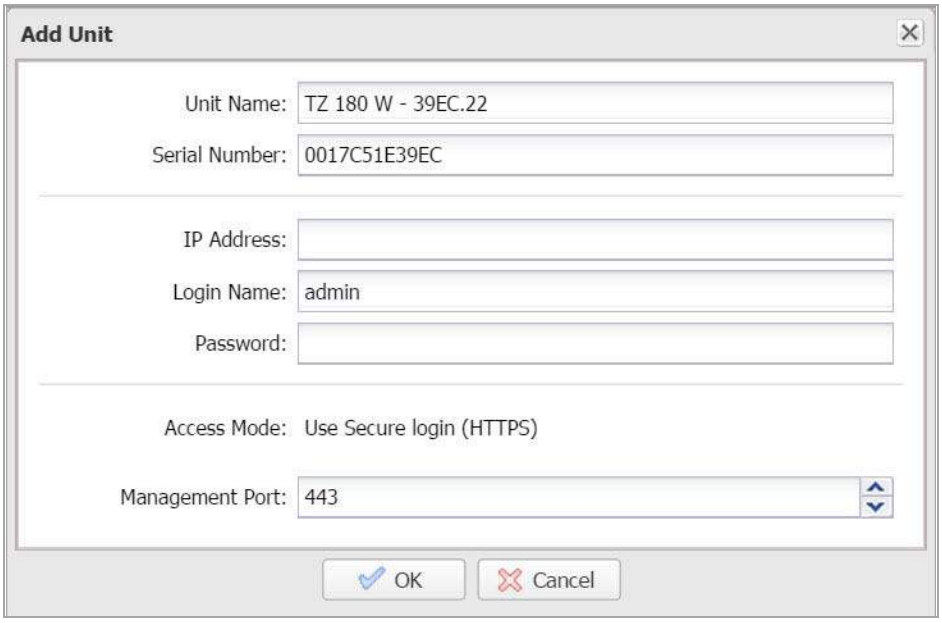
1 Click the appliance tab that corresponds to the type of appliance that you want to add:

- Firewall
- SMA

2 Expand the SonicWall Analyzer tree and select the group to which you want to add the SonicWall appliance. Then, right-click the group and select **Add Unit** from the pop-up menu. To not specify a group,

right-click an open area in the left pane (TreeControl pane) of the SonicWall Analyzer management interface and select **Add Unit** or click the **Add Unit** icon in the tool bar.

The Add Unit dialog box appears:



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

4 Enter the serial number of the SonicWall appliance in the **Serial Number** field.

5 Enter the IP address of the SonicWall appliance in the **IP Address** field.

6 Enter the administrator login name for the SonicWall appliance in the **Login Name** field.

7 Enter the password used to access the SonicWall appliance in the **Password** field.

For Access Mode, select from the following:

1 The SonicWall appliances are connected with HTTPS by default.

2 Enter the port used to connect to the SonicWall appliance in the **Management Port** field (default port for is HTTPS: 443).

3 Click **OK**. The new SonicWall appliance appears in the Analyzer management interface. It has a yellow icon that indicates it has not yet been successfully acquired.

4 Analyzer then attempts to set up an HTTPS connection to access the appliance. Analyzer then reads the appliance configuration and acquires the SonicWall appliance for reporting. This takes a few minutes.

NOTE: After the 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 SonicWall Appliance Settings

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

To modify a SonicWall appliance, complete 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 Adding SonicWall Appliances to Analyzer on page 26.

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

Deleting SonicWall Appliances from Analyzer

To delete a SonicWall appliance from SonicWall Analyzer, complete the following steps:

1 Right-click on a SonicWall appliance in the left pane and select **Delete** from the pop-up menu.

2 In the message that displays, click **Yes**. The SonicWall appliance is deleted from SonicWall Analyzer.

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

Part 2

Dashboard

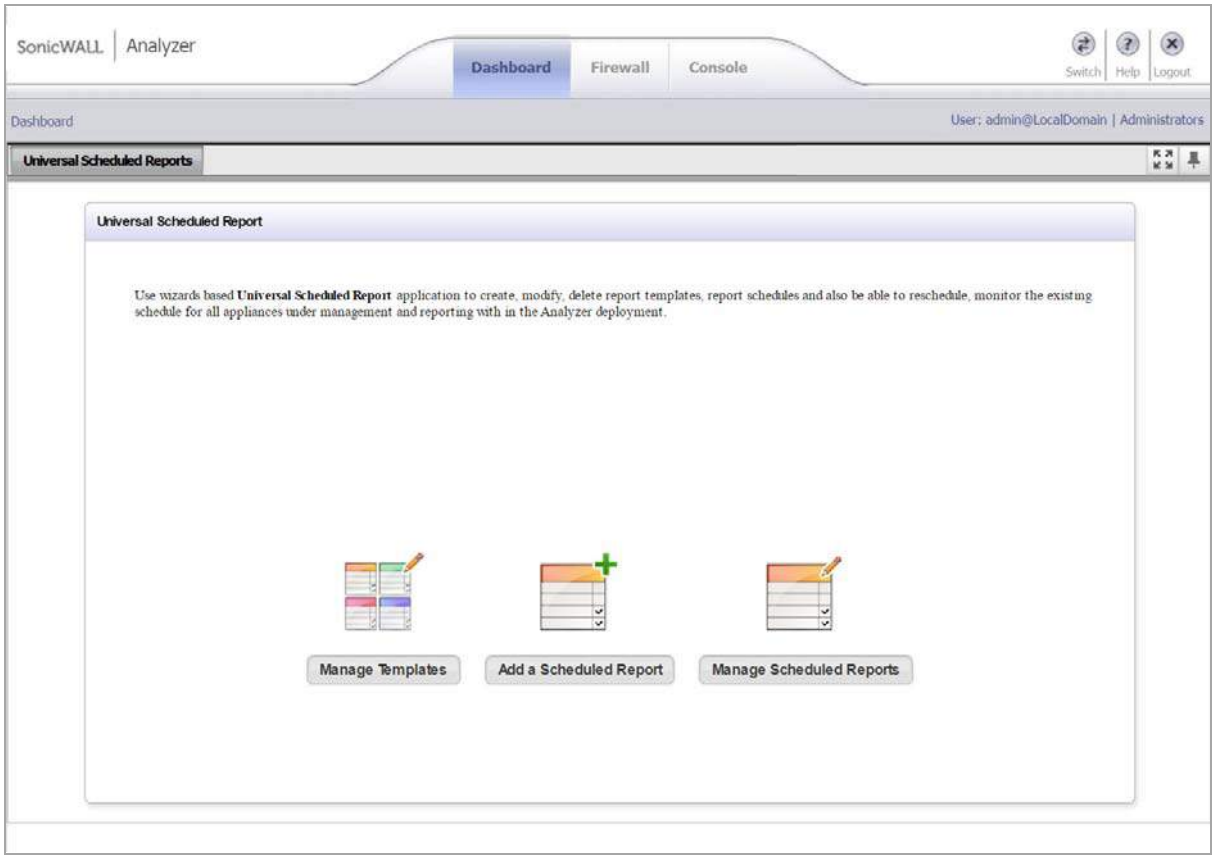
- Using the Dashboard Panel

Using the Dashboard Panel

This chapter provides an overview of the SonicWall Analyzer Dashboard.

See the following sections:

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. You can lock the control bar by clicking on the “pin the control bar” icon.

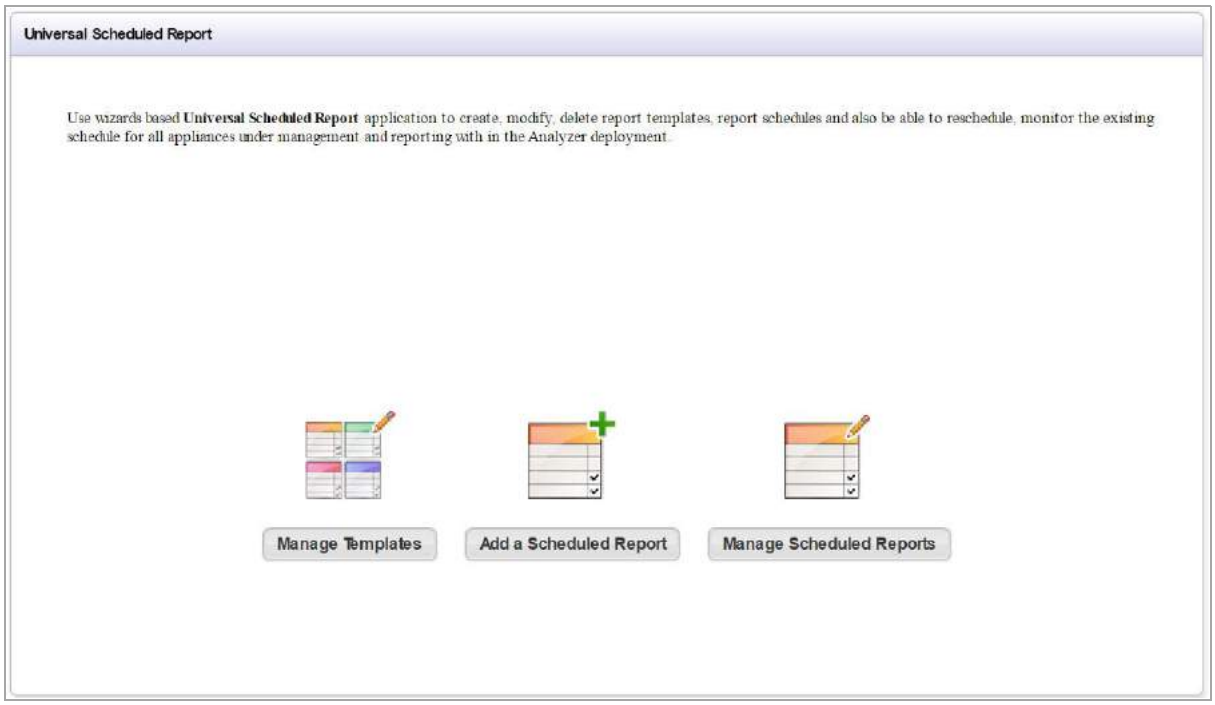


The Dashboard control bar provides the following components:

- **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 SonicWall Analyzer product. It provides management interfaces to let you 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 you 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 on page 31
- Adding a Scheduled Report Component on page 37
- Managing the Scheduled Reports Component on page 49

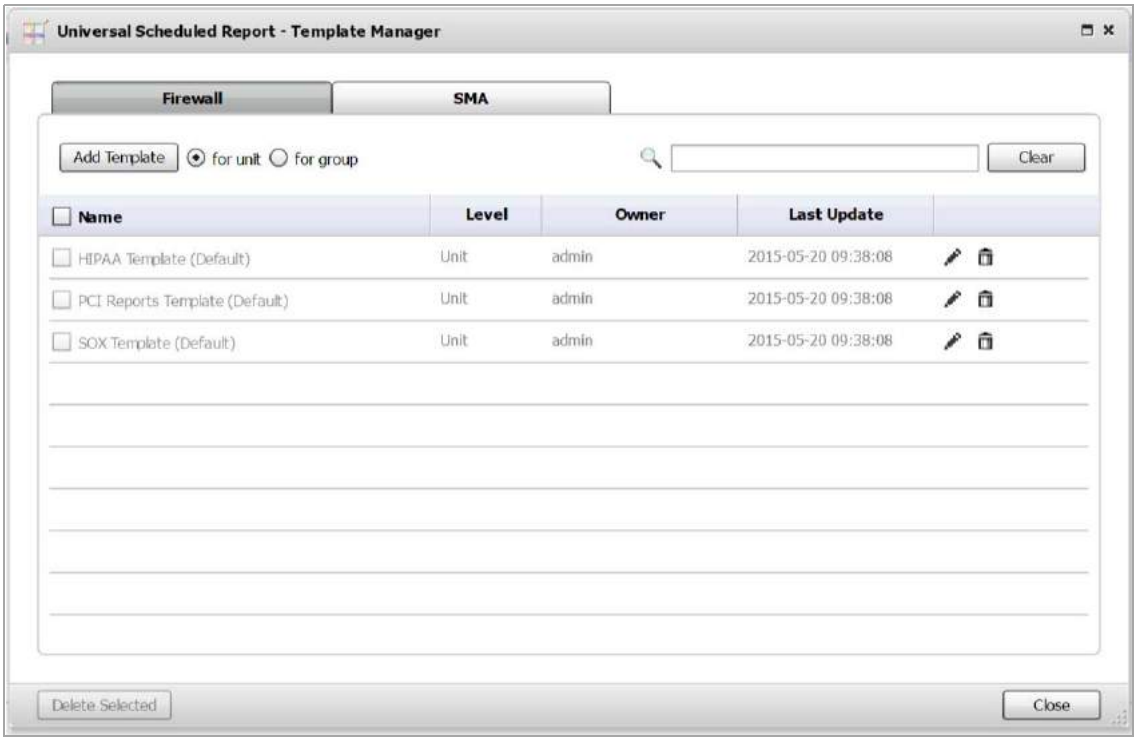
Using the Manage Templates Component

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 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 or higher) 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

To add a template using the Template Manager, complete the following steps:

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



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

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

4 Click **Add Template**.

5 Enter a name for your template.

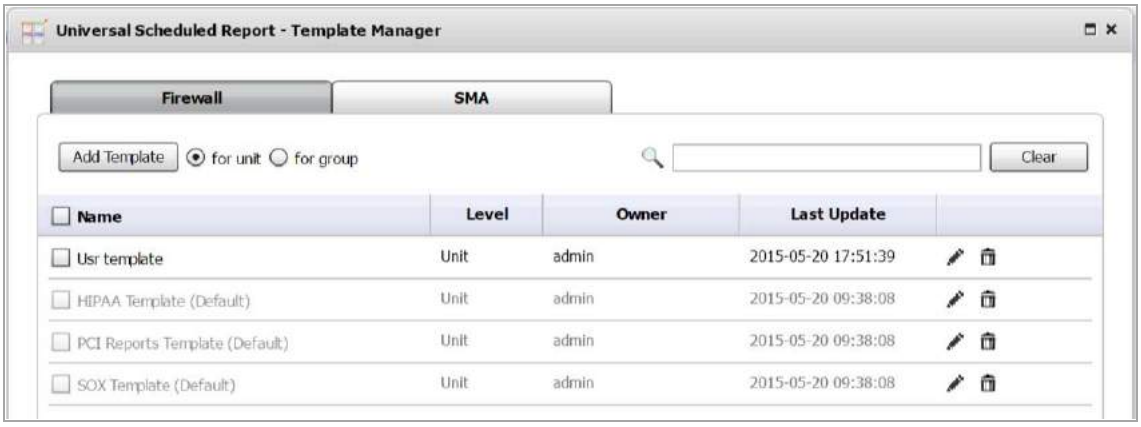
6 **Visible To Non-Administrators** is disabled by default, select the check box to enable this option. This allows the end users to view list of all the report templates at a read-only level.

7 Select the check box next to the **Reports** you wish to use for this template.

8 Select the check box next to the **Policies** you wish to use for this template.

9 Click **Add**.

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 > Manage Templates** allows you to filter the template list by Name, Level, Owner, and Last Update.

To use the search option to find and edit an existing template, complete the following steps:

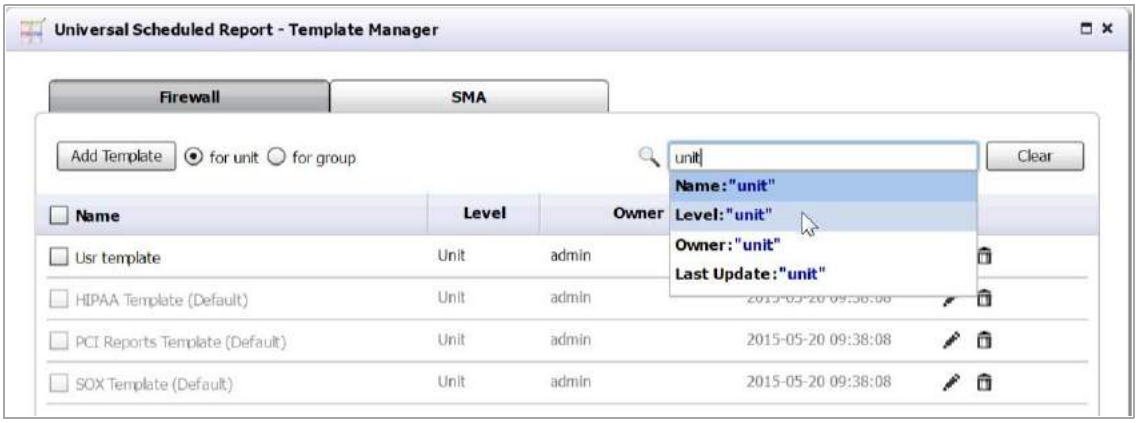
Searching for an Existing Template

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

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

A drop-down appears under the search text field.

3 Select a filter for your search criteria by clicking **Name**, **Level**, **Owner**, or **Last Update** from the search drop-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 **Clear**.

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).

To edit an existing template, complete the following steps:

1 Click the **Edit** icon for the report you wish to edit.

The Edit Template window displays.

2 Edit the name for your template.

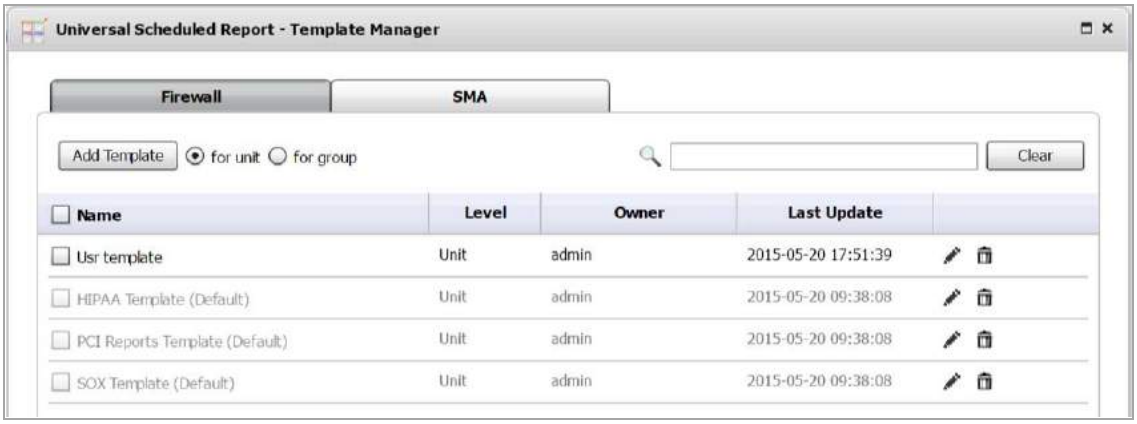
3 **Visible To Non-Administrators** is disabled by default, select the check box to enable this option. This allows the end users to view list of all the report templates at a read-only level.

4 Select the check box next to the **Reports** you wish to use for this template.

5 Select the check box next to the **Polices** you wish to use for this template.

6 Click **Update**.

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 section Searching for an Existing Template on page 34 to search for templates to delete.

To delete a Universal Scheduled Report Template(s), complete the following steps:

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

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

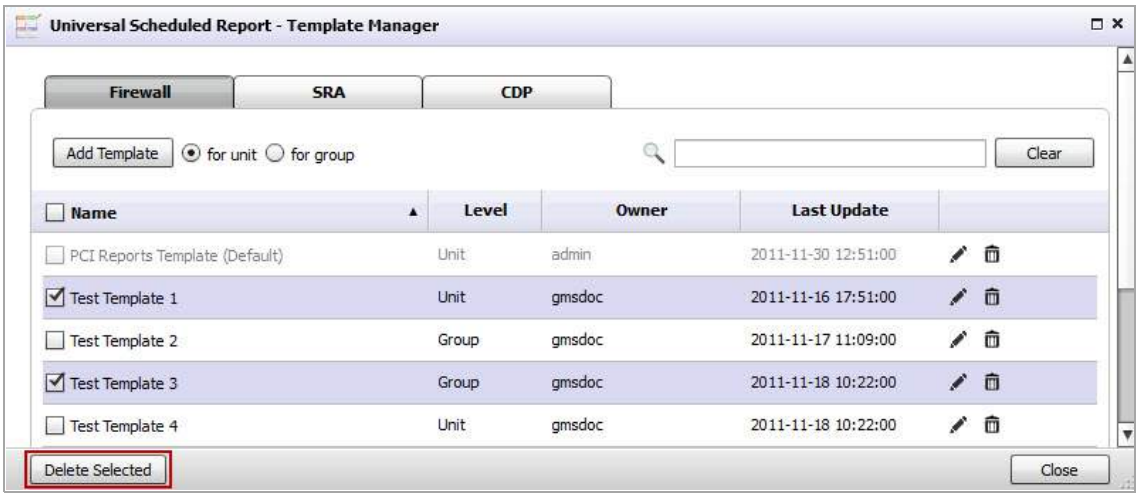
2 Click the **Trash** icon for the template you wish to delete from the Template Manager list.

Deleting Multiple Templates

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

2 Click the check boxes for the templates you wish to delete.

3 Click **Delete Selected**. This button is grayed out by default until a check box is selected.

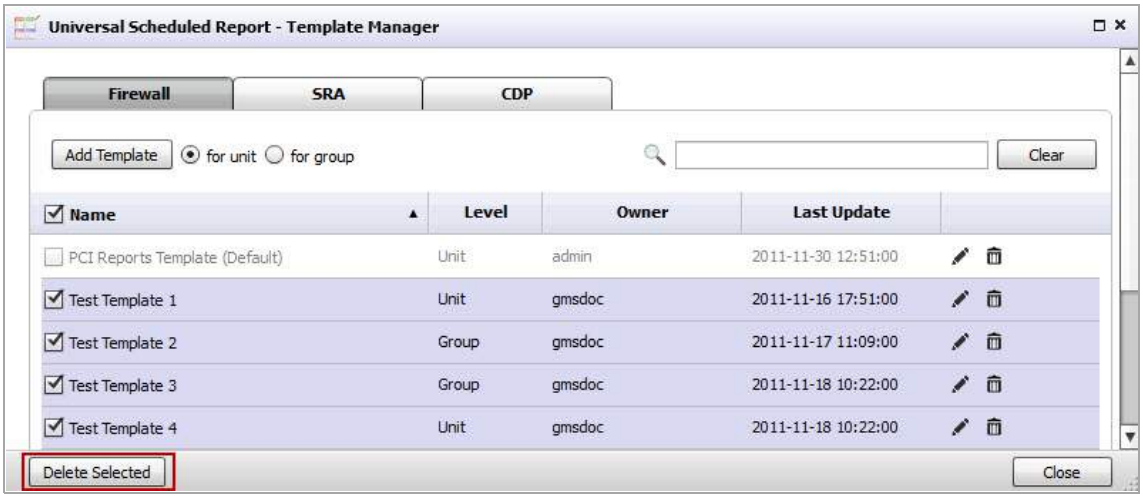


Deleting all Templates

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

2 Select the **Name** check box, this selects all templates in the list.

3 Click **Delete Selected**. This button is grayed out by default until a check box 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 section Using the Manage Templates Component on page 31, 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 five email addresses can be added for a single report). This section contains the following subsections:

Searching for a Group or Device

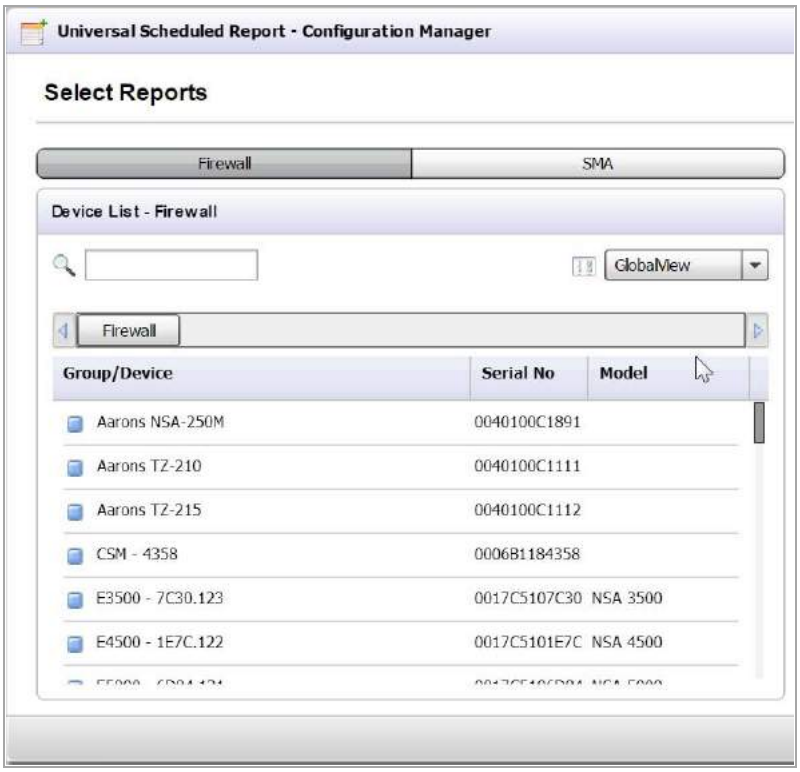
The Search option allows you to filter the Group/Device list by manually entering a device in the search text field and selecting it from the search drop-down list. You can further filter the Group/Device list by clicking the View drop-down and selecting a view type. The following example guides you 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.

1 Navigate to **Universal Scheduled Reports > Add A Scheduled Report**.

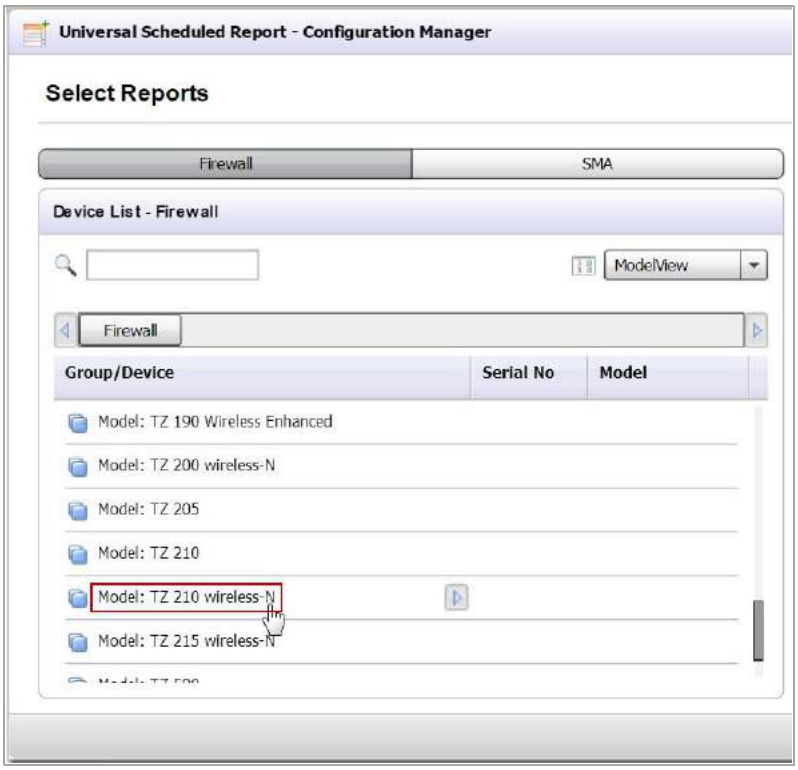
NOTE: The Monitor tab is only available for SonicWall GMS.



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

3 Click the **View** drop-down, then select a view type from the list. In this example, we are selecting **ModelView** (GlobalView is selected by default), because we are searching for an exact appliance model. You can also filter the Device List by FirmwareView, or GlobalView.

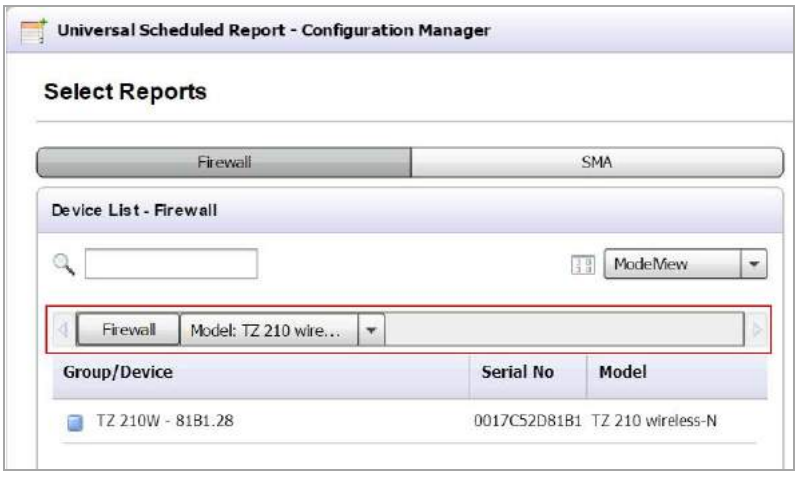
The Device List now displays all the appliance models.



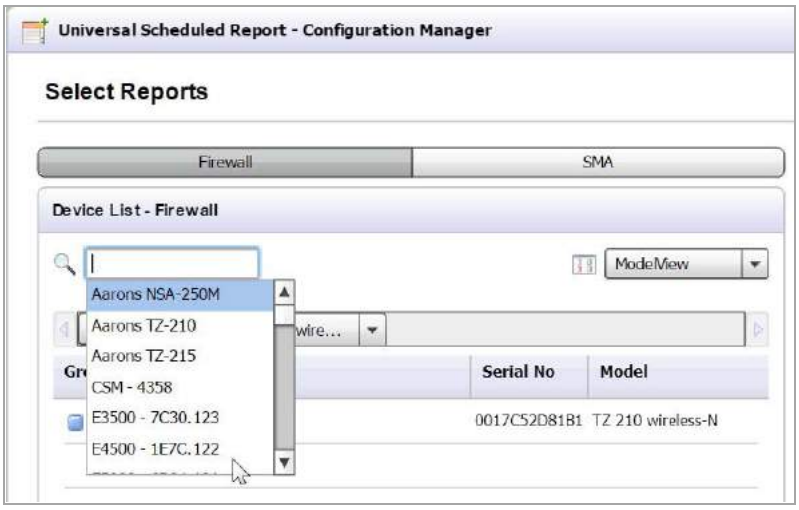
4 Select the **Model: TZ 210 wireless-N**.

A list of devices for that appliance model displays.

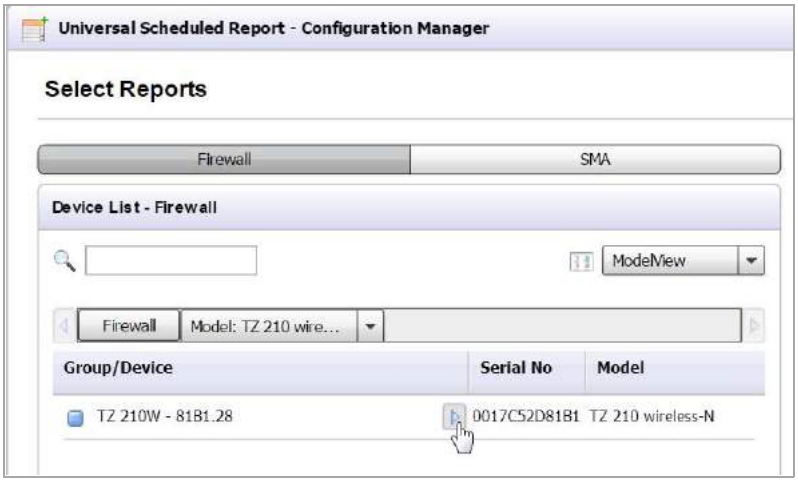
NOTE: Notice that the search history bar populates each time you filter the list. You can use this to navigate back to previous search results.



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



5 Click the **Arrow** icon to schedule a report for that appliance. Refer to Creating a Universal Scheduled Report on page 40 for configuration procedures.



Creating a Universal Scheduled Report

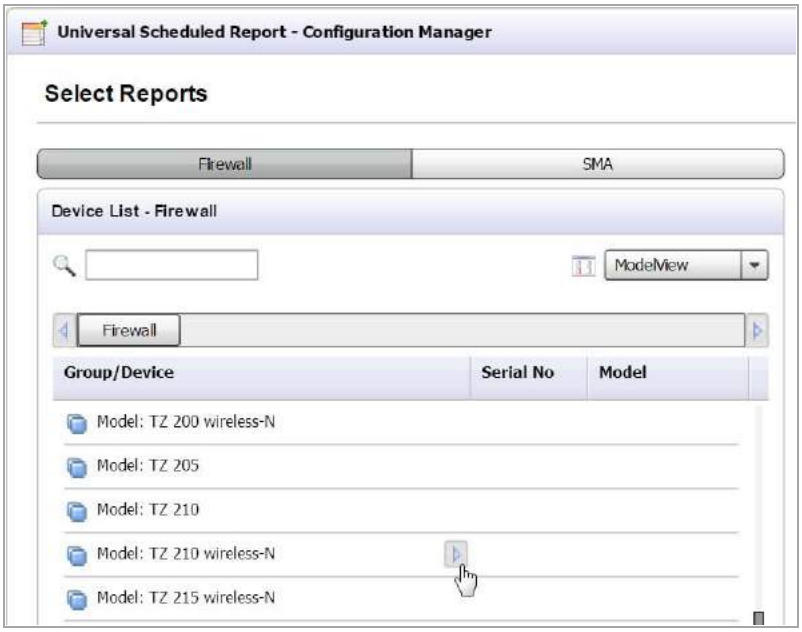
The Universal Scheduled Report - Configuration Manager allows you to create a single report for multiple appliance models/devices at a group and unit level. The following example guides you through the report configuration process, including: Selecting Reports, General Information, and Theme Information, 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 SMA devices (unit level).

Selecting Reports

1 Navigate to **Dashboard > Universal Scheduled Report > Add a Scheduled Report**.

NOTE: The Monitor tab is only available for SonicWall GMS.

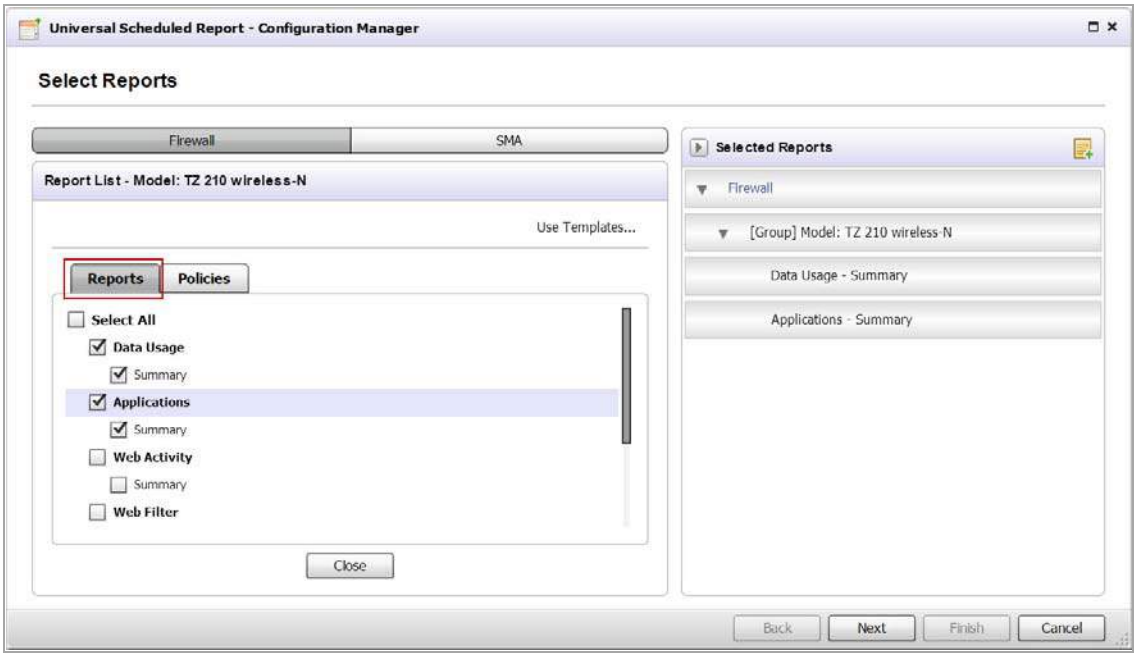


2 Select the **Firewall** tab, located at the top of the Configuration Manager window.

3 Search for the TZ 210 wireless-N model group. Refer to steps 1-3 in the section Searching for a Group or Device on page 38.

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

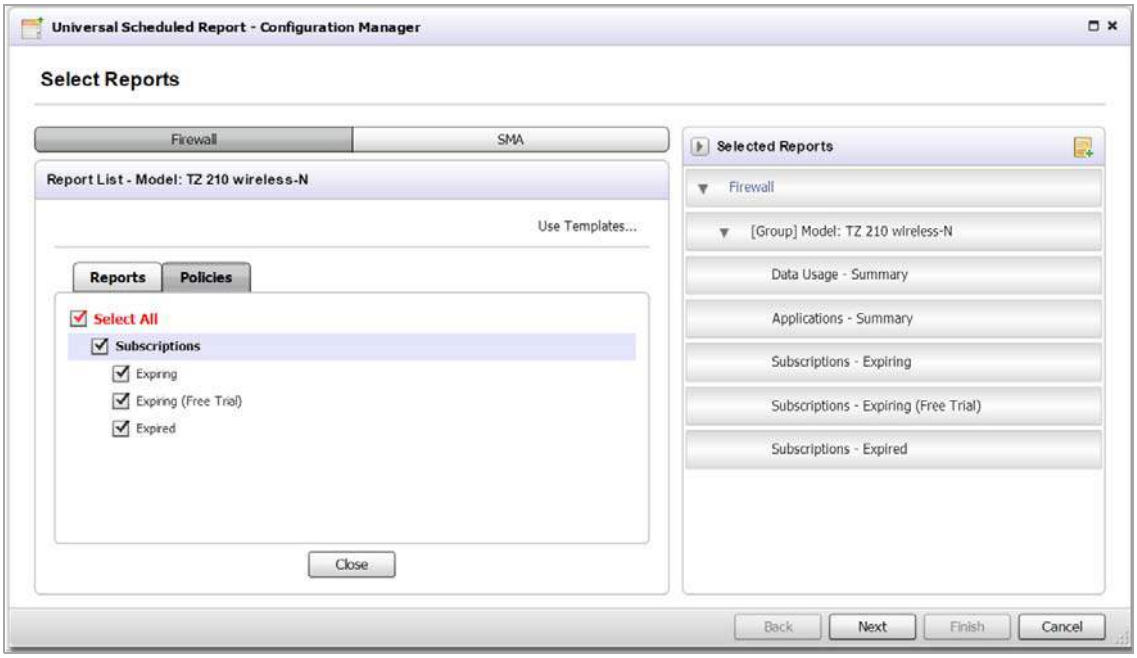
The Reports tab displays in the Reports List.



5 Click the **Reports** tab, then select the check boxes 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.

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



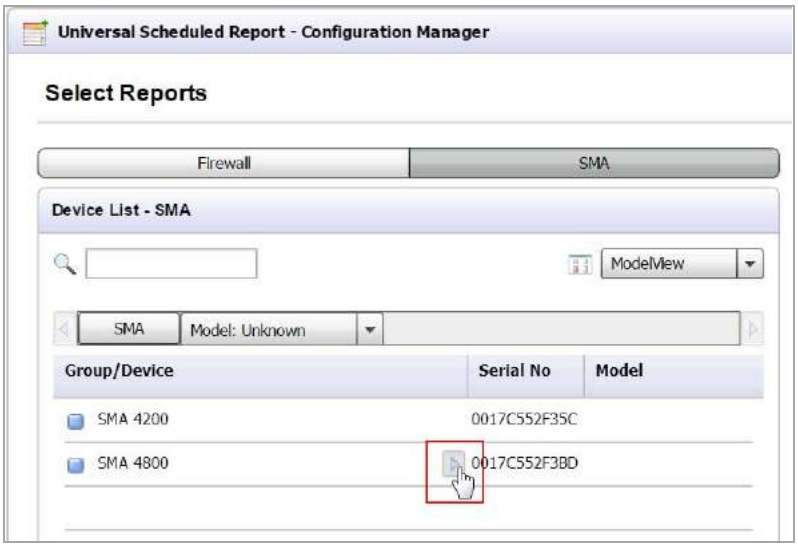
The reports for the Firewall model group are now selected, next is choosing the reports for the SMA device.

7 Select the **SMA** tab.

The SMA models display in the Device List.

8 Click the **Model: SMA 4800**.

The Device List displays all the SMA 4800 devices.

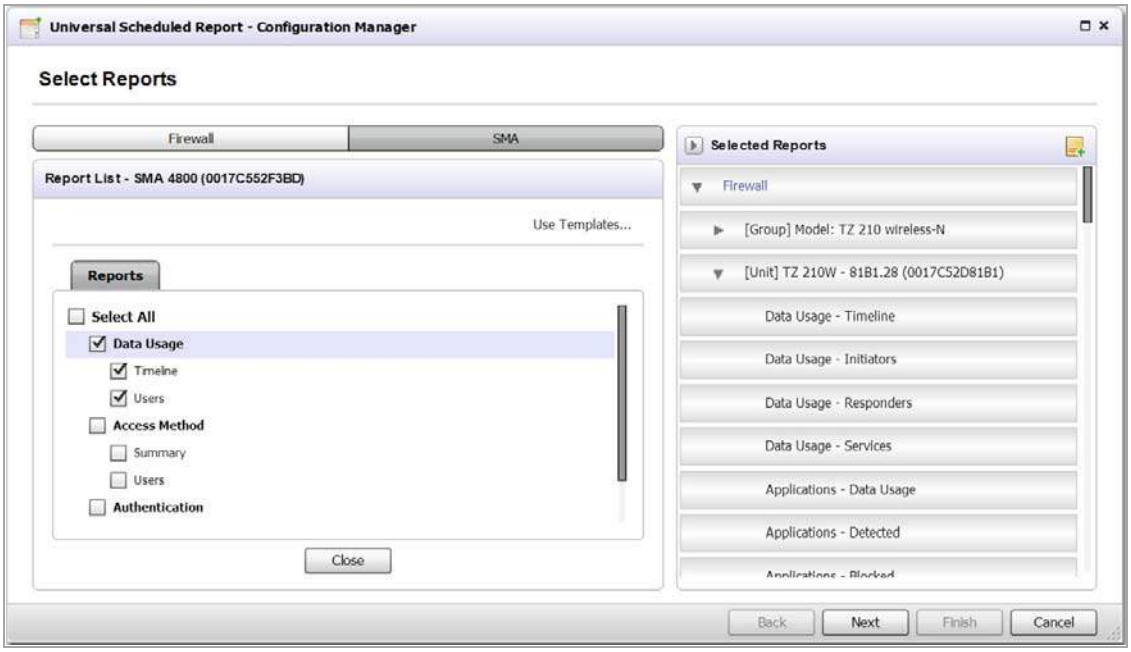


9 Click the **Arrow** icon for the SMA 4800.

The Reports window displays in the Reports List.

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

NOTE: The SMA only offers a Reports tab (no Policies tab).

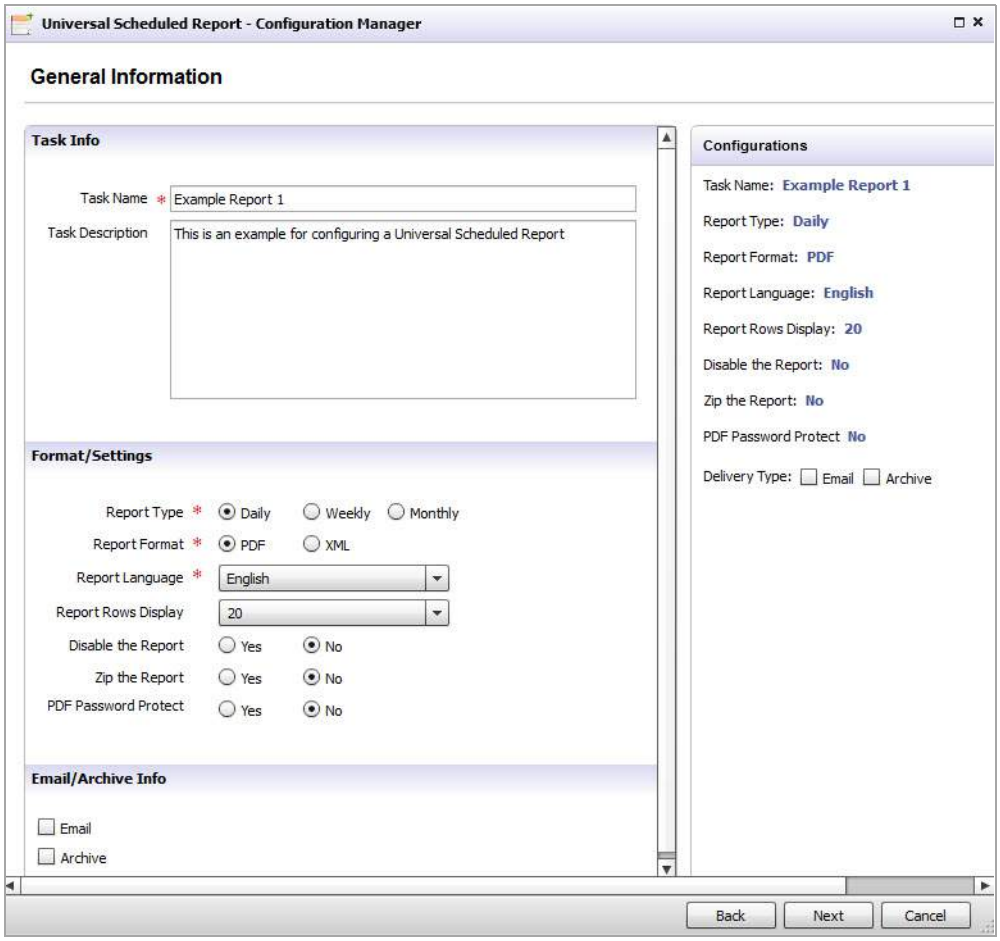


11 Click **Next**.

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.



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

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 is 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), Korean, Spanish, or Portuguese
- Report Rows Display: 5, 10, 20, 50, 100, 250, 500, 750, 1000, 1500, or 2000
- 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)

14 Click the archive check box to save a PDF report to a new folder.

15 Complete the following in the **Email / Archive Info** panel:

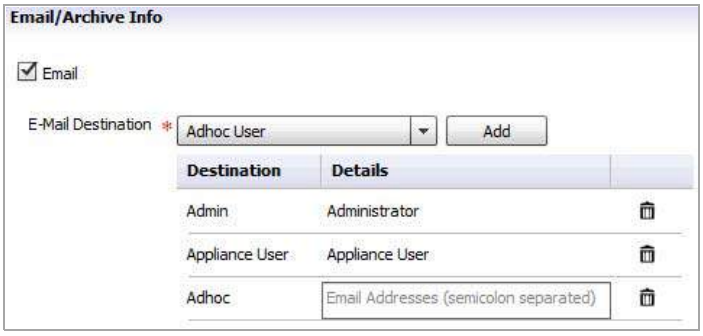
16 Click the E-mail check box to send a PDF report to an email account or alias.

The Email configuration options display.

17 Click the **E-Mail Destination** drop-down, then select an **Administrator** or **Adhoc User**.

18 Click **Add** after each selected destination.

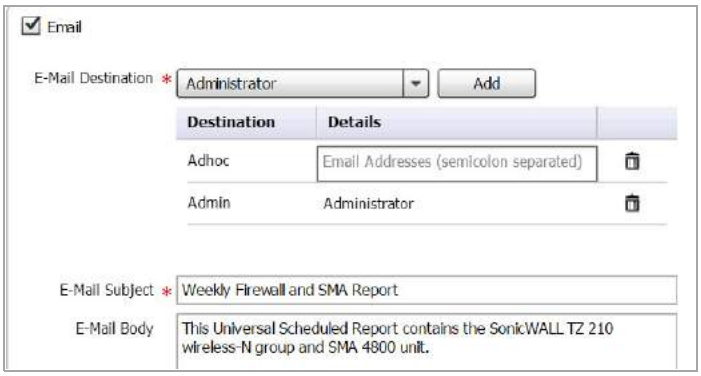
The E-Mail Destination populates in the list.



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

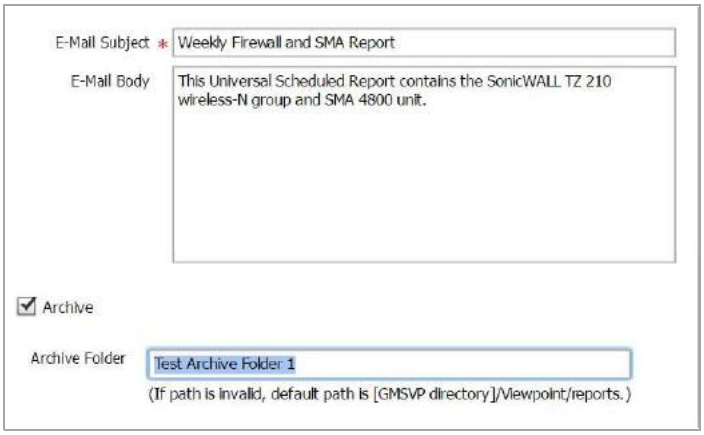
19 Enter the E-mail Subject: **Weekly Firewall and SMA Report**

20 Enter the E-Mail Body: **This Universal Scheduled Report contains the SonicWall TZ 210 wireless-N group and SMA 4800 unit**



21 Click the **Archive** check box to save a PDF report to a new folder.

22 Archive Folder: **Test Archive Folder 1**

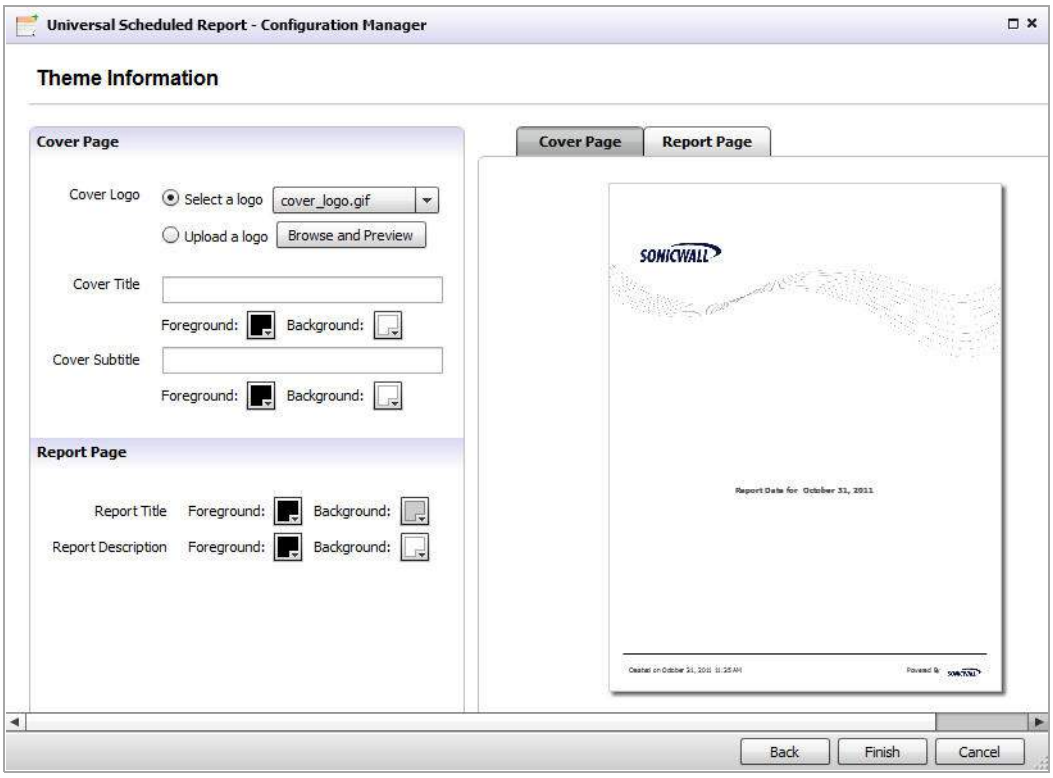


23 Click **Next**.

Theme Information

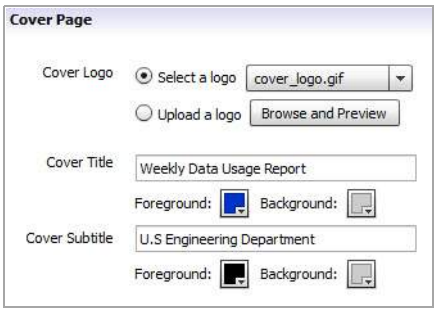
The Theme Information page displays. If **XML** is selected from the General Information page, the Theme Information page is NOT displayed.

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.



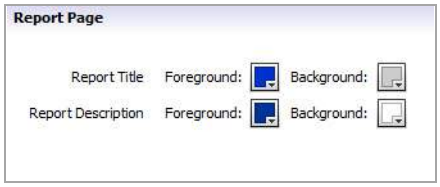
24 Select / Enter the following in the **Cover Page** panel:

- Cover Logo: Select a logo (click the drop-down and select a cover logo image) or Upload a logo (click **Browse** and **Preview** 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

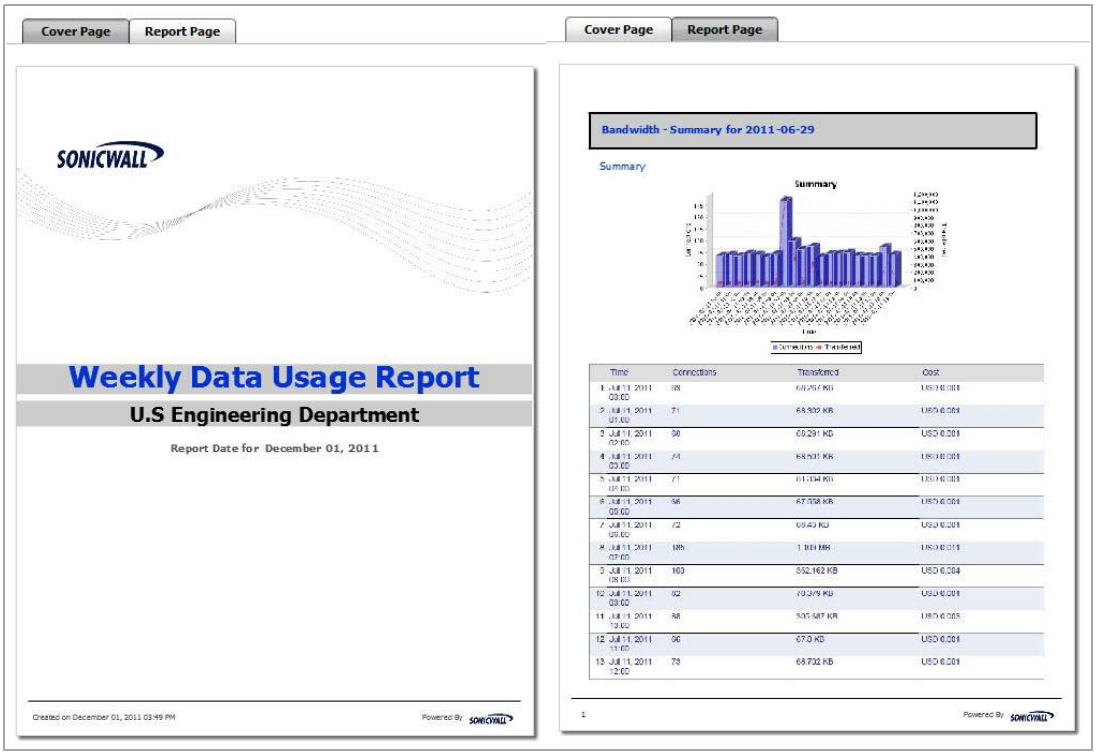


25 Select or enter the following in the **Report Page** panel:

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



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



27 Click **Next** to manage permissions. Continue to the next step.

OR

Click **Finish** to complete the report. The report is now scheduled and can be found in the **Universal Scheduled Reports > Manage Scheduled Reports** page.

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.

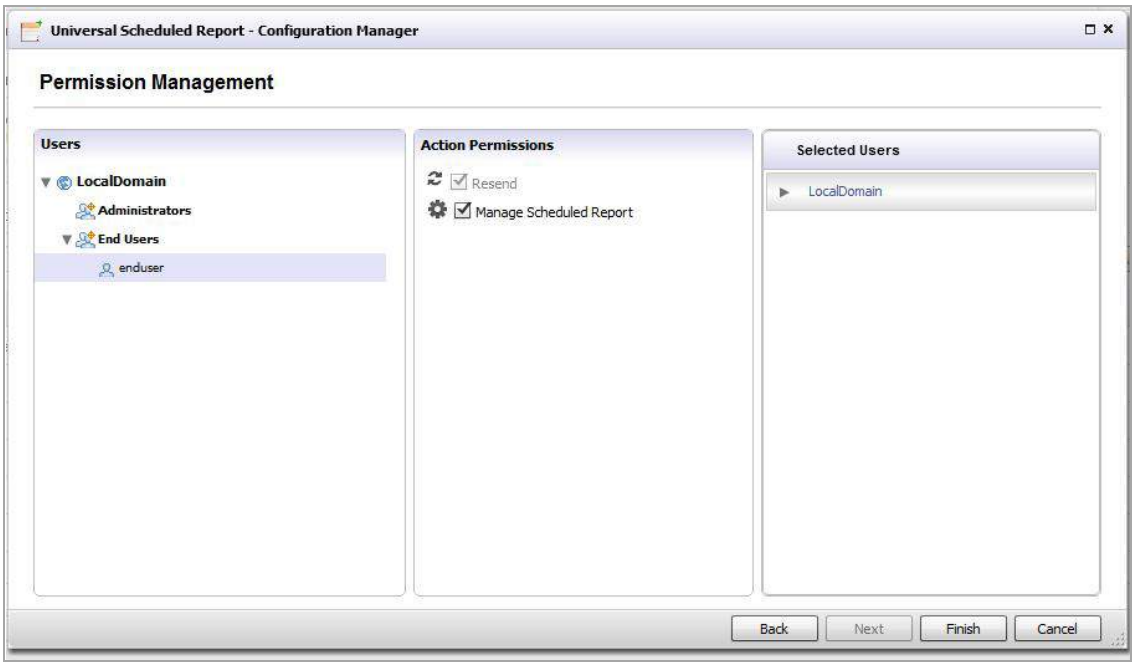
28 In the **Users** panel, select users that you want to give permission to resend or manage this scheduled report. The selected users populate in the **Selected Users** panel.

NOTE: Only the Schedule Report Creator can assign permission resend and manage privileges to other users.—If the Scheduled Report contains reports for multiple units and multiple reports, then the grantee should have permissions to the units and reports which are included for the scheduled report.—Users under the Administrators group have access to all the schedule reports.

29 In the **Action Permissions** panel, click the check box for the type of permissions to give the selected user:

- **Resend** — users with permissions to resend can only run the report.

- **Manage Scheduled Report** — users with manage permissions can run and edit (manage) the report.



30 Click **Finish** to complete the report. The report is now scheduled and can be found in the **Universal Scheduled Reports > Manage Scheduled Reports** page.

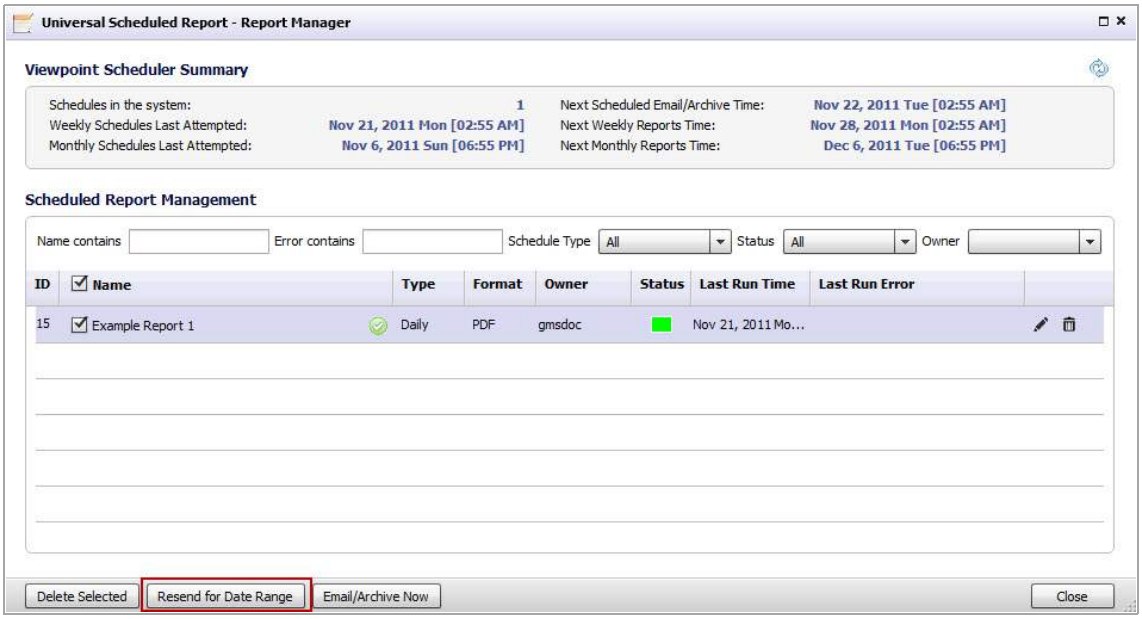
Managing the Scheduled Reports Component

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

To resend a scheduled report, complete the following steps:

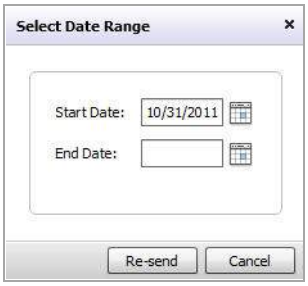
1 Navigate to the **Universal Scheduled Reports > Manage Scheduled Reports** page.



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

3 Click **Resend for Data Range**.

The Select Data Range pop-up window displays.



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

5 Click **Re-send**.

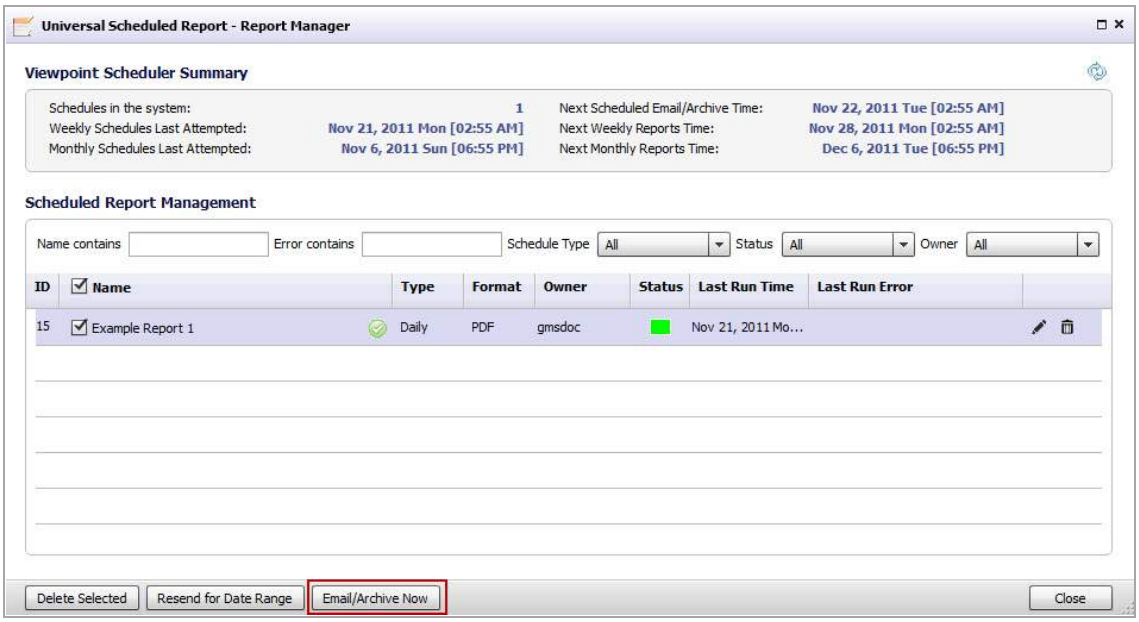
The Info pop-up window displays, confirming the schedule resend is complete.

6 Click **OK**.

Emailing/Archiving Now

To Email/Archive a Universal Scheduled Report before its scheduled sending date, complete the following steps:

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



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

3 Select the check box next to the report name.

4 Click E**mail/Archive Now**.

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

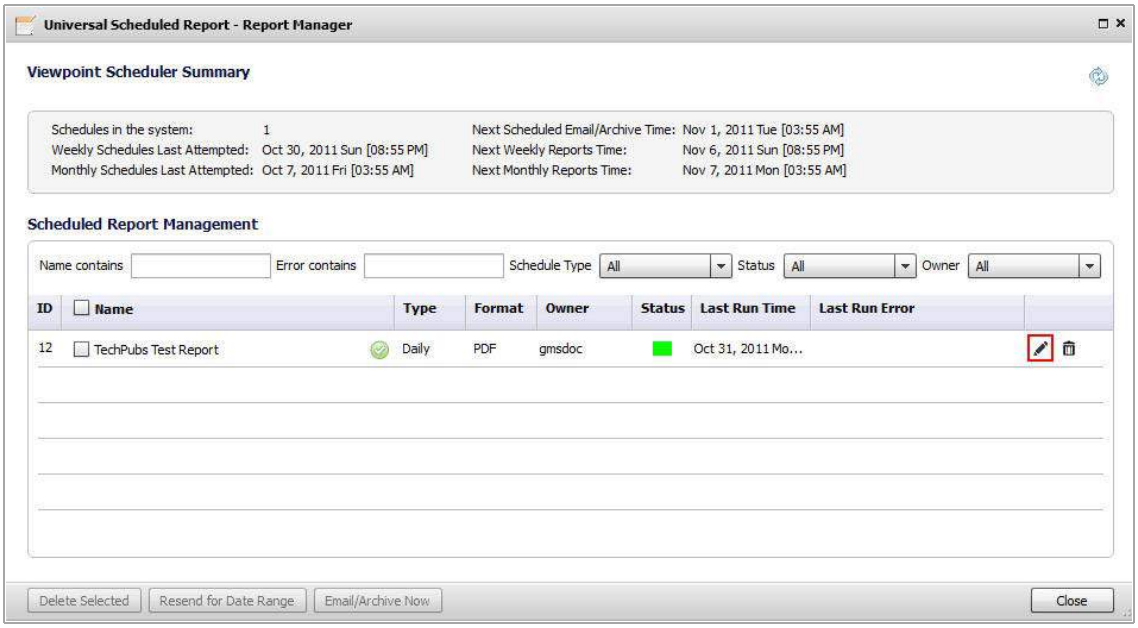
5 Click **OK**.

Your Scheduled report is now Emailed and Archived.

Editing a Scheduled Report

To edit an existing scheduled report, complete the following steps:

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



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

3 To edit the Scheduled Report, use the same configuration procedure shown in Creating a Universal Scheduled Report on page 40.

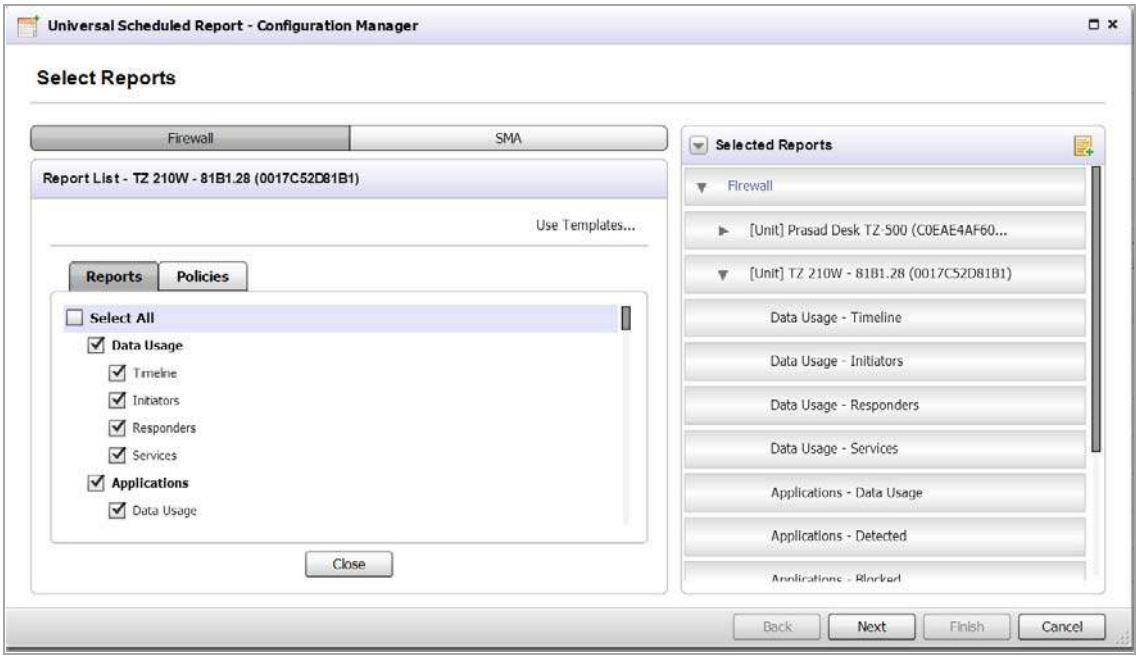
Disabling a Scheduled Report

To disable a scheduled report, complete the following steps:

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

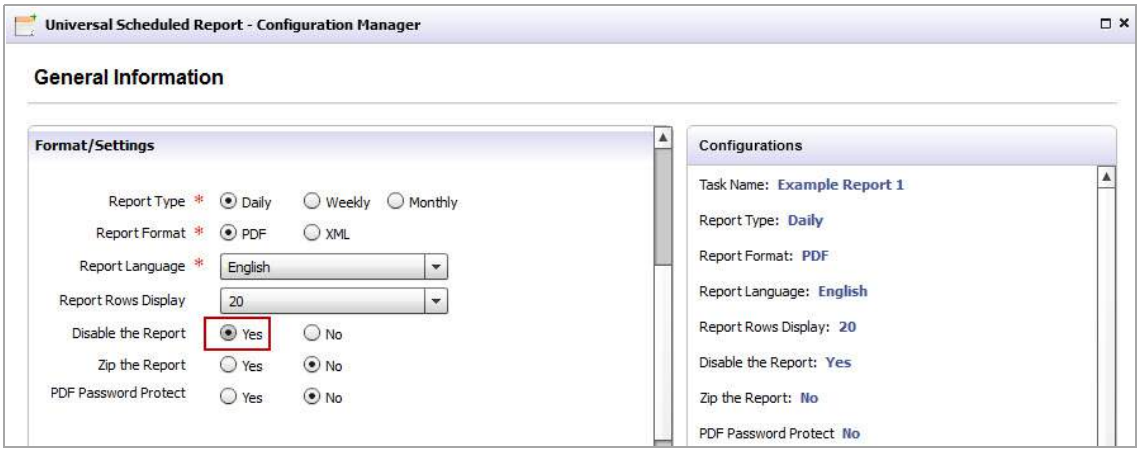
2 Click on the **Edit** icon for the report you wish to disable.

The Universal Scheduled Reports - Configuration Manager window displays.



3 Click **Next**.

The General Information Page displays.



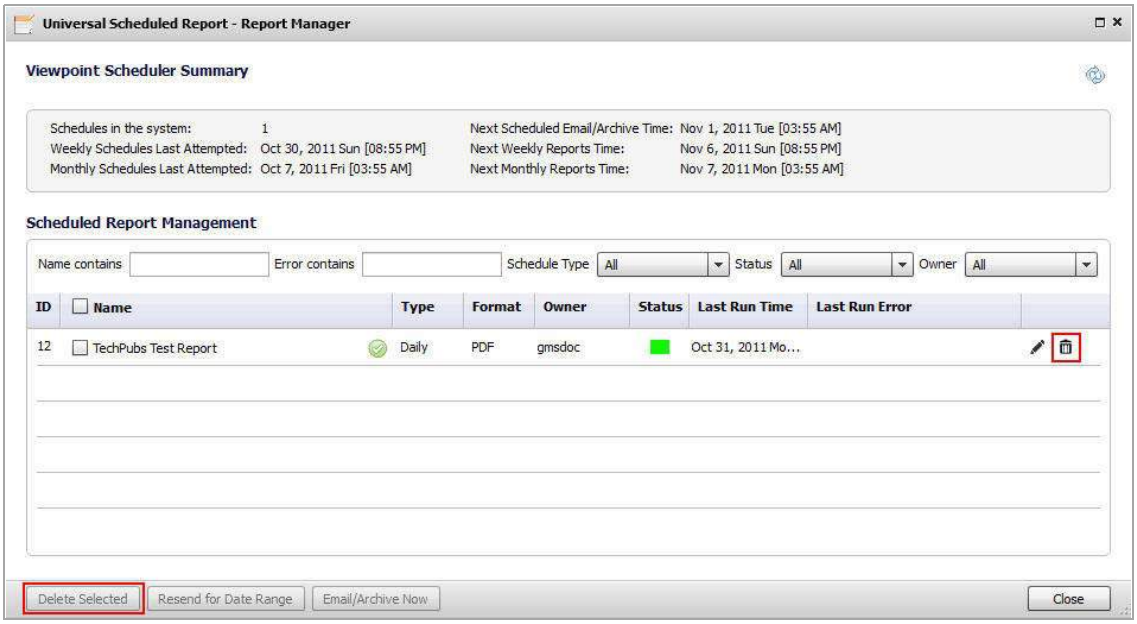
4 In the Format/Settings panel, navigate to the **Disable the Report** option and click **Yes**.

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

Deleting a Scheduled Report

To delete an existing Universal Scheduled Report, complete the following steps:

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



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

3 Click **Delete Selected**.

The selected reports are now deleted.

NOTE: You can also use the **Trash** icon to delete a specific Scheduled Report.

Part 3

Reporting

- Overview of Reporting
- Managing Firewall Reports
- Viewing SMA Reports

4

Overview of Reporting

This chapter describes how to use 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:

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. SonicWall Analyzer Reporting complements SonicWall's Internet security offerings by providing detailed and comprehensive reports of network activity.

The 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 user interface. 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, through a drop-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. See Layout of Reports Display on page 62 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. SonicWall Analyzer waits until you click **Go** before it begins building the new report.

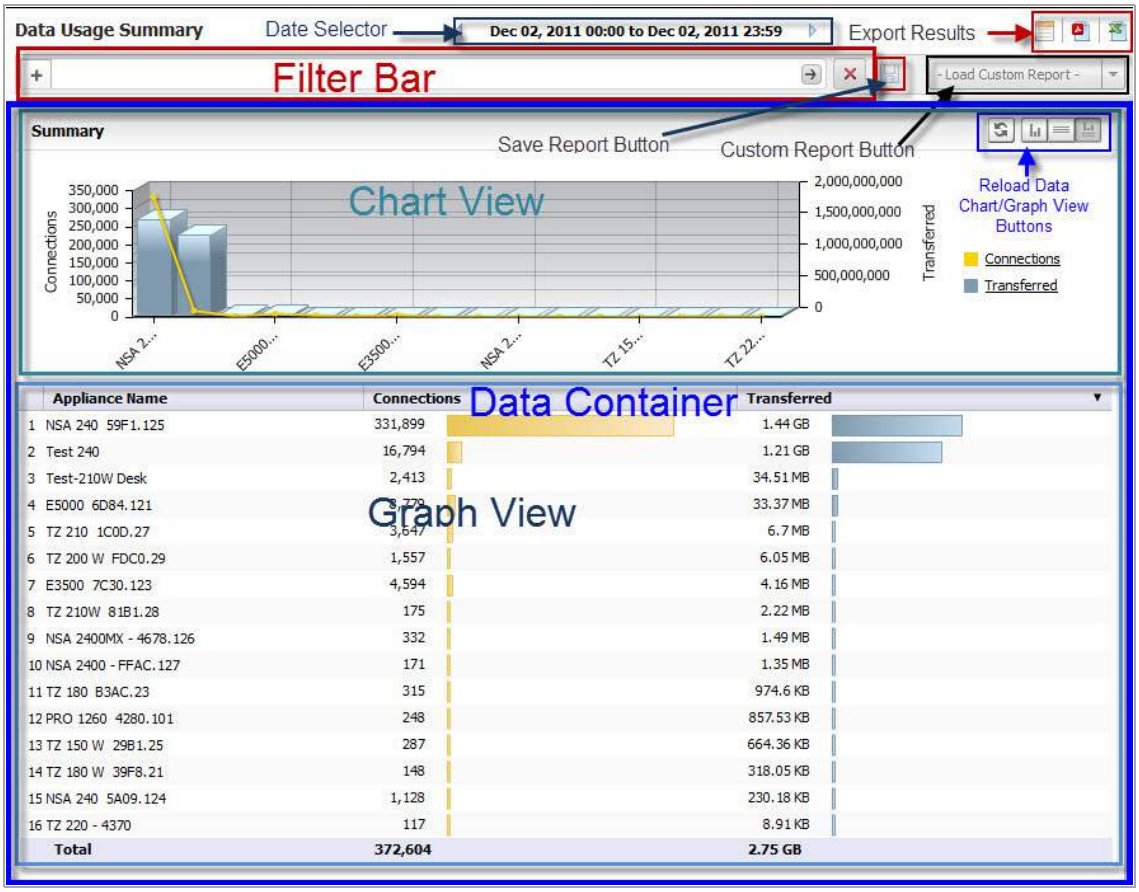
The SonicWall Analyzer Reporting Module provides an interactive interface that:

- 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 and SMA tabs is divided into three panes: 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 view or 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 collapses 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 drop-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 SMA tabs:

Firewall Reports

Feature	Description
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.

SMA Reports

Feature	Description
General	Provides general unit and license status.
Data Usage*	Provides an overall data usage report.
User Activity Reports	Produces a detailed 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.

Navigating SonicWall Analyzer Reporting

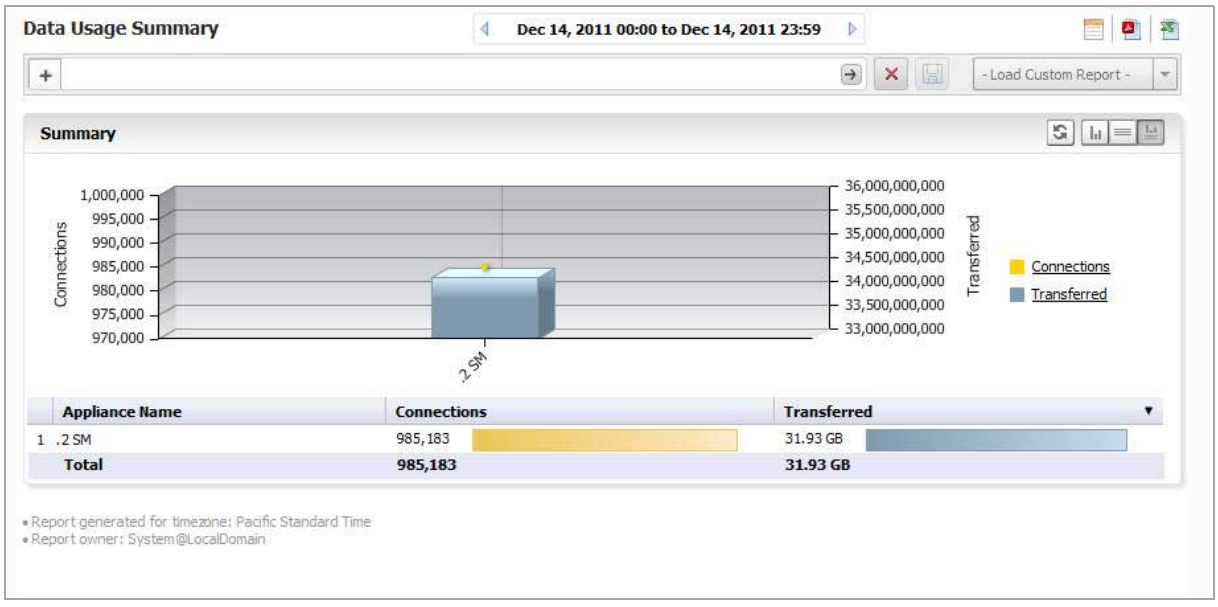
SonicWall Analyzer Reporting is a robust and powerful tool you can use to view detailed reports for individual SonicWall appliances.

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 SonicWall Analyzer. See the following sections:

Global Views

From the Global view of the Firewall Panel, Summary reports are available for all SonicWall appliances connected to 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 **My Reports** view icon in the upper-left 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 defaults back to the Chart and Grid View.

Unit View

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

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 Using the Universal Scheduled Reports Application on page 31.

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 might 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 might 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.

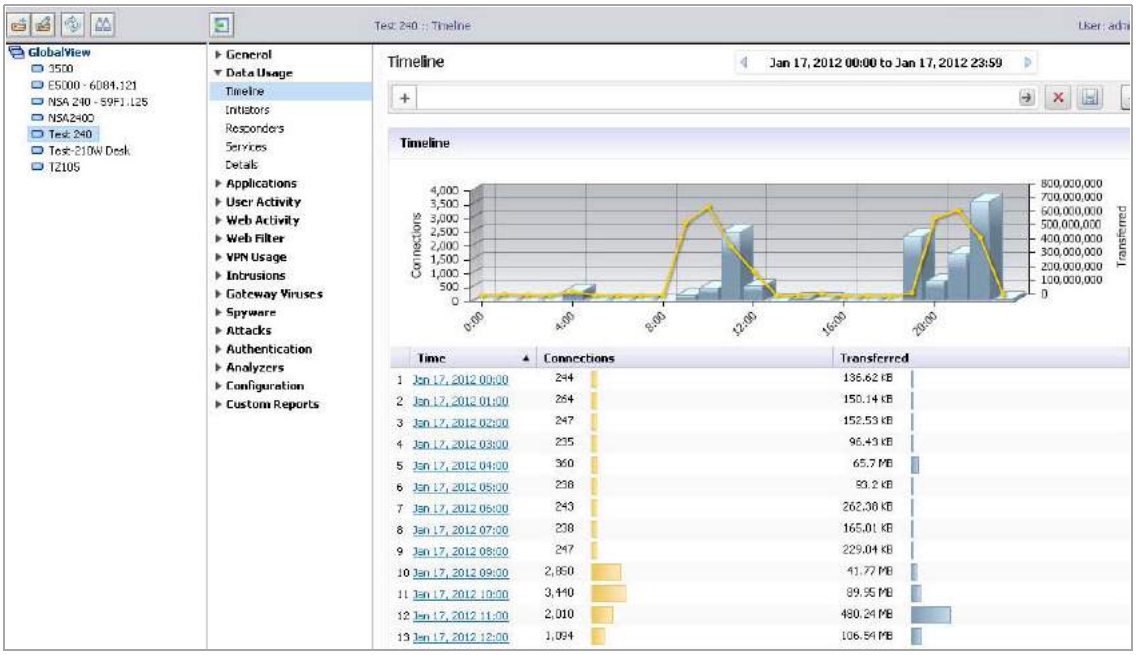
The reports available are usually the reports that appear as sections in the Details view. The Details entry is a shortcut to a view of all the available reports.

To access the Reports, use the following steps:

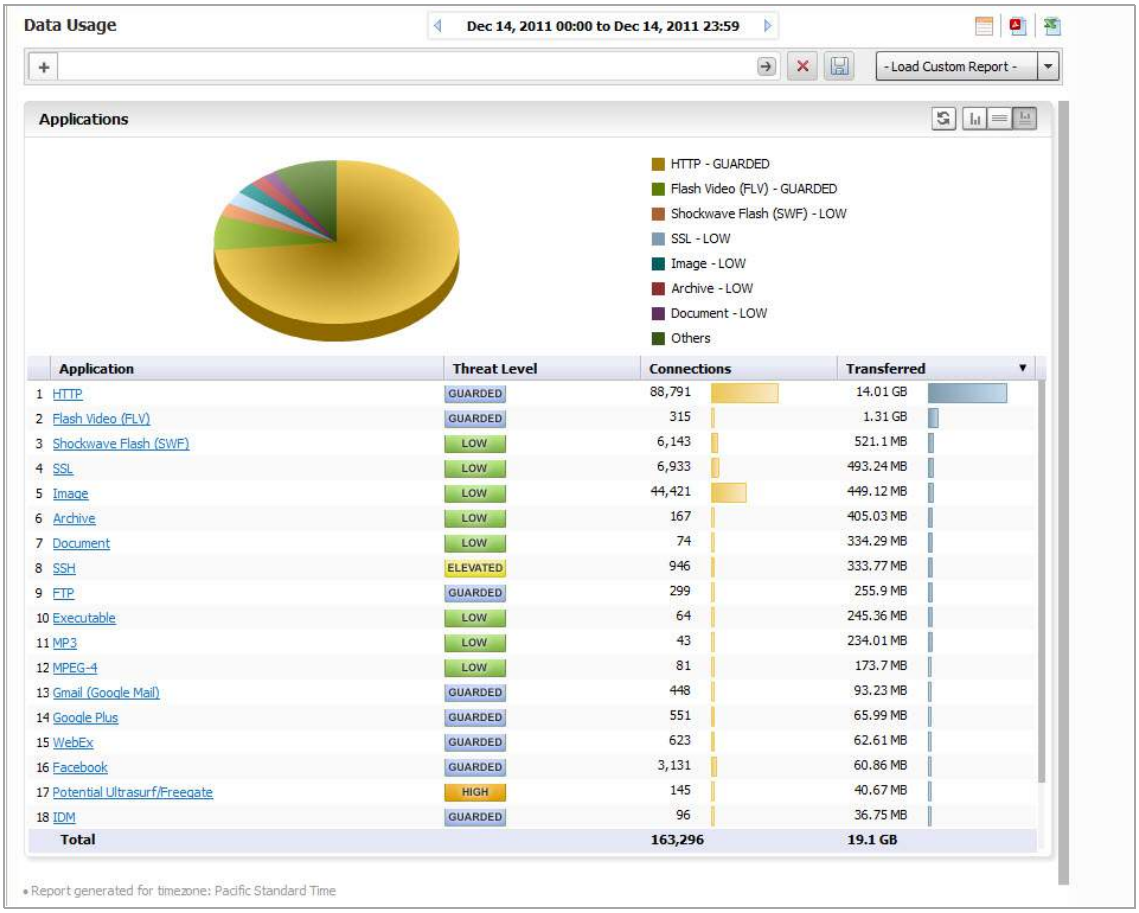
1 Click on the desired tab at the top of the SonicWall Analyzer interface.

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

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.



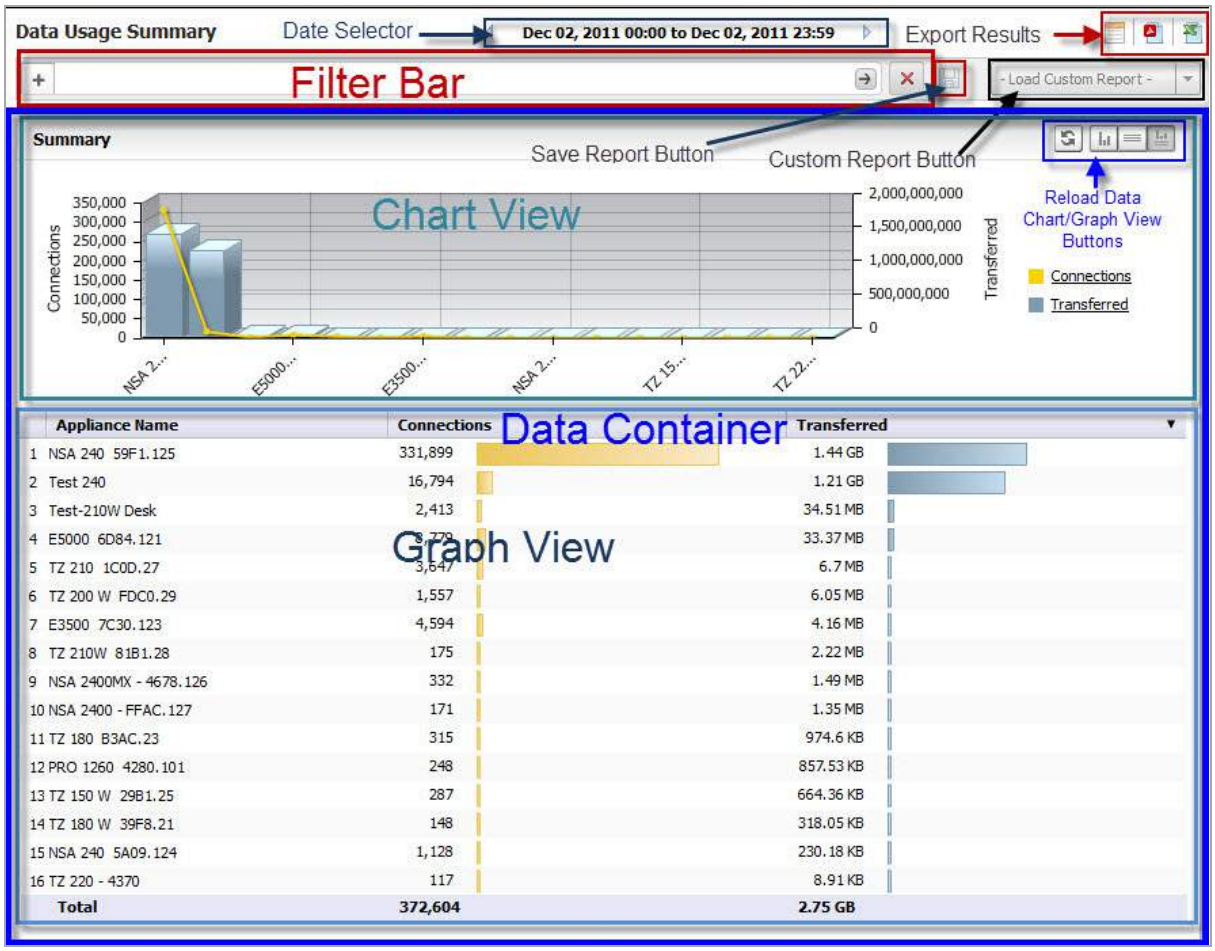
NOTE: As you navigate the Firewall panel with a single SonicWall appliance selected and apply filter settings, your filter settings remain in effect throughout the session. To remove filter settings, click on the search bar **Remove Filters**. (Refer to the graphic in Layout of Reports Display on page 62.)

Layout of Reports Display

The Report Display is comprised of the following areas:

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

The figure that follows 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

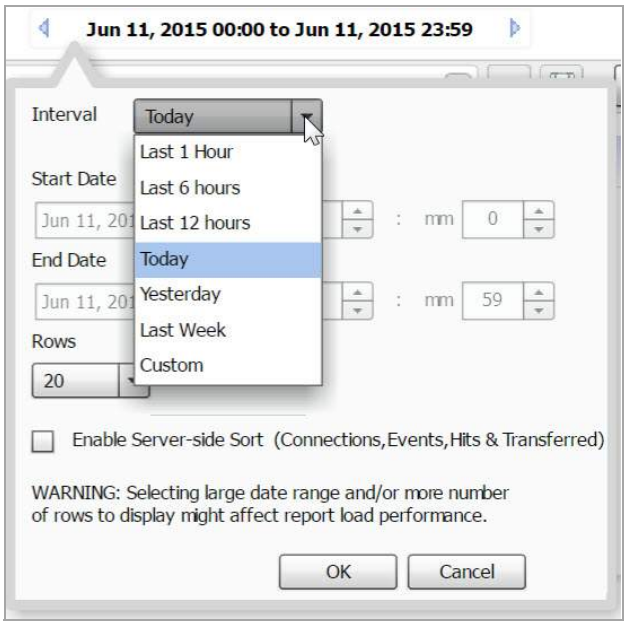
The **Date Selector** allows you to generate a report for only a specific date and time range. Use the right and left quick-link arrows to move backward and forward in time, a day at a time. Clicking the time field on the Date Selector brings up a drop-down menu that allows you to customize your time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



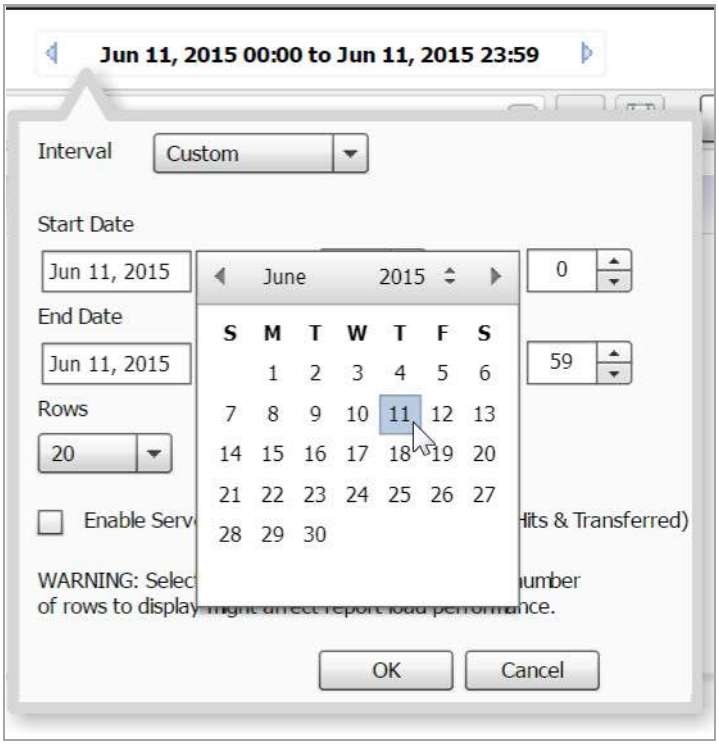
You can select from:

- 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 drop-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.

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

In the Interval menu, you can either set the date manually or by using the drop-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 is not available (grayed out).



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).

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 drop-down appears, specify the number of rows. Select **5**, **10**, **20**, **50**, or **100** from the **Rows** drop-down list to limit the display to a the specified number of lines, for easier viewing.

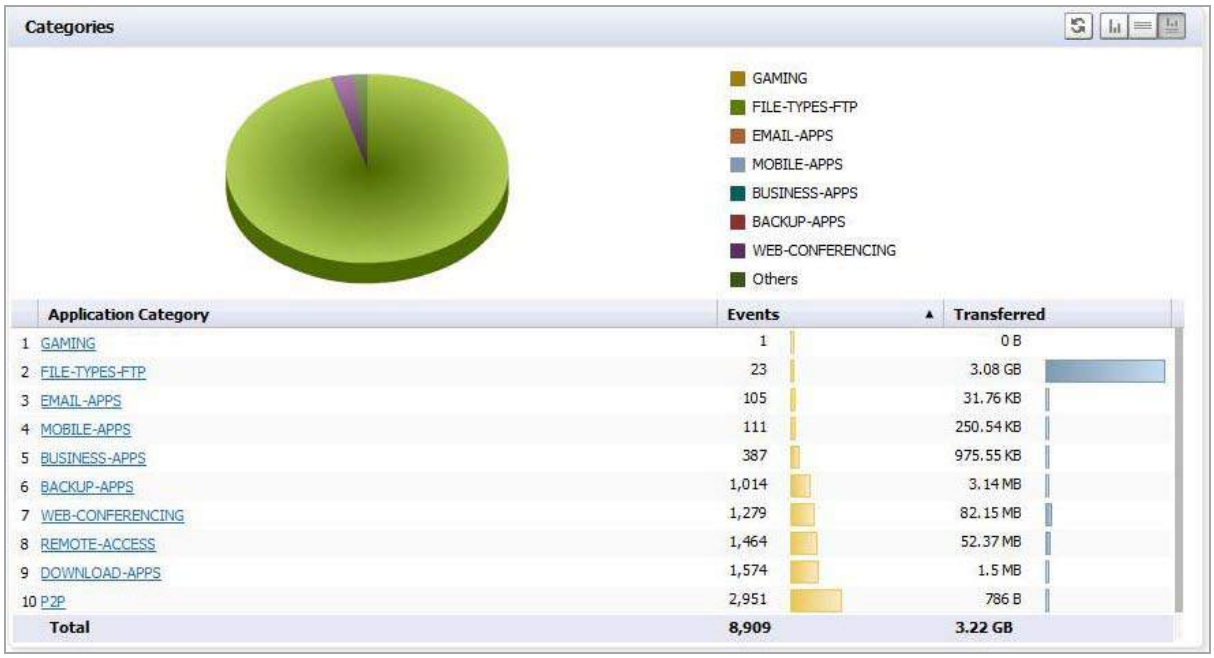
4 Click **OK** to generate the report.

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 apply only to the data in those rows. If you reverse the sort order by clicking on the column bar, only the displayed items are re-sorted.

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

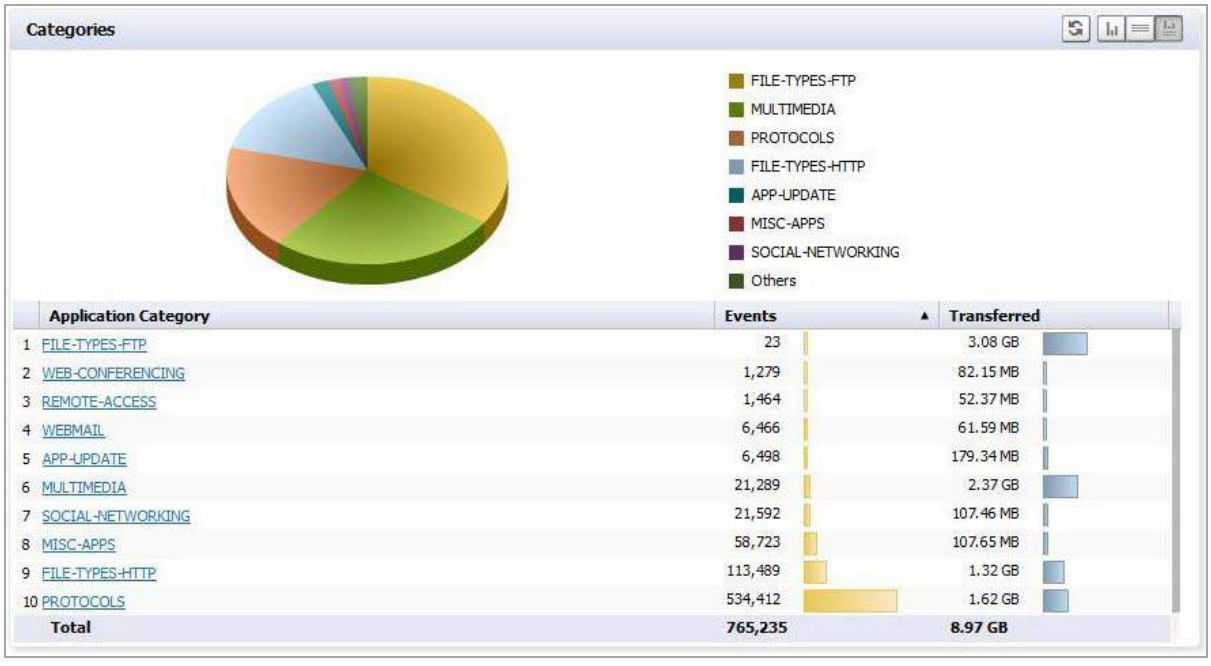
By default, Client-side Sort is used, which sorts only the currently viewable data, which was retrieved the first time the data base was clicked on.

For example, the image that follows 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**

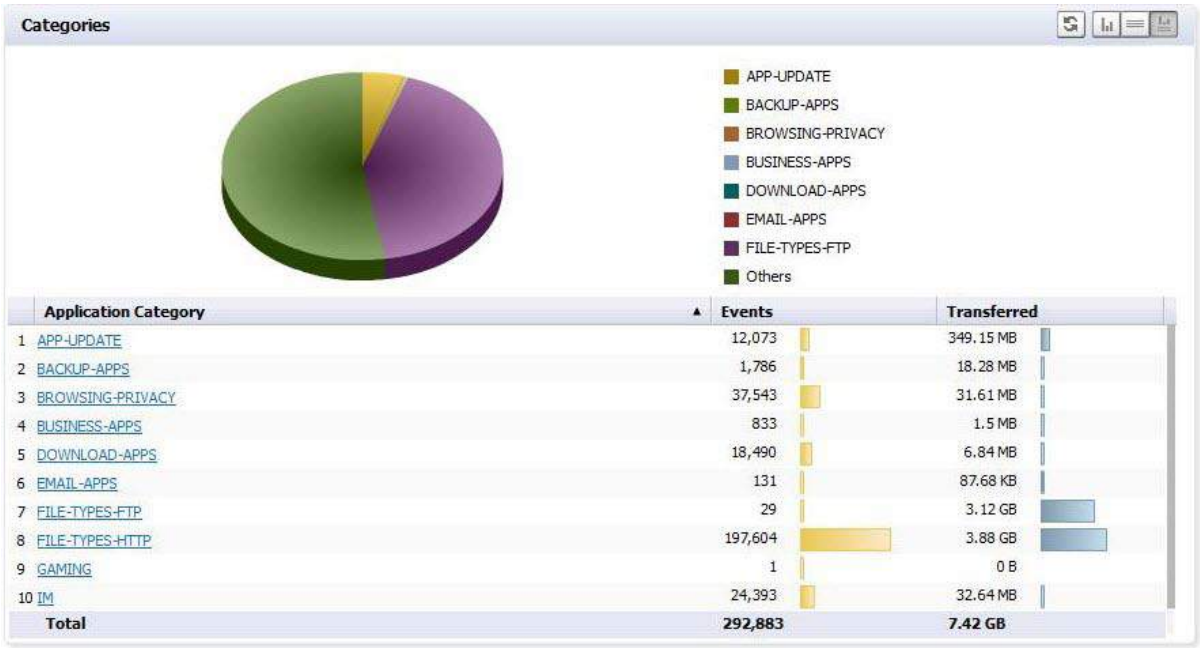
If you re-rank the column to see the lowest number of hits, it ranks only the items displayed in the ten rows you selected.



	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 re-sorts 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

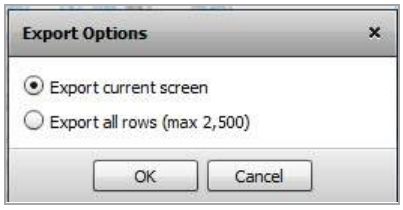
The **Export to PDF** and **Export to CSV** icons allow you to save a report in either PDF or Excel format.

These buttons provide the following export options:

- **Export to PDF** — This button allows 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 **Export to PDF**, 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 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 **Add Filter (+)** for adding filters and a **Go** button to apply filters, as well as the **Clear Filter** button to clear all filters.

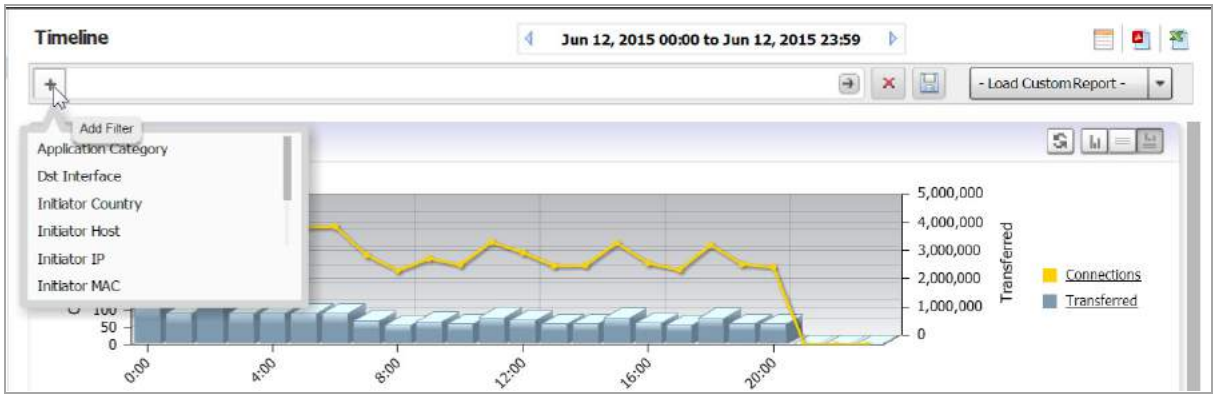
Using the Filter Bar allows you to view subsets of the report data, based on a set of pre-defined filters.

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 on page 70 for more information.

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

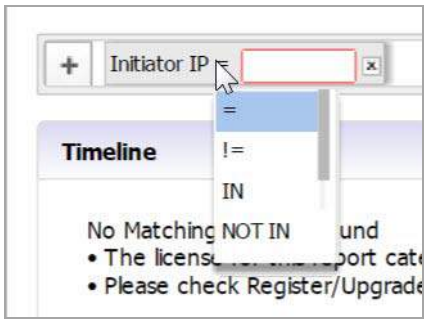
Click **Add Filter** (+) on the left to display a drop-down menu, which can then be used to fine-tune the report data by selecting categories.



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

Filter criteria are context-dependant, meaning that 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 and so on.

Operators are specified by clicking on the default operator to bring up the drop-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 the Filter Operators table.

Filter Operators

Operator	Definition
=	Only data that exactly matches the filter input numerical value is included in the report
!=	Data values that are not equal to the input numerical value are included in the report
>	Data values that are greater than the input value are included in the report.
>=	Data values that are greater than or equal to the input value are included in the report.
<	Data values that are less than the input value are included in the report.
<=	Data values that are less than or equal to the input value are included in the report.
IN	Data values that are in the input value are included in the report.
NOT IN	Data values that are not in the input value are included in the report.
LIKE	Data values that are like the input value are included in the report.
NOT LIKE	Data values that are not like the input value are included in the report.
IS	Data values that are between the input values are included in the report. Separate the vales by using a hyphen with a space on either side, such as “172.30.72.16 - 172.30.72.19.”
IN RANGE	Subnet data that is in the specified range is included in the report.
NOT IN RANGE	Subnet data that is not in the specified range is 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, and so on.

Using the Filter Bar

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

To add a filter:

1 Click the **Add Filter (+)** menu and select a filter from the drop-down menu. Available Filter categories can differ, depending on the report, and could require parameters.

> **NOTE:** 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. You can create reports with filters on VLAN Interfaces by using the Interface Filter (Source or Destination), and using the VLAN interface name with ':' replaced by '-'. VLAN Interfaces typically are as follows: X8:V100, X0:V20, and so on. When VLAN interface information is sent in the syslogs, the character ':' is replaced with '-'. So, you must use values such as X8-V100, X0-V20 in the Interface filters.

2 Click **Go** (right arrow) to add a filter Each filter must be applied by clicking **Go** before you can select and apply the next filter. The filter bar shows all filters added, whether added from the menu bar or drop-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.

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

Adding Filters Implicitly

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.

To add a filter to a "drillable" column containing hypertext links:

1 Right-click on a hypertext column cell and select **Add Filter** from the resulting drop-down context menu.

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

After being added, the filter is added to the filter area of the Search Bar and no longer appears in the drop-down list. The report displays only results restricted by that filter.

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.

To save a report, along with its filter criteria:

1. Click **Save Report**.
2. Assign it a file name for later reference.
3. To view a saved Custom Report, click **Custom Reports** to bring up a menu that contains a list of all saved Custom reports available for viewing. Selecting a Custom Report from this drop-down loads data for the selected report into the Report Data Container.
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.
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 **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 **Load Custom Reports**.

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

When the Configuration Manager menu comes up, it is 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.

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.

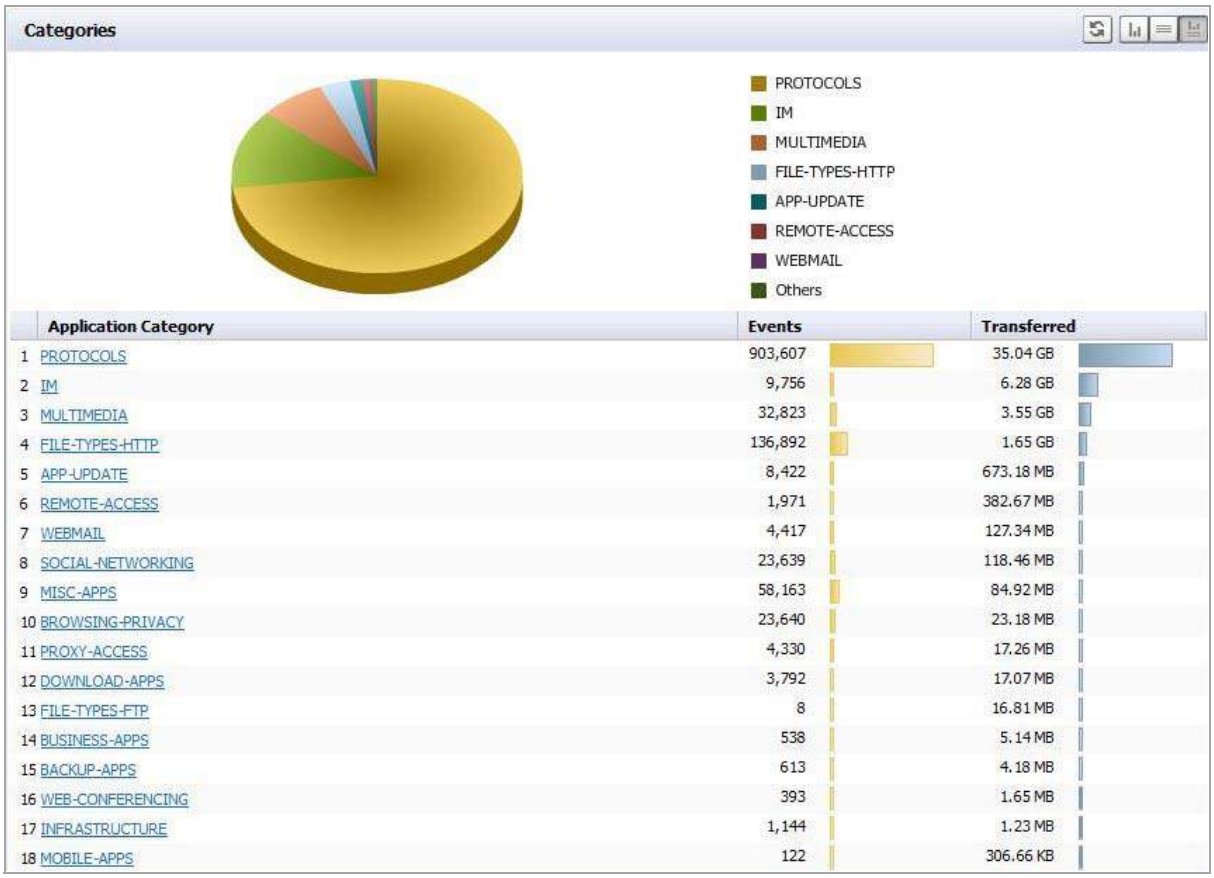
Detail-level reports are available either by “drilling down” on hyperlinks in the Root-level view, or, for some types of Reports, as a shortcut on the Report tab.

NOTE: Cell data in the report container can be copied by right-clicking the cell and selecting Copy Cell Data from the drop-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 might 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

TIP: At times, you might 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 might 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.

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 three 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 can 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 previously. Clicking this button instructs 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 drop-down menu. The syslog fields corresponding to the applied filter comes up.

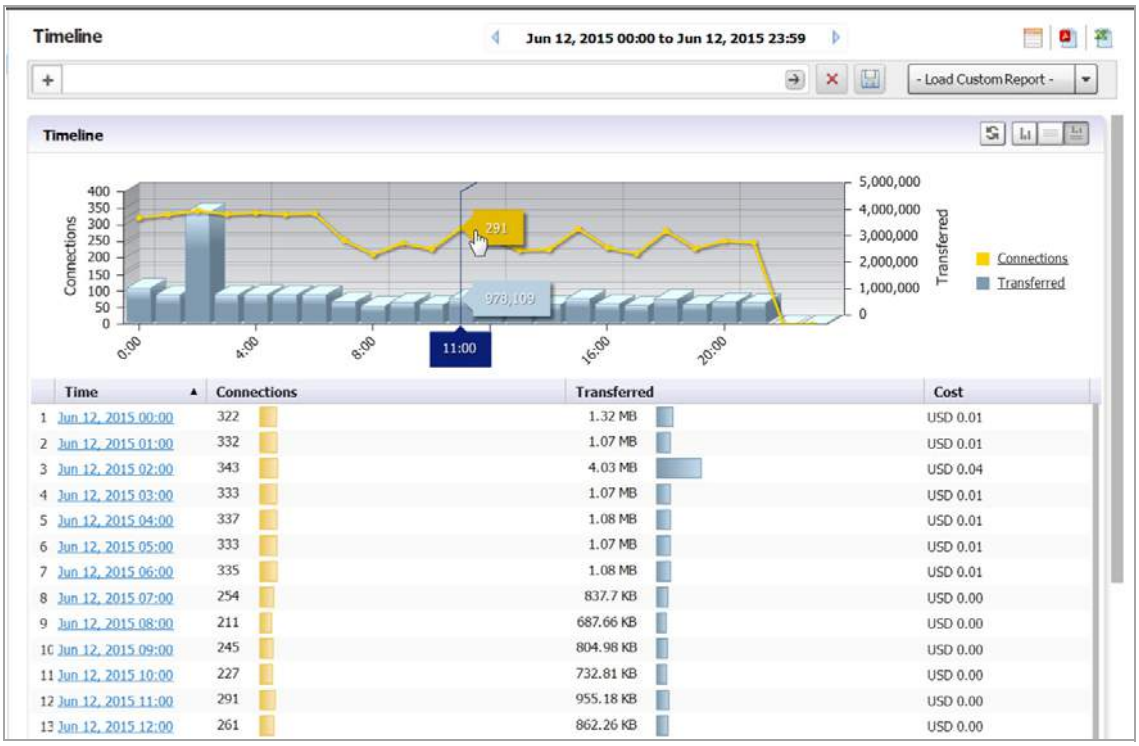
Drilling Down

Sections in the Grid display might 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 is 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.

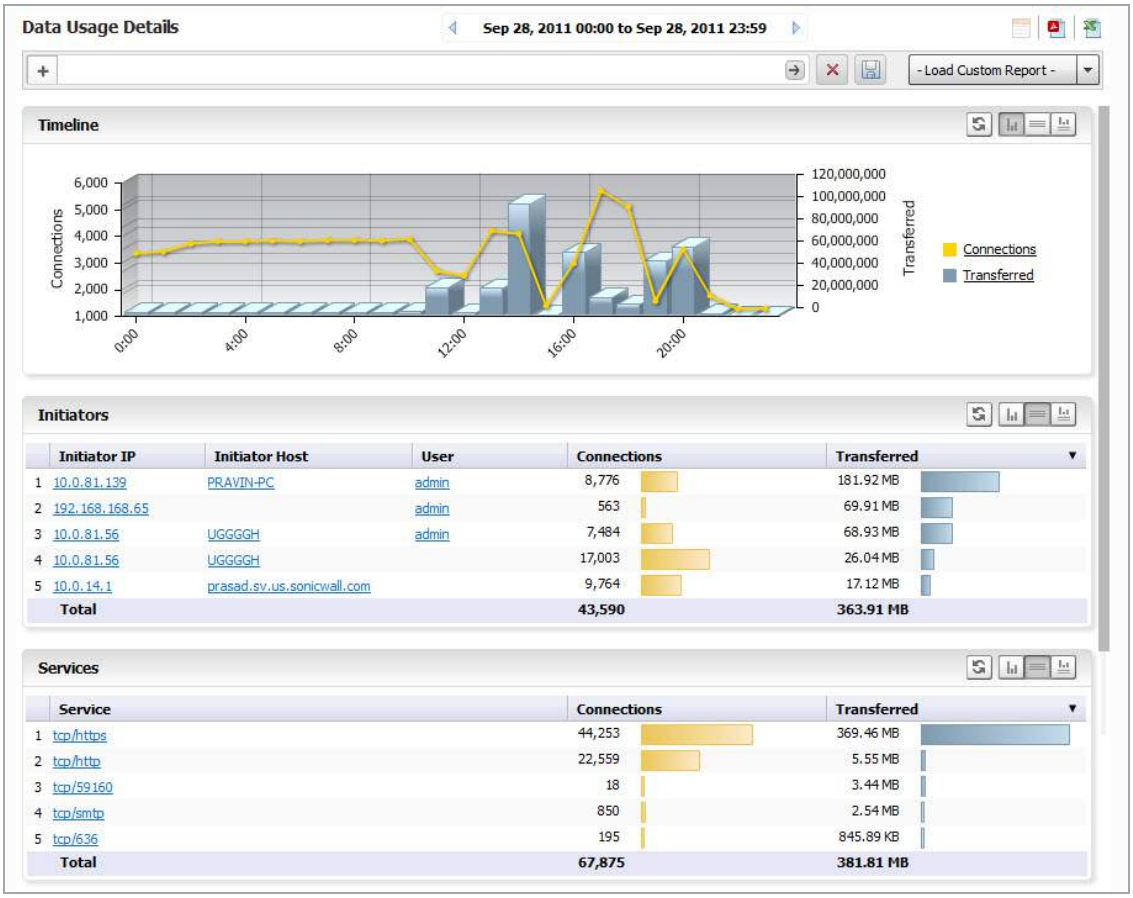
1 Click on an appliance, then click **Data Usage** on the Reports tab. You see a timeline showing connections.



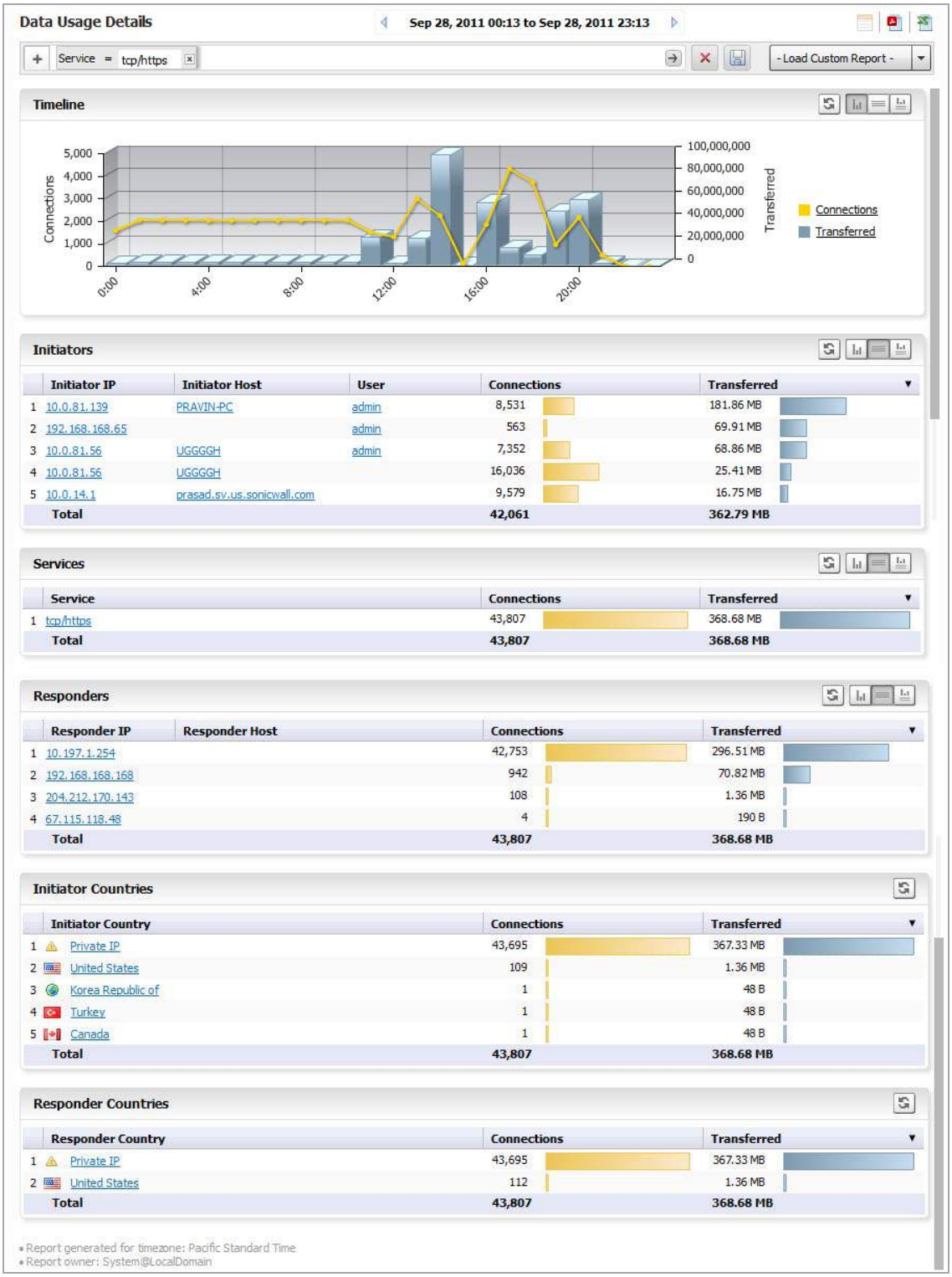
	Time	Connections	Transferred	Cost
1	Jun 12, 2015 00:00	322	1.32 MB	USD 0.01
2	Jun 12, 2015 01:00	332	1.07 MB	USD 0.01
3	Jun 12, 2015 02:00	343	4.03 MB	USD 0.04
4	Jun 12, 2015 03:00	333	1.07 MB	USD 0.01
5	Jun 12, 2015 04:00	337	1.08 MB	USD 0.01
6	Jun 12, 2015 05:00	333	1.07 MB	USD 0.01
7	Jun 12, 2015 06:00	335	1.08 MB	USD 0.01
8	Jun 12, 2015 07:00	254	837.7 KB	USD 0.00
9	Jun 12, 2015 08:00	211	687.66 KB	USD 0.00
10	Jun 12, 2015 09:00	245	804.98 KB	USD 0.00
11	Jun 12, 2015 10:00	227	732.81 KB	USD 0.00
12	Jun 12, 2015 11:00	291	955.18 KB	USD 0.00
13	Jun 12, 2015 12:00	261	862.26 KB	USD 0.00

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 might 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 shows the detail view applicable to that filter.

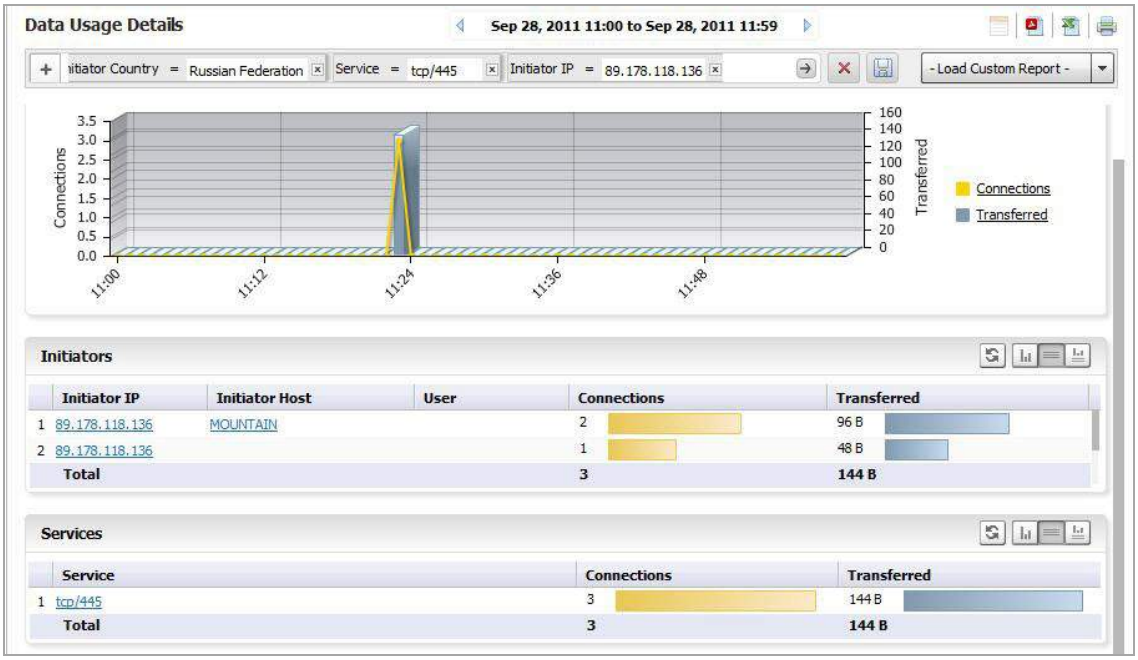


3 To further filter the output, to view only tcp/https usage, click on the tcp/https entry under **Services**. A **Detail** report, filtered to show only usage of tcp/https, comes up. Notice that a Service entry has been added to the Filter Bar.



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

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



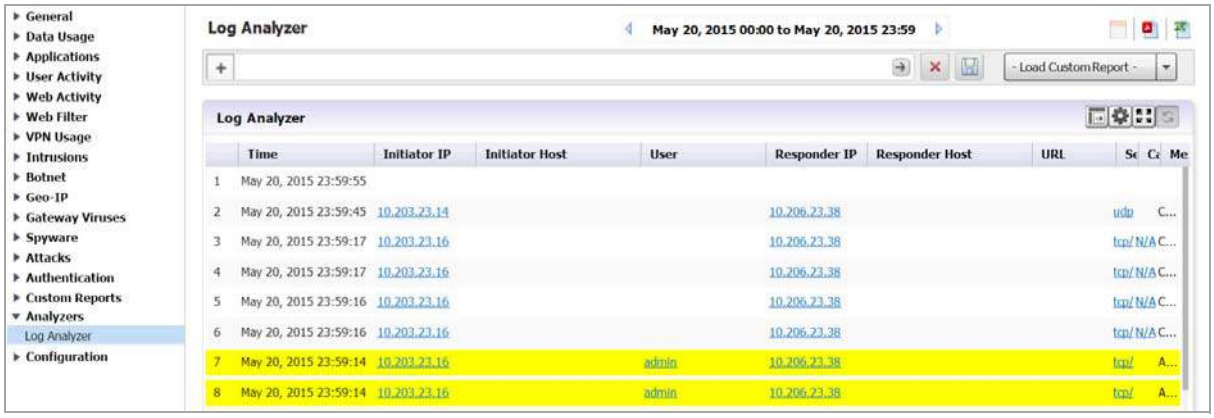
NOTE: Many report categories contain a Details item in the list of reports. This link provides a shortcut directly to the Detail view of all sub-sections of the report. You can apply filters directly to the Detail view to further constrain the displayed information.

The Log Analyzer provides the most detailed Report information.

4 To view the Log Analyzer, go to the **Reports** tab after 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 might wish to limit the amount of data displayed on the page. The amount of data in the report can also affect the loading speed.

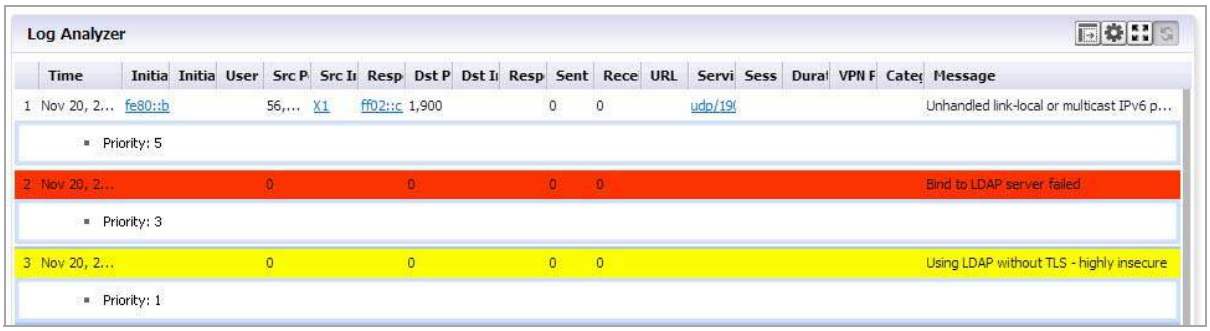
The Log Analyzer contains information about each connection, including port and interface information, number of Bytes sent, and so on.



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 drill-down process.

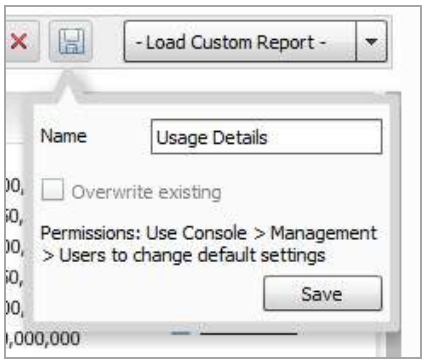
Click on a row to expand the log, additional information can be viewed here:



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 **Save** to bring up a drop-down allowing you to save a custom report.



This menu is 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 is added to the drop-down menu accessed when you click **Load Custom Report**. It is also added to the Reports Tab list under Custom. When a specific Custom report is selected on the Load Custom Report drop-down menu, the button reflects the name of that report.

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

Troubleshooting Reports

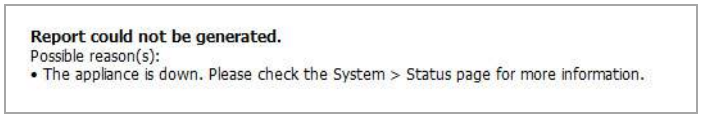
One of the most common reasons when a report does not display is that no data is available for the selected appliance. There are several reasons why you might see this error. Analyzer displays the most likely reason(s) and gives you instructions for ways to resolve the problem.

The most common examples are as follows:

Appliance is in a Provisioned State:

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

Appliance is Down



No Matching Records Found

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 Analyzer Reports on the Console tab

There are management settings for the Analyzer Reporting Module on the Analyzer **Console** tab. A Reports selection is available on the left menu bar, which allows you to set up certain tasks in the right Management pane that 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 Summarizer parameters and schedule emailing or archiving of reports.

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

Reports generated by pre 8.0 releases of SonicWall Analyzer can still be viewed, but require specific configuration. See Managing Legacy Reports on page 155.

5

Managing 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 SonicWall Analyzer Reporting Overview on page 56.

The Firewall reports display either summary or unit views of connections, bandwidth, uptime, intrusions and attacks, and SMA 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, complete the following steps:

1 Log in to your Analyzer management console.

2 Click the **Firewall** tab.

3 Select an appliance or global view from the TreeControl.

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.

- Real-Time Viewer
  - Summary: Syslog

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, Initiator MAC, User, Connections, and total Transferred, displayed as a pie chart
    - Responders: Top Responders, listed by IP address, Responder Host, Responder MAC, Connections, and total amount Transferred, 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: Initiator IPs, Initiator Host, Initiator MAC, Users, Connections, total amount transferred, 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
    - Categories: hits and browse time listed by information category
    - Sites: sites visited by IP, name, and category, with hits and browse time
    - Initiators: Initiator IP, Initiator Host, Initiator MAC, with User, Browse Time, Hits, and total amount transferred
    - 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
    - Categories: 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

    - Blocked: blocked intrusions and number of attempts at access
    - Targets: number of intrusion events by target host and IP
    - Initiators: Initiator host and IP with category and use
    - Timeline: intrusions listed by time of day
    - Details: provides a shortcut to an access timeline and Detail view normally reached by drilling down. Detail sections include: Categories, Sites, and Initiators.
    - Alerts: provides a list of intrusion alerts
- Botnets
    - Initiators: Initiator host and IP with category and use
    - Responders:
    - Attacks:
    - Timeline: Intrusions listed by time of day
- Geo-IP
    - Responder Countries: Blocked traffic that is based on the traffic's country of origin or destination
    - Initiator Countries:
- Capture ATP
    - Status - files scanned in the last 30 days with applicable filters
    - Summary
    - Blocked - virus attacks blocked by Capture ATP and the number of attempts at access
- 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
    - Details: provides a shortcut to an access timeline and Detail view normally reached by drilling down. Detail sections include: Categories, Sites, and Initiators.
    - Alerts: provides a list of virus alerts
- 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
    - Details: provides a shortcut to an access timeline and Detail view normally reached by drilling down. Detail sections include: Categories, Sites, and Initiators.
    - Alerts: provides a list of spyware alerts
- 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
    - Up/Down Status
        - Timeline: provides a timeline of unit availability. No Detail sections are available.
    - 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.
    - Flow Activity
        - Real-Time Viewer: real-time data displayed graphically.
        - Top Flows Dashboard: displays top flows per report type.
        - Flow Analytics: monitors applications, users, URLs, initiators, responders, threats, VoIP, VPNs, devices, and contents.
        - Flow Reports: real-time reports displayed graphically.

Understanding the Data Container

The Report contains a filter bar at the top, plus the actual Data Container. The default Data Container contains an interactive chart view that contains either a grid view, containing a text version of the information. One or more sections might 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 can 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 that 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 Using the Log Analyzer on page 108.

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 that 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 **Save** on the Filter Bar. The saved view now appears under Custom Reports.

To learn more about Custom reports, see Custom Reports on page 108.

How to View Firewall Reports

The Firewall Summary reports display an overview of bandwidth, uptime, intrusions and attacks, and SMA 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.

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.

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.

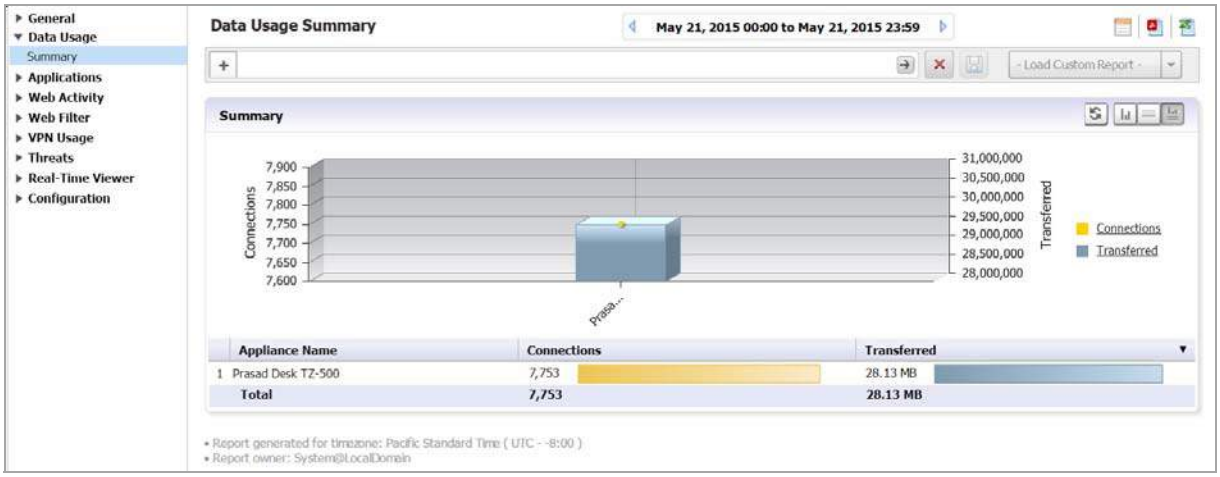
To view the Summary report, complete the following steps:

1 Click the **Firewall** tab.

2 Select the global icon.

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 Unit Level Status Reports

Unit level reports display status for an individual SonicWall appliance. From this information, you can locate trouble spots within your network, such as a SonicWall appliance that is having network connectivity issues caused by the ISP. You can also monitor web usage, including attempts to reach filtered sites, as well as incoming attacks on your network.

NOTE: Global reports are displayed in Analyzer's timezone. Reports for individual SonicWall security appliances are displayed in the individual appliance's time zone.

Viewing Data Usage Reports

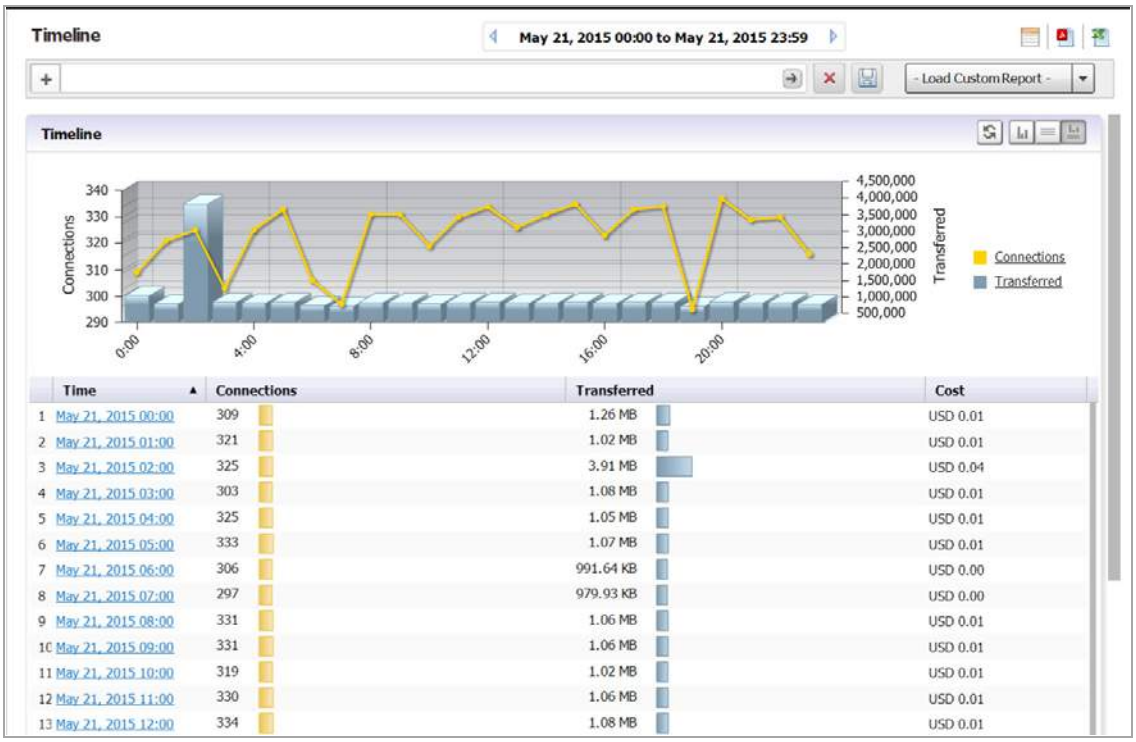
The default Data Usage report displays a timeline for hours that the selected SonicWall appliance was online and functional during the time period with connections, transferred connections, and cost displayed.

To view data usage reports, complete the following steps:

1 Click the **Firewall** tab.

2 Select the global icon or a SonicWall appliance.

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



This report is drillable. Click on an Initiator IP entry to break the Timeline report down into its Detail View report groups for the selected IP address. These groups also contain drillable hyperlinks that takes you to more specific Detail View information. The columns can also be filtered.

Viewing Applications Reports

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

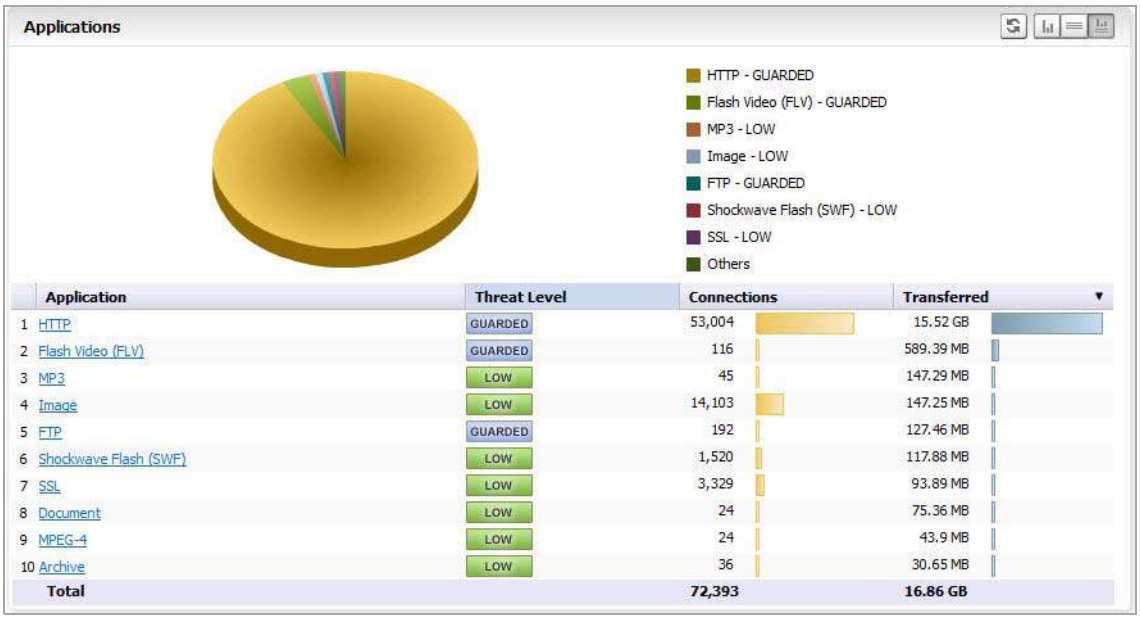
To view Application reports, complete the following steps:

1 Click the **Firewall** tab.

2 Select a SonicWall appliance.

3 Click **Applications > 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 User Activity Logs

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

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 displays 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.

To view User Activity Logs, complete the following steps:

1 Click the **Firewall** tab.

2 Select a SonicWall appliance.

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 displays, with the User filter pre-selected. You can enter a specific user name, or use the LIKE operator wildcards (*) to match multiple names.

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

The customized User Activity Details report displays 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 cannot be available for all of these categories.

Viewing Web Activity Reports

Web Activity Reports provide detailed reports on browsing history.

To view Web Activity Reports, complete the following steps:

1. Click the **Firewall** tab.
2. Select a SonicWall appliance.
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.

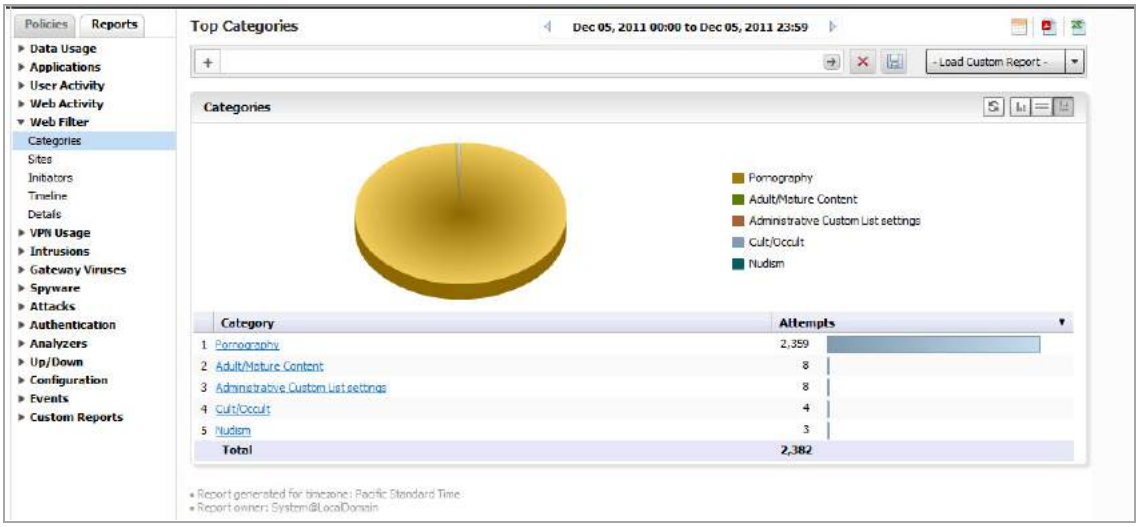
Viewing Web Filter Reports

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

To view Web Filter Reports, complete the following steps:

1. Click the **Firewall** tab.
2. Select the global icon or a SonicWall appliance.
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.

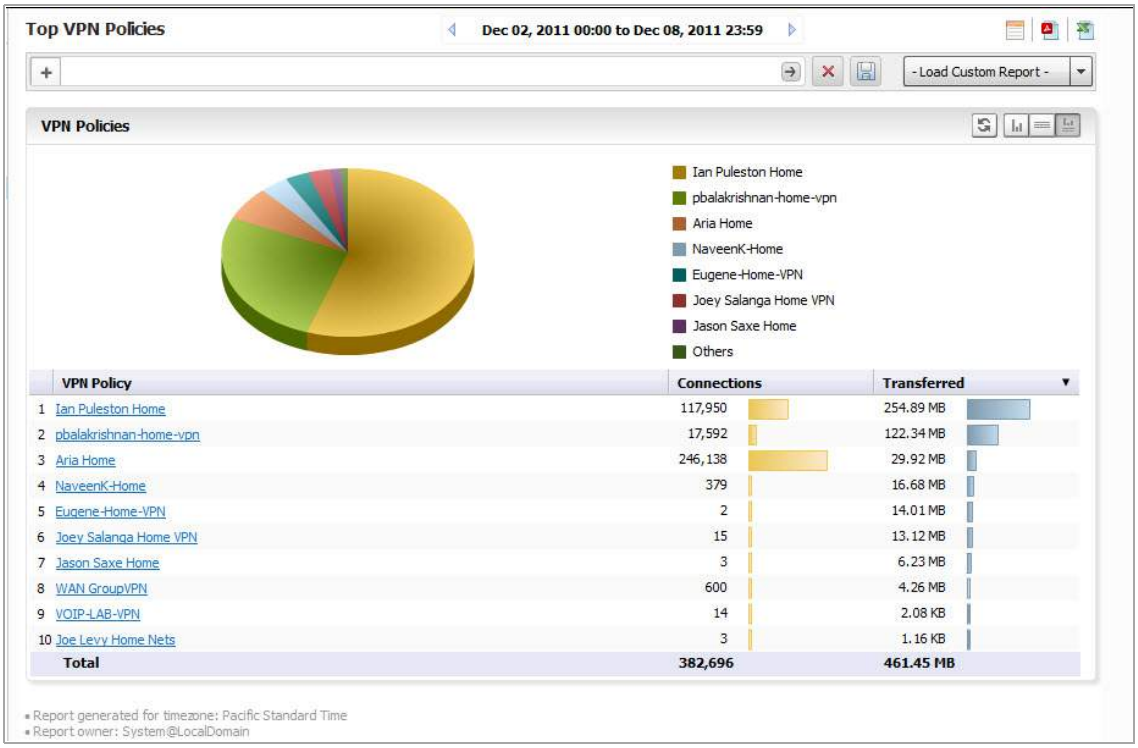
To view VPN Usage reports, complete the following steps:

1 Click the **Firewall** tab.

2 Select a SonicWall appliance.

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.

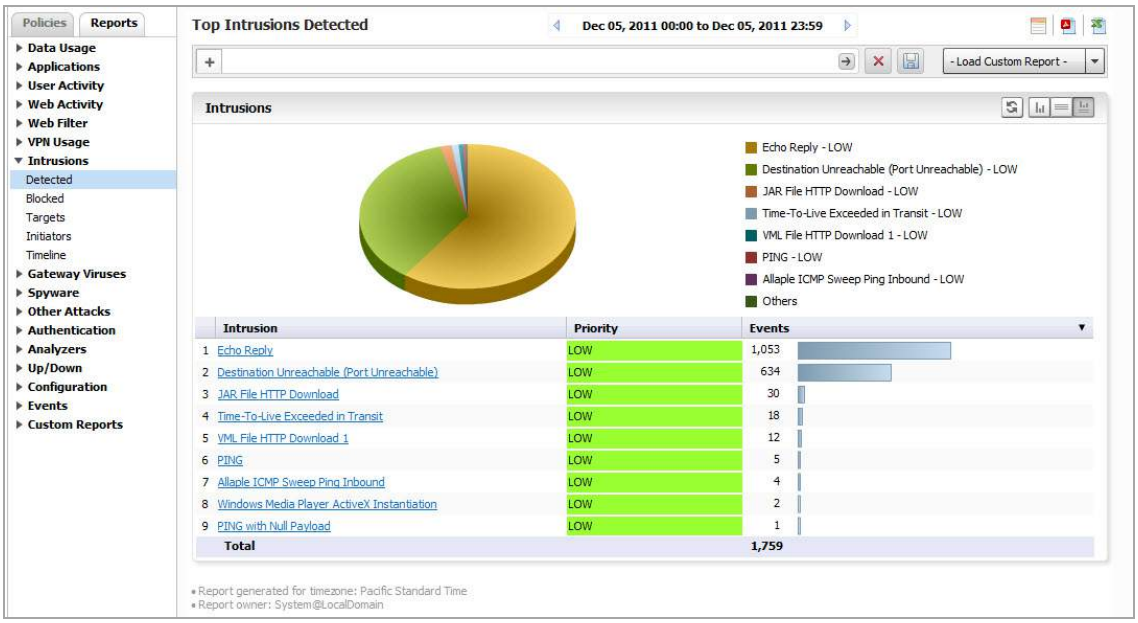
To view Intrusion Reports, complete the following steps:

1 Click the **Firewall** tab.

2 Select a SonicWall appliance.

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 Botnet Reports

Botnet reports provide details on the botnet attempts that were blocked when attempting to access the firewall.

To view Botnet Reports, complete the following steps:

1 Click the **Reports** tab.

2 Select a SonicWall appliance.

3 Click **Botnet > Initiators**.

The top botnet attacks report appears. The Initiators report provides a pie chart and a list of the initiating IP addresses, countries, hosts, and events, with number of attempts for each.

Drill down for additional detailed views of Attacks, Targets, Initiators, Ports affected, Initiator Countries, and Target Countries.

Viewing Geo-IP Reports

Geo-IP reports provide details on the botnet attempts that were blocked when attempting to access the firewall.

To view Geo-IP Reports, complete the following steps:

1 Click the **Reports** tab.

2 Select a SonicWall appliance.

3 Click **Geo-IP > Initiator Countries**.

The top Geo-IP initiator report appears. The Initiators report provides a pie chart of threat initiator countries blocked and events, with number of attempts for each.

Drill down for additional detailed views of Initiator IPs, Hosts, Initiator MACs, Users, and Events.

Viewing Capture ATP Status

The Capture Advance Threat Protection (ATP) reports provide details on whether a file is malicious or not by transmitting the file to the cloud where the SonicWall Capture ATP service analyzes the file to determine if it contains a virus or other malicious elements.

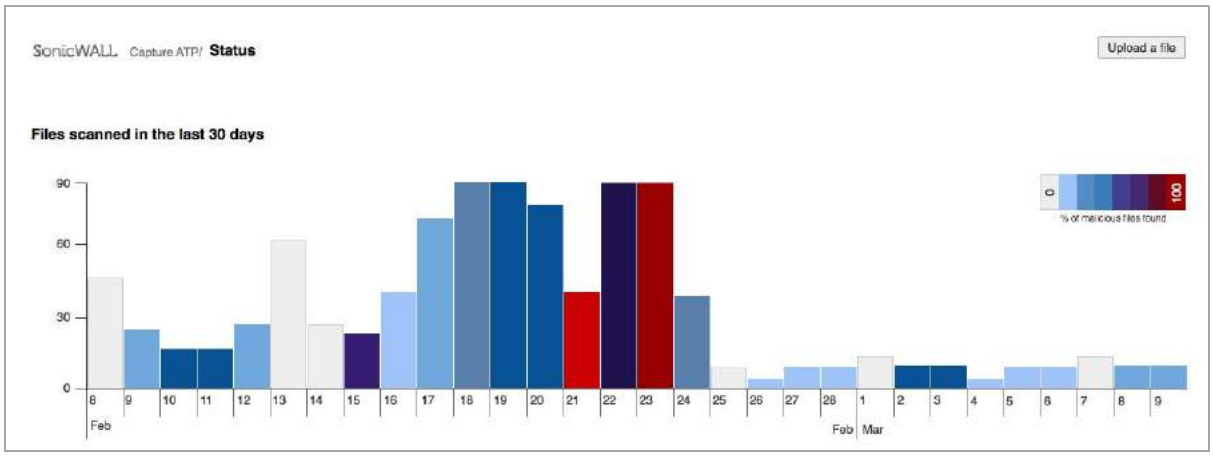
NOTE: A Capture ATP service license is required to use the Capture ATP features. Before you can enable Capture ATP, the Gateway Anti-Virus and Cloud Anti-Virus Database services must be enabled in Analyzer.

Topics:

- Viewing the graph and log table on page 92
- Filtering the log table on page 95

Viewing the graph and log table

The **Capture ATP > Status** page displays a graph and a log table that provide information for each file that has been scanned. Files can be uploaded to Capture ATP for scanning from this page by clicking the **Upload a file** button.



The graph shows the number of files scanned for each day. The X axis represents time and shows only the last 30 days. Each tick is one day. The Y axis represents the number of files scanned.

The percentage of malicious files found is represented by the color of each bar in the graph. The key shows the percentage that each color represents. Zero means no malicious files were found.

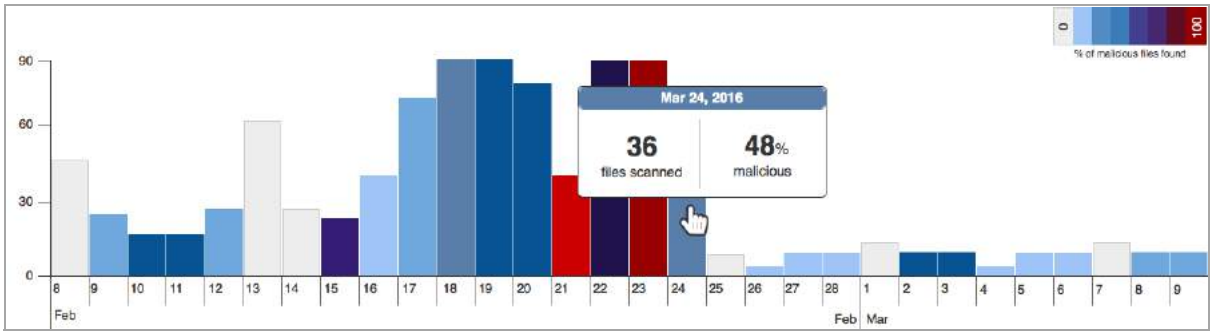
Below the graph, the log table shows information for each file that has been scanned. You can customize what is displayed in the log table, by clicking the Add filter… link. The graph, log table, and filters are bound, and any interactions on one will affect the others.

Viewing 1,859 files scanned.

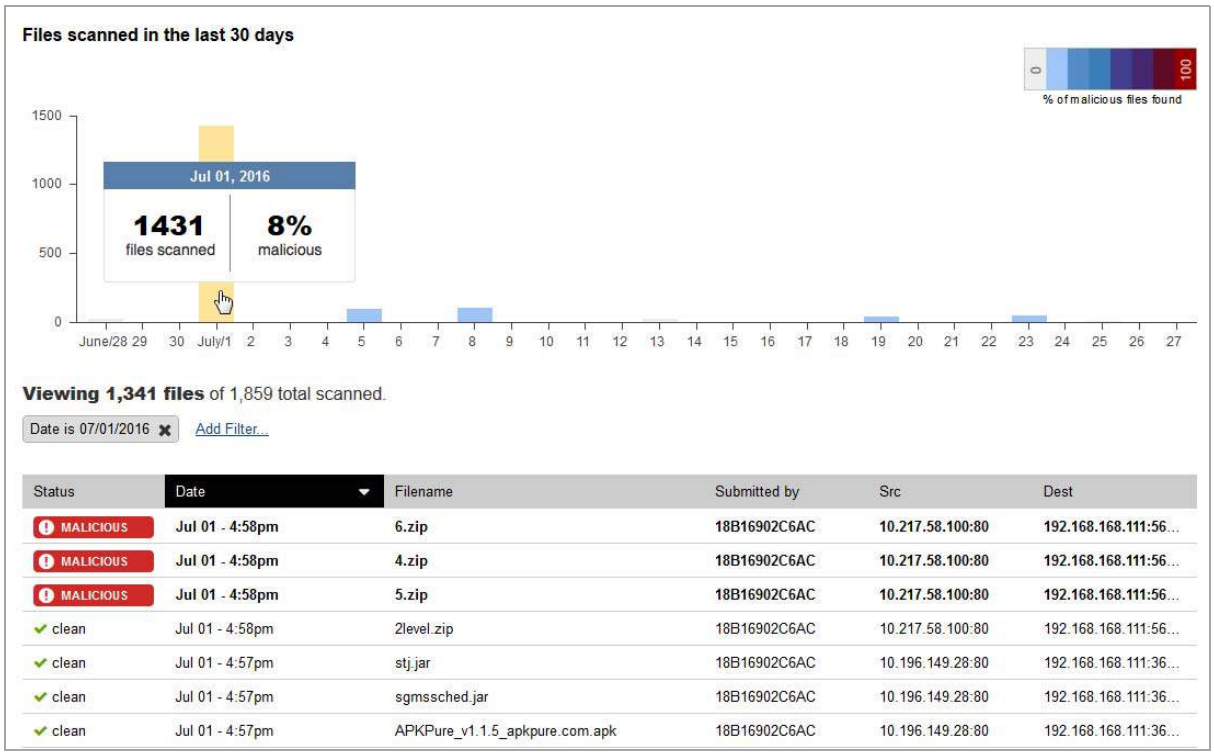
No filters applied. Add Filter...

Status	Date	Filename	Submitted by	Src	Dest
clean	Jul 25 - 5:56pm	FileZilla_Server-0_9_57.exe	(uploaded)	127.0.0.1	127.0.0.1
clean	Jul 24 - 10:08pm	s.jar	18B16902C6AC	10.217.58.100:80	192.168.168.9:3613
clean	Jul 24 - 10:01pm	stj.zip	18B16902C6AC	10.217.58.100:80	192.168.168.9:2933
clean	Jul 23 - 11:19am	vsjitdebugger.exe	18B16902C6AC	10.217.58.100:80	192.168.168.9:48726
clean	Jul 23 - 11:19am	vssadmin.exe	18B16902C6AC	10.217.58.100:80	192.168.168.9:48727
clean	Jul 23 - 11:19am	w32tm.exe	18B16902C6AC	10.217.58.100:80	192.168.168.9:48728
clean	Jul 23 - 11:19am	waitfor.exe	18B16902C6AC	10.217.58.100:80	192.168.168.9:48729
clean	Jul 23 - 11:19am	wecutil.exe	18B16902C6AC	10.217.58.100:80	192.168.168.9:48730
clean	Jul 23 - 11:19am	wermgr.exe	18B16902C6AC	10.217.58.100:80	192.168.168.9:48731
MALICIOUS	**Jul 23 - 11:19am**	**test2.zip**	**18B16902C6AC**	**10.217.58.100:80**	**192.168.168.9:48716**
clean	Jul 23 - 11:19am	test3.zip	18B16902C6AC	10.217.58.100:80	192.168.168.9:48717

When you hover over a bar, a popup shows the actual numbers of files scanned and malicious files found.



You can click on a single bar in the graph to set the filter for the log table to show the details of that bar only.



The log table allows you to scroll through the list of scanned files. If a scan fails, that row is dimmed. If a malicious file is found, that row is bolded. Clicking on any row opens the threat report. For more information about threat reports, see Viewing Threat Reports.

The heading for this page is dynamic and may appear in two states:

- When no filters are applied - Viewing n files scanned.
- When filters are applied - Viewing n files of n total scanned.

The columns for the log table are:

- The STATUS column displays these states:
  - scan pending - the scan is still in progress
  - clean - the scan has completed, but no judgment is confirmed yet
  - scan failed - the scan has failed
  - MALICIOUS - the scan has completed, and the judgment is malicious (the word MALICIOUS is displayed in small caps in a red tag with a warning symbol)
- The **Filename** column displays the name of the file.
- The **Date** column displays the date that the file was scanned.
- The **Submitted** by column displays the serial number of the firewall that submitted the file to Capture ATP.
- The **Src** column displays the source IP address where the file originated.
- The **Dest** column displays the destination IP address where the file was sent.

The columns can be sorted as follows:

- Currently, the Date column can be sorted in ascending or descending order.
- The default sort order is reverse chronological order with the most recent items on top.

- The heading for a sorted column has a black background with an arrow indicating the direction of the sort.
- Clicking the column heading sorts that column and toggles it in ascending or descending order.
- The selected sort order is persistent as filters are added or removed.

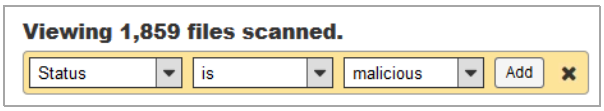
Filtering the log table

You can filter the entries in the log table by adding a filter that only displays certain criteria for a certain column, such as the status, date, or src, and so on.

To add a filter to the log table:

1 On the **Capture ATP > Status** page, click the **Add filter...** link.

The filter builder bar appears.



2 Select the criteria you want from the drop-down menus:

a From the first drop-down menu, select the column name, such as **Status**.

b From the second drop-down menu, select the operator: **is** or **is not**.

c From the third drop-down menu, select the appropriate criteria for the selected column.

3 Click **Add**.

The filter builder bar disappears, and a filter tag is created.

NOTE: Only one type of filter can be applied to the log table at a time.

The **Add Filter...** link reappears after the filter is added and the table results are updated immediately.

If you press **X**, the filter tag disappears and the filter is not applied to the log table.

Uploading a file for analysis

You can upload files to be scanned using the **Upload a File** button on the **Capture ATP > Status** page.

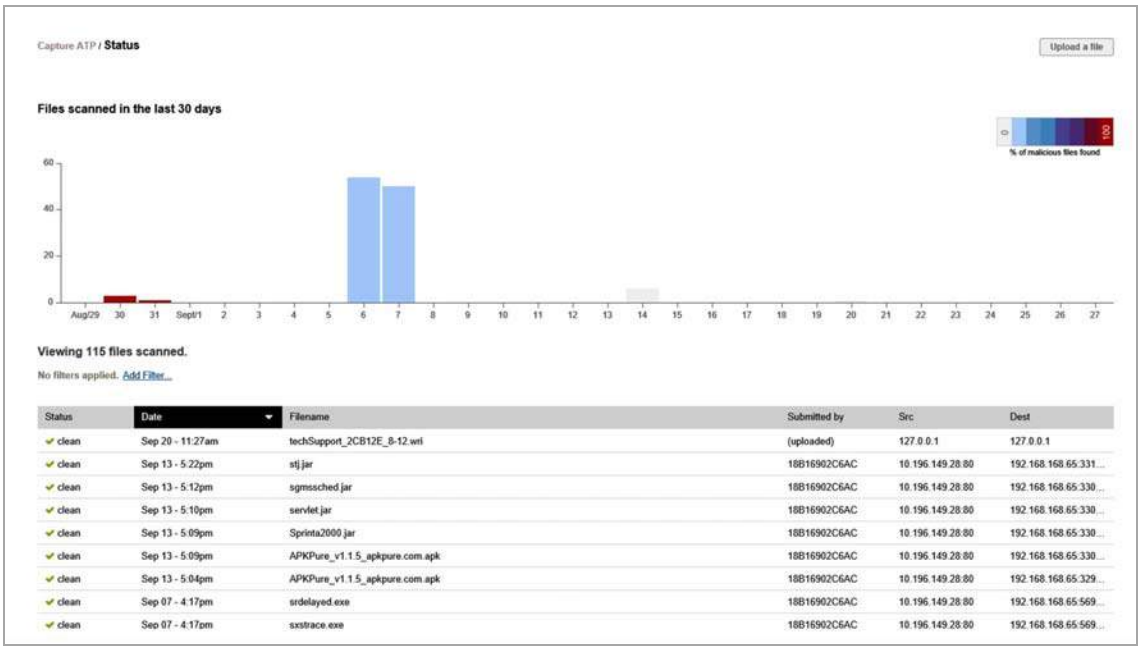
To upload a file for scanning, complete the following steps:

1 Click the **Firewall** tab.

2 Select a SonicWall appliance.

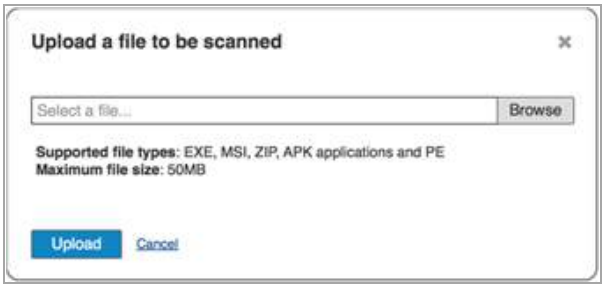
3 Click **Capture ATP > Status**.

The files scanned status report appears.



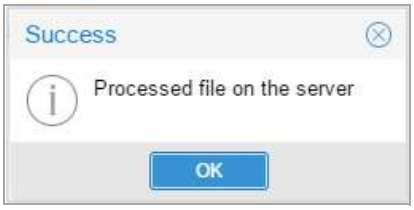
1 On the **Capture ATP > Status** page, click **Upload a File**.

The upload a file to be scanned dialog appears.

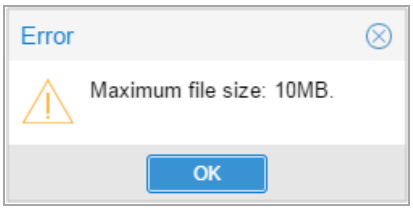


2 Click **Browse**, locate, and select the file you want to scan.

If the upload completes successfully, this message is shown:



If upload fails, an error message is displayed. If it fails because of file size limitations, you will see an error message similar to this:



Viewing threat reports

When you click on any row in the logs table on the **Capture ATP > Status** page, the Capture ATP threat report appears in a new browser window. The report format varies depending on whether a full analysis was performed or the judgment was based on preprocessing.

Topics:

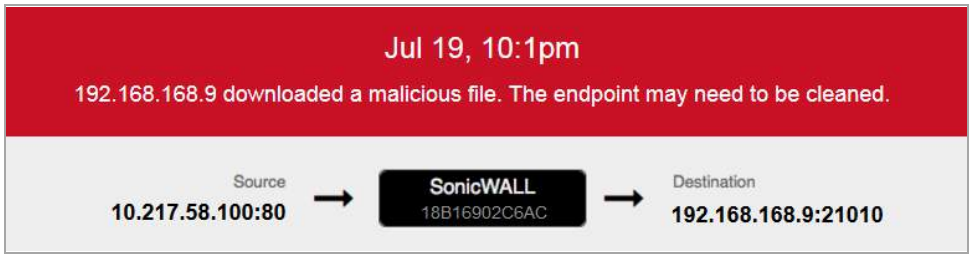
Launching the threat report from the logs table

You can launch a threat report by clicking on any row in the logs table on the **Capture ATP > Status** page. Hovering your mouse pointer over a row highlights it, and you can click anywhere in the row to launch the threat report in a new browser window.

An exception exists for archives which do not contain any supported file types. In this case, no threat report is launched.

Viewing the threat report header

The report header is very similar among the various threat reports. This section describes the header components and variations.



Colored banner:

- The colored banner is red for a malicious file, and blue for a clean file.
- The top entry displays the date and time that the file was submitted to Capture ATP for analysis.
- Below the date and time, a summary of the result is displayed.

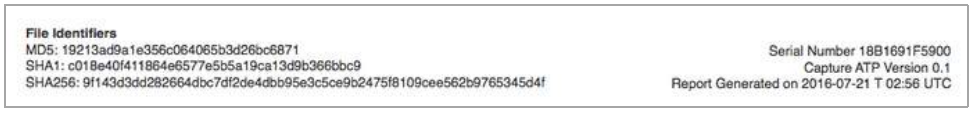
Lower banner:

- The lower part of the banner contains the connection information.
- On the left is the IP address (IPv4) and port number of the connection source. This is the address from which the file was sent.
- In the middle is the firewall identified by its serial number or friendly name.

- On the right is the IP address (IPv4) and port number of the connection destination. This is the address to which the file is being sent.

Viewing the threat report footer

The report footer is very similar among the various threat reports.



The File Identifiers are displayed at the left side of the footer. The following file identifiers are displayed, one per line:

- MD5
- SHA1
- SHA256

On the right side of the footer, the following information is displayed:

- **Serial Number** - This is the serial number of the firewall that sent the file. This is not displayed if the file was manually uploaded.
- **Capture ATP Version** - This is the software version number of the Capture ATP service running in the cloud.
- **Report Generated** - This is the timestamp in UTC format of when the report was generated.

Viewing the static file information

The static file information is displayed on the left side of the threat report, and is similar across all types of reports.

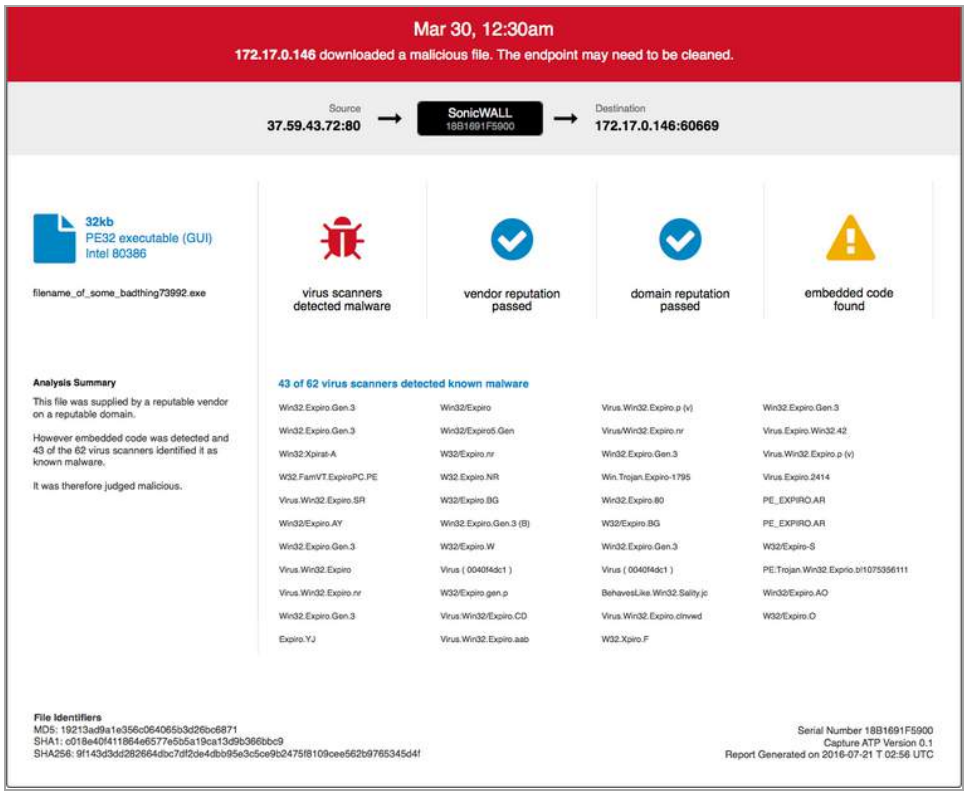
The file information includes:

- File size in kilobits (kb)
- File type
- File name as it was intercepted by the firewall

Viewing threat reports from preprocessing

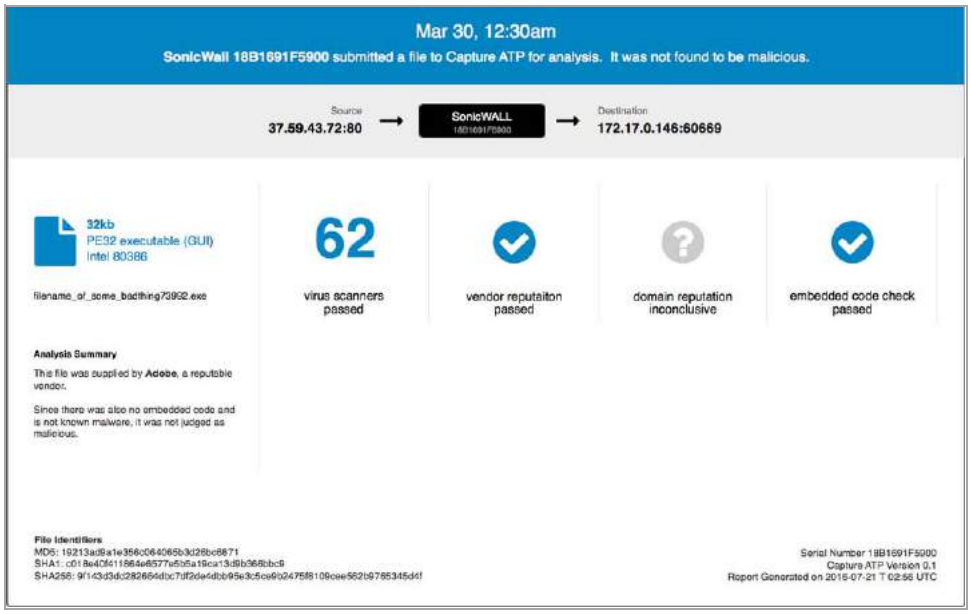
There are varying amounts of data on a preprocessor threat report, based on whether the file was found to be malicious or clean.

Preprocessor threat report for a malicious file:



The above threat report format is seen when the virus scans reveal malware in the file.

Preprocessor threat report for a clean file:



A clean threat report like the one shown above is seen in either of the following two cases:

Case one:

- Virus scans are inconclusive or all good.
- The file matches domain or vendor allow lists.

Case two:

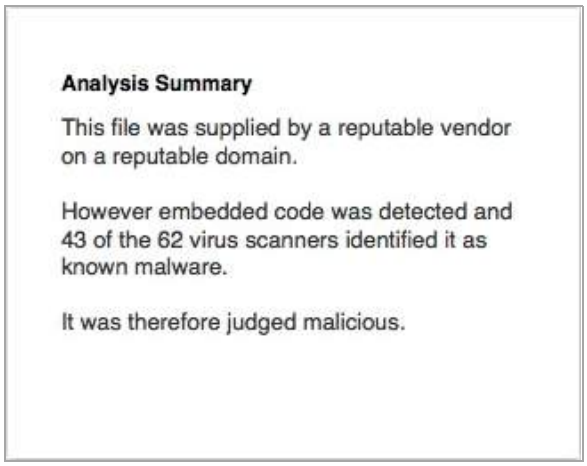
- Virus scans are inconclusive or all good.
- No embedded code is present in the file.

See the following topics for more information about preprocessor reports:

- Analysis summary and status boxes in preprocessor reports
- Malware names in preprocessor reports

Analysis summary and status boxes in preprocessor reports

Preprocessor threat reports contain an Analysis Summary section on the left side, which summarizes the findings based on the four phases of analysis during preprocessing.



The results from the four phases of preprocessing are displayed in the status boxes.

Each phase results in a true or false outcome. The following table shows what happens in the process depending on the result of each phase of the preprocessing.

Four areas of preprocessor analysis

Preprocessor phase result	Virus scanners detect malware?	Vendor reputation - on Allow list?	Domain reputation - on Allow list?	Embedded code found in the file?
True	Malicious	Non-malicious	Non-malicious	Continue analysis
False	Continue analysis	Continue analysis	Continue analysis	**Non-malicious**

Some phase results trigger an immediate judgment of either Malicious or Non-malicious, as indicated in the above table. Otherwise, that phase ends with the “Continue analysis” state.

If all phases of preprocessing result in the “Continue analysis” state, the file is sent to the cloud for full analysis by Capture ATP.

NOTE: The vendor reputation filter is only applicable to PE files, and the domain reputation might not be available for files delivered over SMTP. In these cases, the “Continue analysis” state is the phase result.

Malware names in preprocessor reports

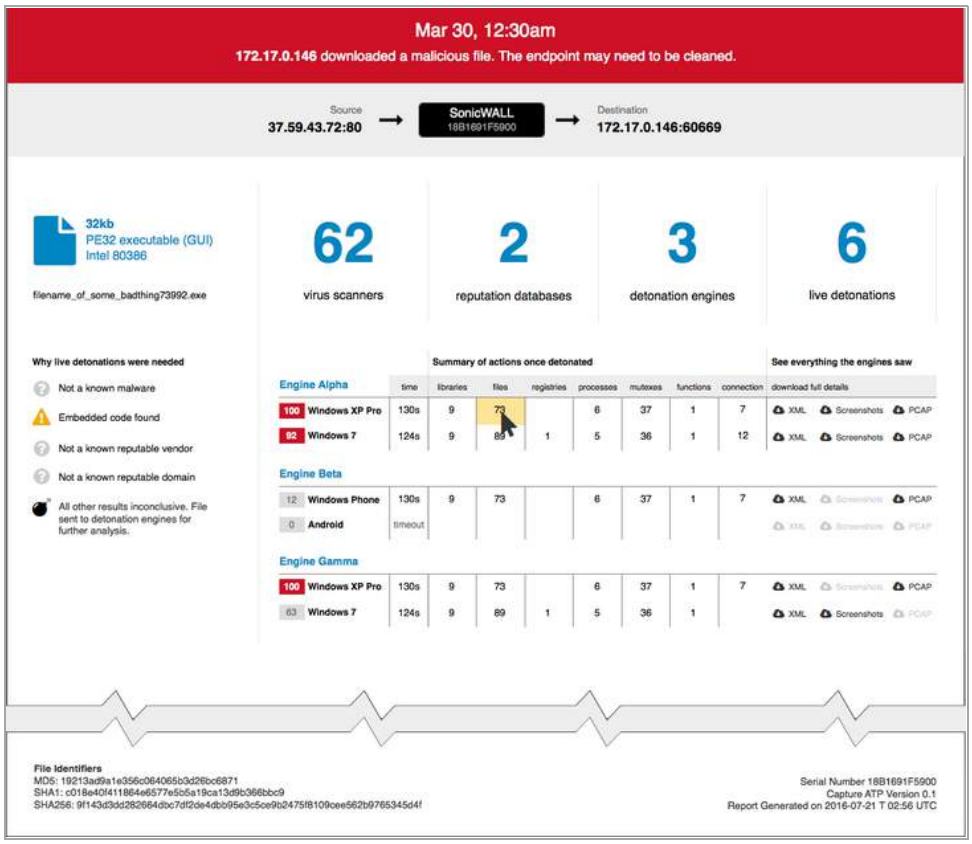
If the virus scanners detect known malware in the file, all virus names are listed in the content area of the report.

43 of 62 virus scanners detected known malware

Win32.Expiro.Gen.3	Win32/Expiro	Virus.Win32.Expiro.p (v)	Win32.Expiro.Gen.3
Win32.Expiro.Gen.3	Win32/Expiro5.Gen	Virus/Win32.Expiro.nr	Virus.Expiro.Win32.42
Win32:Xpirat-A	W32/Expiro.nr	Win32.Expiro.Gen.3	Virus.Win32.Expiro.p (v)
W32.FamVT.ExpiroPC.PE	W32.Expiro.NR	Win.Trojan.Expiro-1795	Virus.Expiro.2414
Virus.Win32.Expiro.SR	W32/Expiro.BG	Win32.Expiro.80	PE_EXPIRO.AR
Win32/Expiro.AY	Win32.Expiro.Gen.3 (B)	W32/Expiro.BG	PE_EXPIRO.AR
Win32.Expiro.Gen.3	W32/Expiro.W	Win32.Expiro.Gen.3	W32/Expiro-S
Virus.Win32.Expiro	Virus (0040f4dc1)	Virus (0040f4dc1)	PE:Trojan.Win32.Exprio.b!1075356111
Virus.Win32.Expiro.nr	W32/Expiro.gen.p	BehavesLike.Win32.Sality.jc	Win32/Expiro.AO
Win32.Expiro.Gen.3	Virus:Win32/Expiro.CD	Virus.Win32.Expiro.clnvwd	W32/Expiro.O
Expiro.YJ	Virus.Win32.Expiro.aab	W32.Xpiro.F	

Viewing threat reports from a full analysis

Full analysis threat reports provide the same set of information for both malicious and non-malicious files, although the banner color is different.



This Threat Report format is used when the following conditions occur:

- Virus scans are inconclusive or all good.
- Embedded code is present in the file.
- The file does not match domain or vendor allow lists.

See the following topics for more information about full analysis reports:

- Why live detonations were needed
- Status boxes in a full analysis threat report
- Analysis engine results tables

Why live detonations were needed

The left side of the full analysis threat report displays a summary of the preprocessing results as an explanation of why live detonations were needed. The term live detonations is used to indicate that one or more analysis engines and multiple environments were used to analyze the file in the cloud servers.

The set of preprocessing results which lead to full analysis of the file is shown below:

Status boxes in a full analysis threat report

The status boxes in full analysis threat reports display status from preprocessing results as well as information about the analysis performed in the cloud servers.

Virus scanners:

- This is the number of Anti-Virus vendors used, regardless of the judgment from each.
- SonicWall Gateway Anti-Virus and Cloud Anti-Virus each count as one.
- Additional virus scanners from many AV products and online scan engines are included in the total.

Reputation databases:

- One is the vendors allowed list.
- One is the domains allowed list.

Detonation engines:

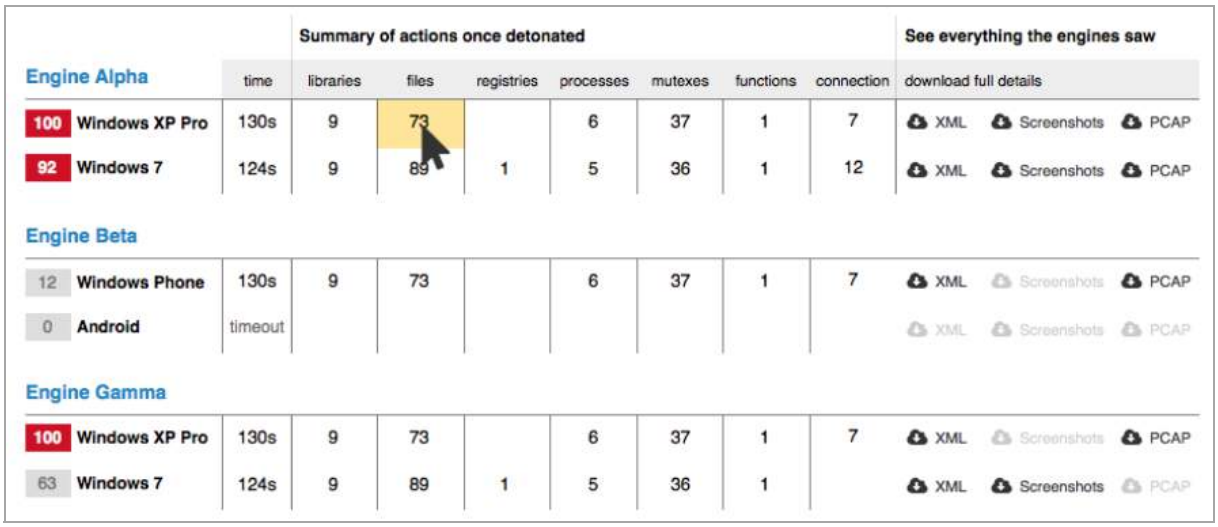
- This is the number of analysis engines used to analyze the file.
- One is the SonicWall analysis engine.
- Additional analysis engines from third-party vendors are included in the count.

Live detonations:

- This is the total number of environments used across all analysis engines.
- The environment is comprised of the analysis engine and the operating system on which it was run.

Analysis engine results tables

Under the status boxes, the full analysis threat report displays multiple tables showing the results from each analysis engine.



		Summary of actions once detonated							See everything the engines saw
Engine Alpha	time	libraries	files	registries	processes	mutexes	functions	connection	download full details
100 Windows XP Pro	130s	9	73		6	37	1	7	XML Screenshots PCAP
92 Windows 7	124s	9	89	1	5	36	1	12	XML Screenshots PCAP
Engine Beta									
12 Windows Phone	130s	9	73		6	37	1	7	XML Screenshots PCAP
0 Android	timeout								XML Screenshots PCAP
Engine Gamma									
100 Windows XP Pro	130s	9	73		6	37	1	7	XML Screenshots PCAP
63 Windows 7	124s	9	89	1	5	36	1		XML Screenshots PCAP

The engines are designated by names from the Greek alphabet, such as Alpha, Beta, Gamma, and so on.

Each row represents a separate environment, and indicates the operating system in which the engine was executed.

The overall score from the analysis in each environment is displayed in a highlighted box to the left of the operating system. The color of the box indicates whether the score triggered a malicious or non-malicious judgment:

- A score in a red box indicates a malicious judgment
- A score in a grey box indicates a non-malicious judgment

For each environment, the columns provide the analysis duration and a summary of actions once detonated:

- **Time** - The time taken by the analysis, using 's' for seconds, 'm' for minutes, and timeout if the analysis did not complete.
- **Libraries** - Cumulative count of malware libraries that were read during the analysis.
- **Files** - Cumulative count of files that were created, read, updated or deleted during the analysis.
- **Registries** - Cumulative count of OS registries that were read during the analysis.
- **Processes** - Cumulative count of processes that were created during the analysis.
- **Mutexes** - Cumulative count of mutual exclusion objects that were used during the analysis to lock a resource for exclusive access.
- **Functions** - Cumulative count of functions executed during the analysis.
- **Connection** - Cumulative count of network connections that were created during the analysis.

You can click any cell in the Summary of actions table to jump to the full data available further down in the report. Blank cells are not clickable.

The last column provides access to the full details of the analysis by the different engines:

- **XML** - Clicking here lets you open or save an XML file which contains all the detailed data behind the above counts.
- **Screenshots** - Clicking here lets you open or save a zip file of all the screenshots produced by the analysis.
- **PCAP** - Clicking here lets you open or save a packet capture file in libpcap format with details about the connections opened during the analysis.

Viewing Gateway Viruses Reports

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

To view Gateway Virus Reports, complete the following steps:

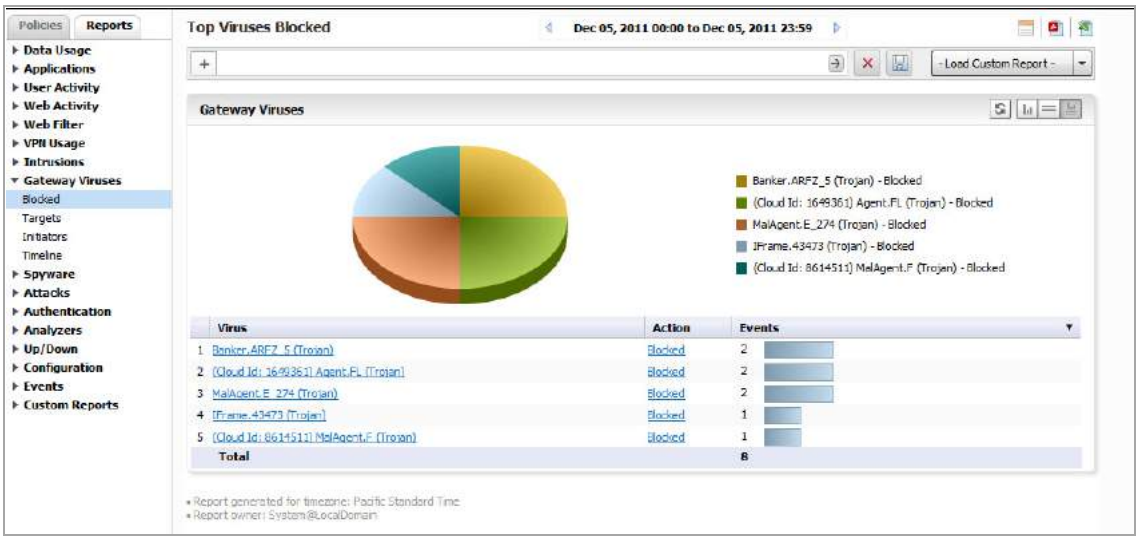
1 Click the **Firewall** tab.

2 Select a SonicWall appliance.

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.

To view Spyware Reports, complete the following steps:

1 Click the **Firewall** tab.

2 Select a SonicWall appliance.

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 Reports

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

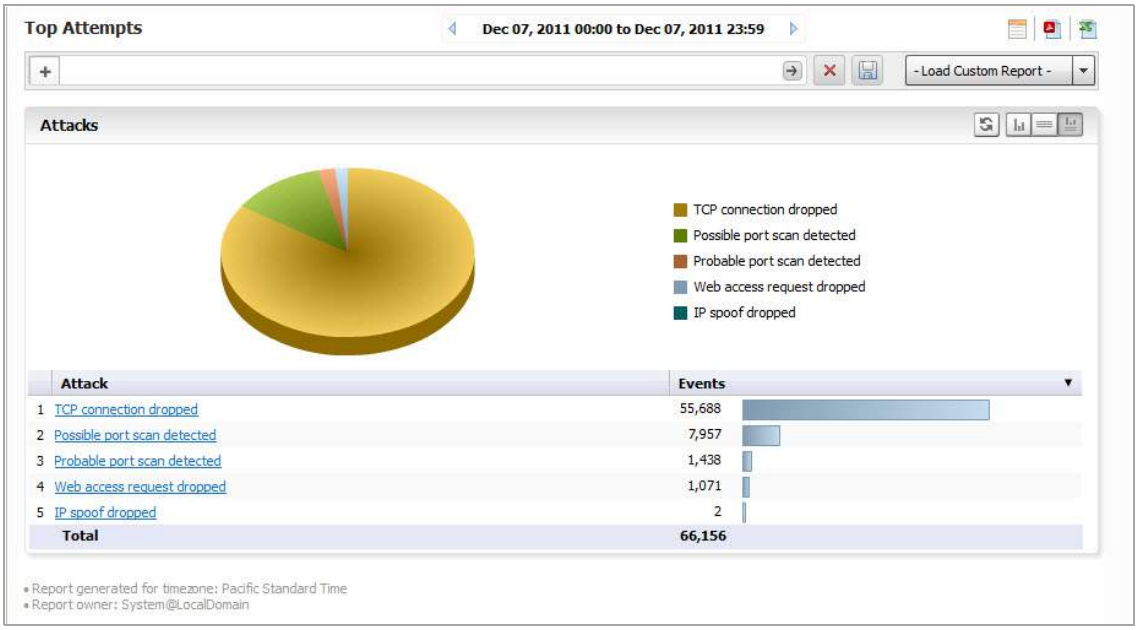
To view Attacks Reports, complete the following steps:

1 Click the **Firewall** tab.

2 Select a SonicWall appliance.

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.

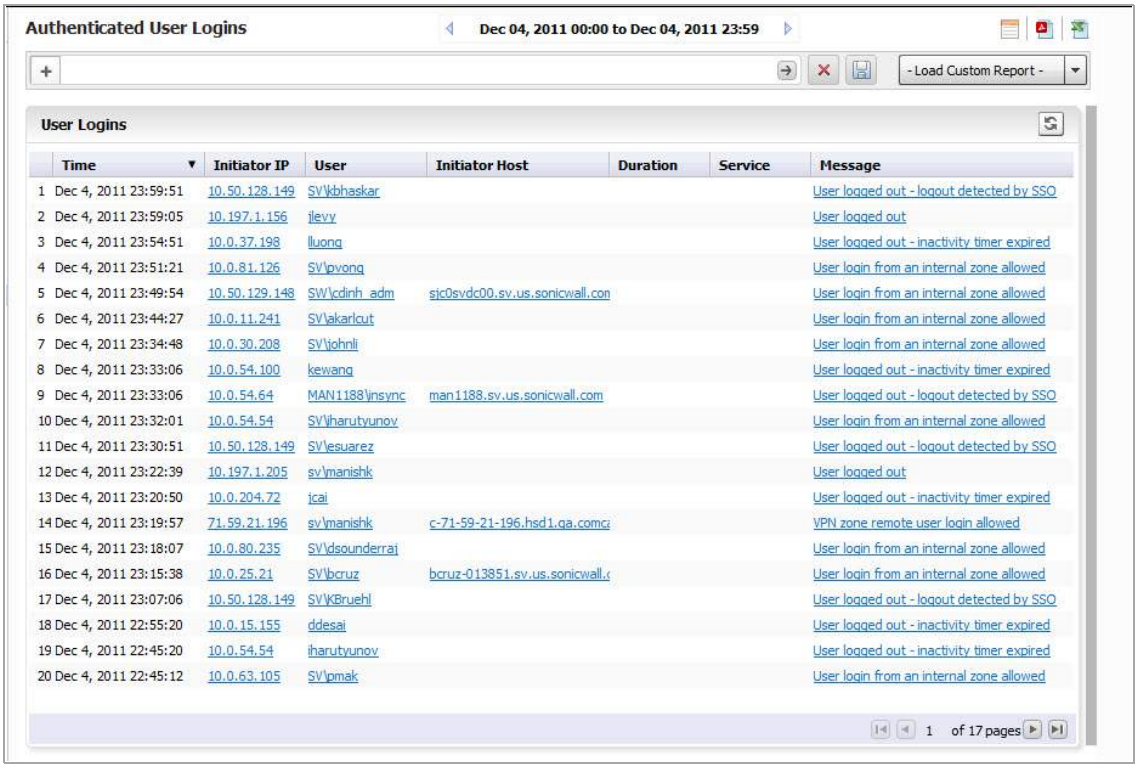
To view Authentication Reports, complete the following steps:

1 Click the **Firewall** tab.

2 Select a SonicWall appliance.

3 Click **Authentication > User Login**.

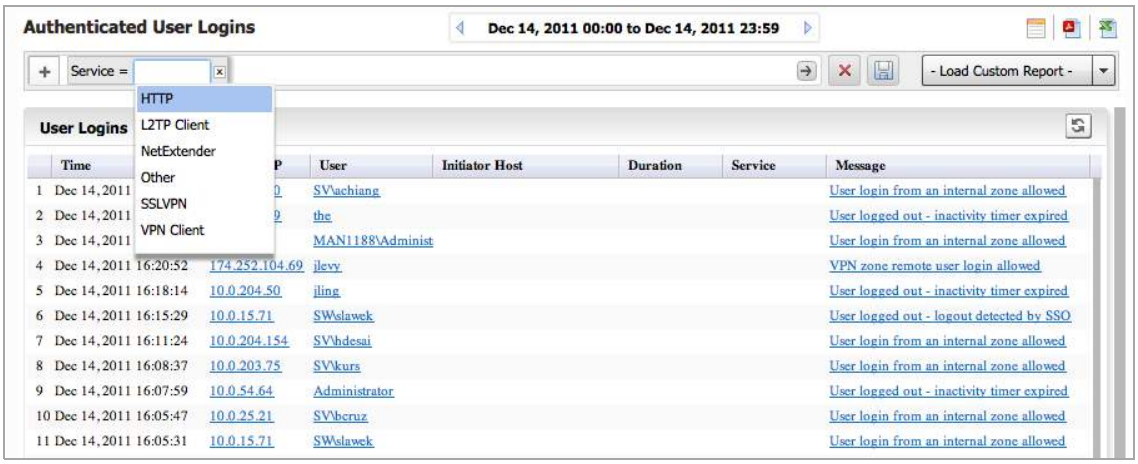
The Authentication report displays a list of authenticated users, their IP addresses, service, time they were logged in, and type of login/logout. Additional Reports are available for Administrator logins and failed login attempts.



Clicking on hyperlinks provides additional filtering for the reports.

You can filter on the Service to view SMA and other appliances by drilling down to the syslog:

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



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.

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 drop-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.

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, and so on. The Log Analyzer is only available at the individual unit level.

Because of space constraints, some column items, particularly the log event messages, might 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 drop-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.

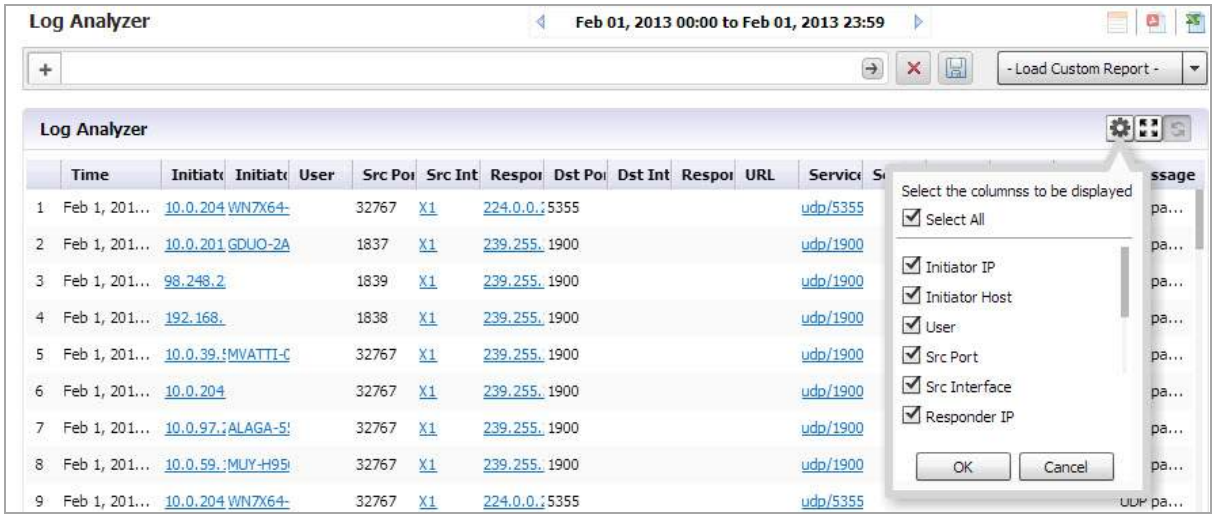
Viewing the Log Analyzer

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 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

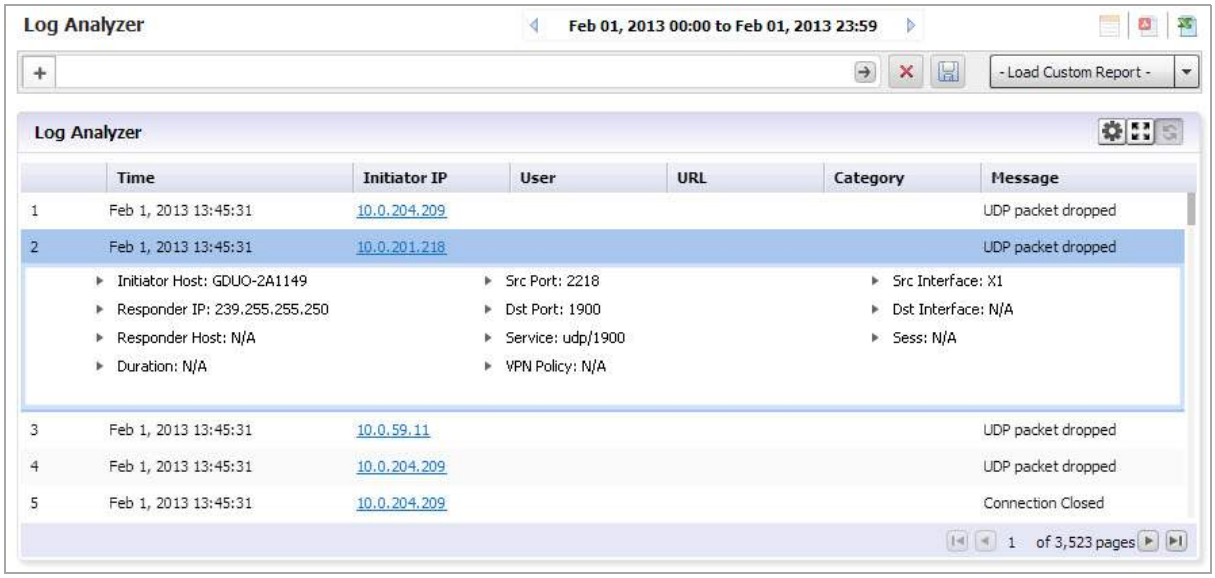
ones that you do not want to display. By configuring the displayed columns, the Log Analyzer gives a more clean, concise, and meaningful way to view the logs, instead of displaying unnecessary columns that take up valuable real estate.



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 information at once, the row-based expansion simplifies the screen and gives on-demand information through a single click.



Click on each row to drop-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 populates 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.

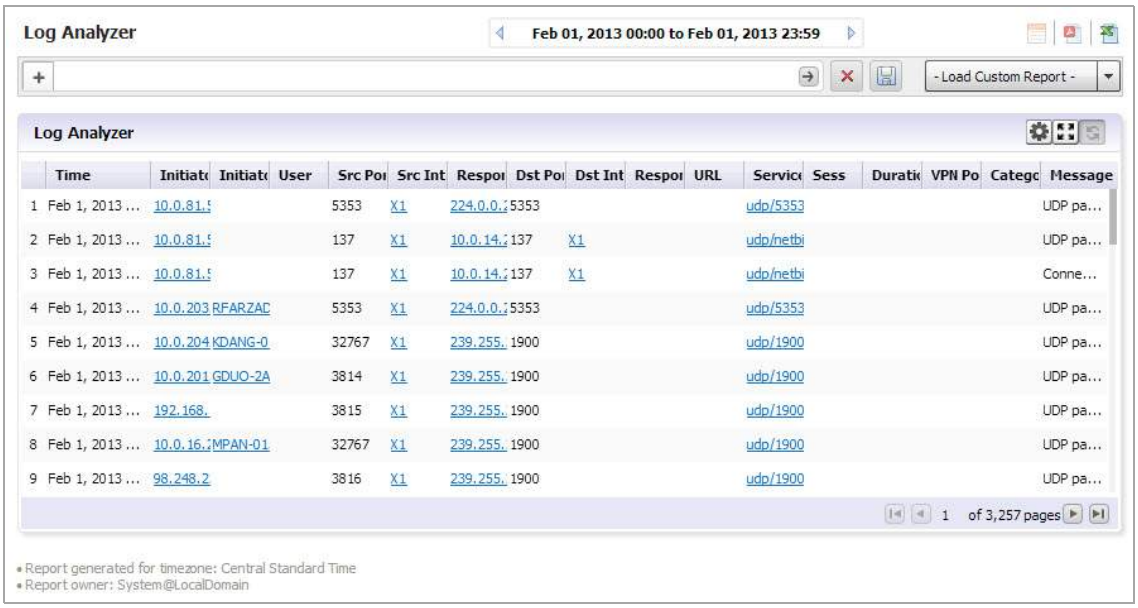
Filtering the Analyzer Log

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, complete the following steps:

1 Select a SonicWall appliance from the TreeControl pane.

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 are saved. If saving to PDF, a maximum of 2500 rows are saved. If saving to Excel, a maximum of 10,000 rows are saved.

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.

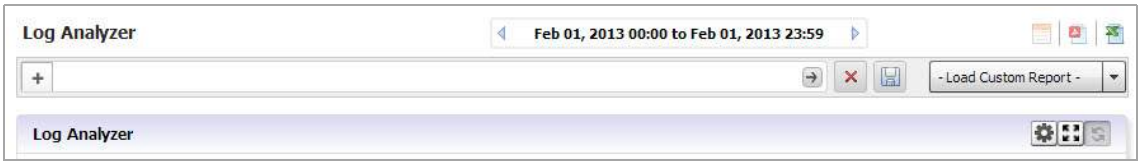
If you are viewing the log in the Log Analyzer view for a specific application entry, only those filters specific to that entry are available.

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

Log Analyzer Use Case

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

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

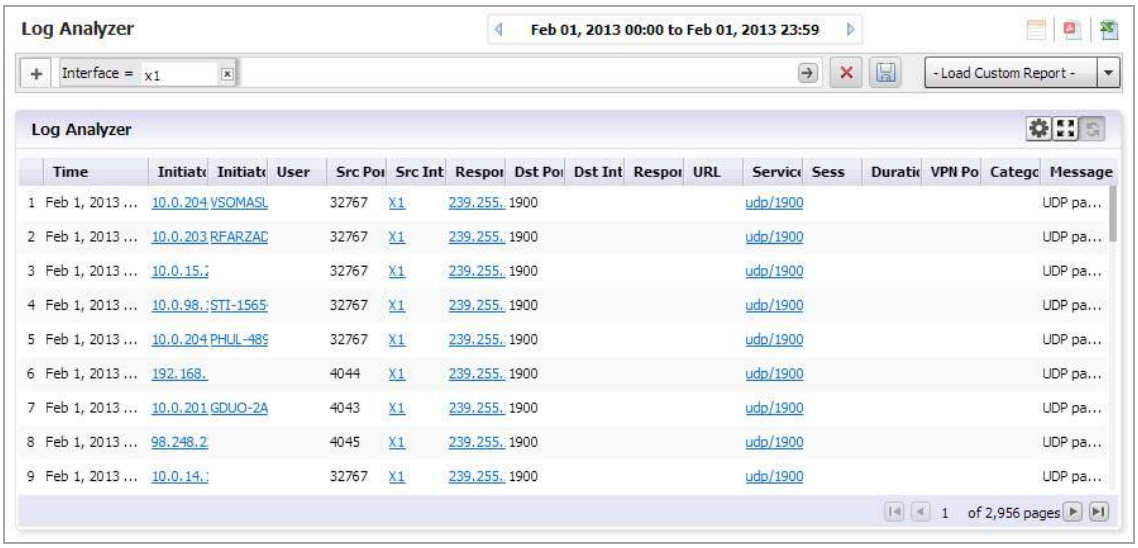


1 In the Log Analyzer, click on the + to add a filter, and select the **Interface** filter.

2 Type in X1 to specify the default interface filter.

3 Click **Go**.

The Log Analyzer is filtered on the X1 port interface.



This allows you to begin debugging, or further investigate the 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, by completing the following steps:

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

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

3 Click **Update**. The cost is immediately reflected 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

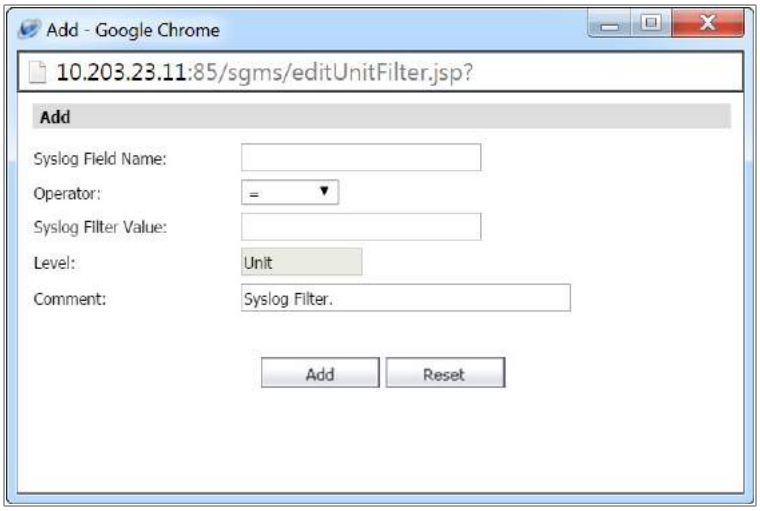
filtered syslogs are, however, stored in the file system and archived, thus ensuring that all syslogs are available for audit trailing purposes. Excluding data from being uploaded to the Reporting database in this way can be useful in maintaining confidentiality regarding use history, or eliminating 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

To add an Exclusion filter,

1 Click on **Configuration > Syslog Filter**.

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

2 To configure and add an Exclusion Filter, click **Add**. The Add Filter menu appears.



3 Specify the field you want to modify, and select an operator and value.

4 Add a comment to help identify the filter.

5 Click **Update**.

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

Viewing SMA Reports

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

This chapter contains the following sections:

SMA Reporting Overview

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

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

For a general introduction to reporting, see SonicWall Analyzer Reporting Overview on page 56.

SMA Reports Tab

The SMA tab gives you access to the Secure Mobile Access (SMA) 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 SMA Reporting?

Secure Mobile Access (SMA) 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 SMA reporting provides a visual presentation of User connectivity activity, Up_Down status, and other reports related to remote access. With SMA 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 SMA reporting. SonicWall appliances managed with SMA provide Resource Activity reports for tracking the source, destination, and other information about resource activity passing through a SonicWall SMA 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.

After 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 SMA Reporting

SMA 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 SMA reporting feature:

- SMA 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 SMA 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 three 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.

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

Using and Configuring SMA Reporting

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

- Viewing Available SMA Report Types on page 116
- Configuring SMA Scheduled Reports on page 117

Viewing Available SMA Report Types

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

1 Log in to your Analyzer management console.

2 Click the **SMA** tab.

The following types of reports are available:

Global Level Reports

- Data Usage
    - Summary: connections per SMA 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 SMA 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 SMA Scheduled Reports

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

To configure SMA 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 SMA Reports

SMA 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 SMA Summary Reports

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

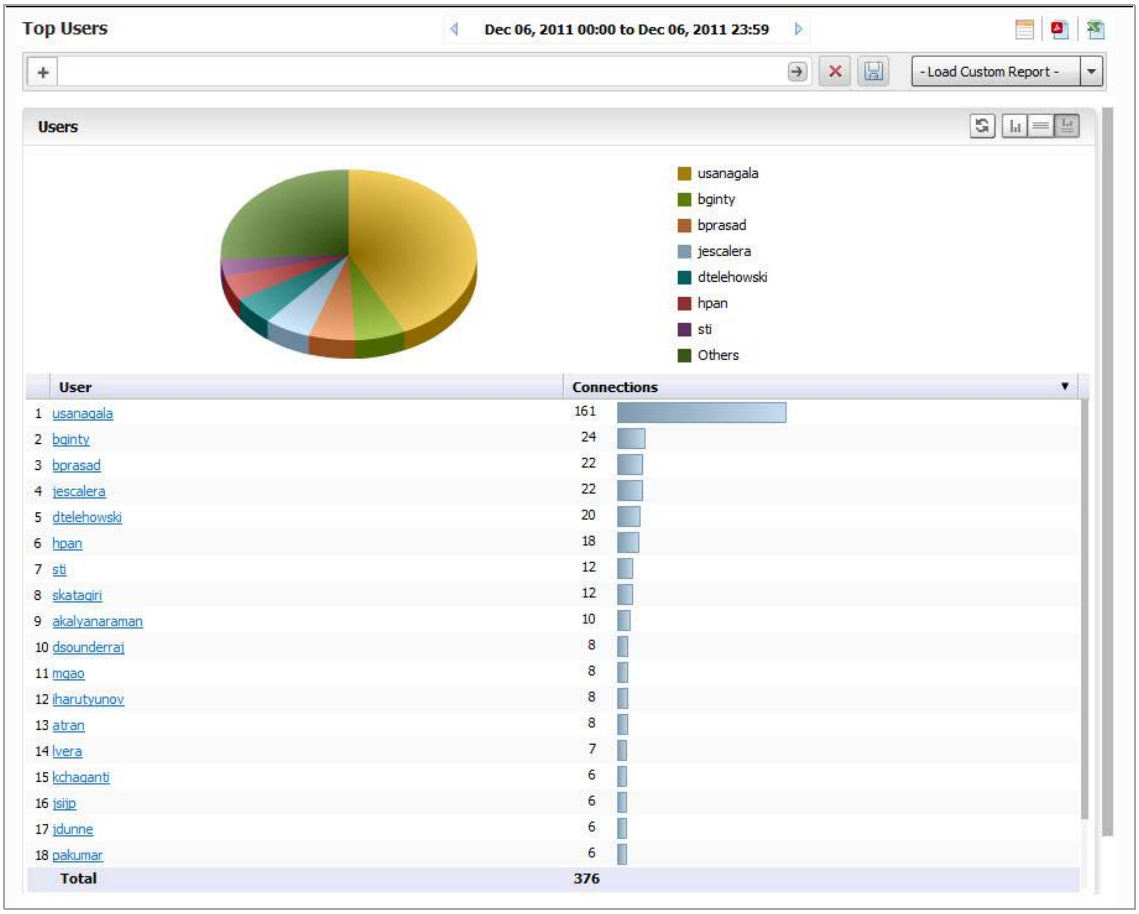
The SMA Summary report is available for Data Usage, Web Application Firewall (WAF), and Connections. It shows the number of connections handled by the SMA appliances on the specified day or interval. The grid-level reports lists each appliance by name, along with the number of connections.

To view the Data Usage Summary report, complete the following steps:

1 Click the **SMA** tab.

2 Select the global icon.

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 SMA 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.

Topics:

Viewing Unit-Level Data Usage Reports

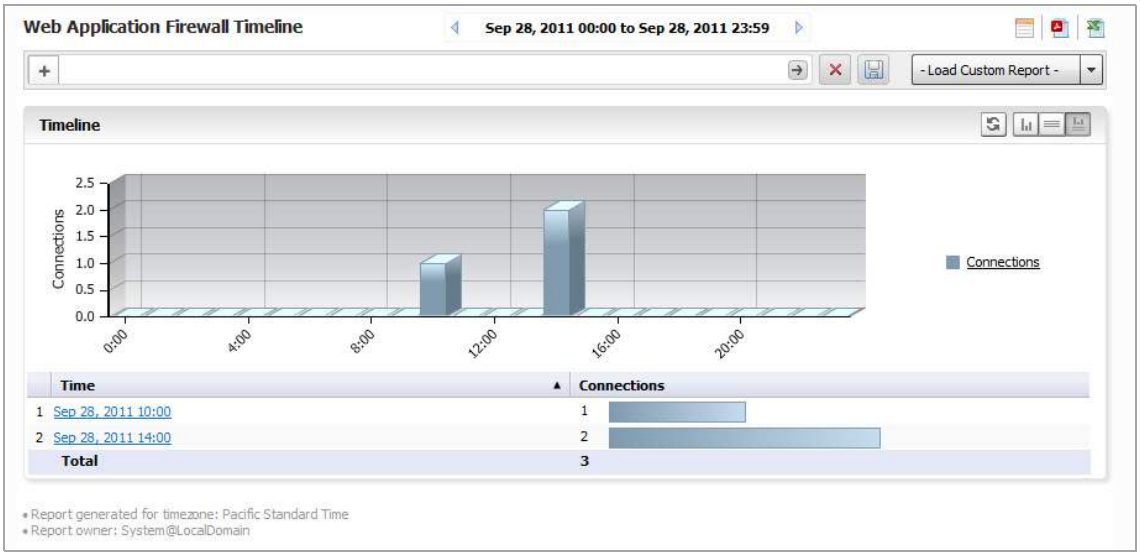
To view Unit-Level Data Usage Reports, complete the following steps:

1 Click the **SMA** tab.

2 Select the desired Unit.

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

4 The graph displays the number of connections to the selected SMA 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 SMA appliance

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 drop-down calendar.

6 After selecting a date, click **Search**. The Analyzer Reporting Module displays the report for the selected day.

NOTE: The date setting stays in effect for all similar reports during your active login session.

Viewing SMA Top Users Reports

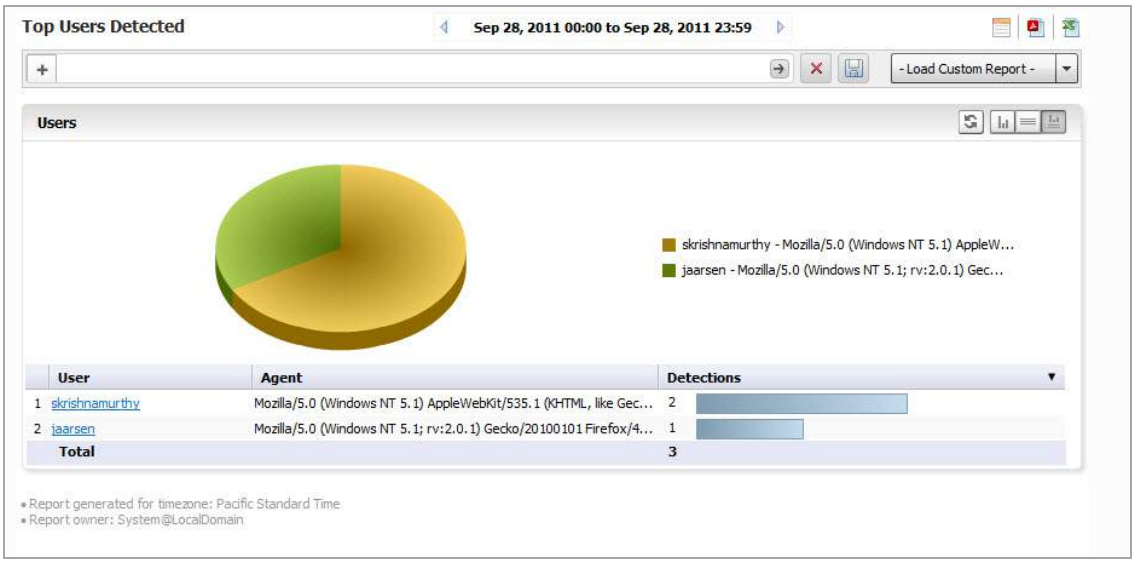
The Top Users report displays the users who used the most connections on the specified date.

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

1 Click the **SMA** tab.

2 Select the SMA appliance.

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



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 drop-down calendar.

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 takes 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 user.

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 displays a list of saved reports under the Filter Bar.

To create a new report, use the Filter Bar as described in the following steps:

1 Click the **Firewall** tab.

2 Select a SonicWall appliance.

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 displays, with the User filter pre-selected. You can enter a specific user name, or use the LIKE operator wildcards (*) to match multiple names.

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

The customized User Activity Details report displays 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 might 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

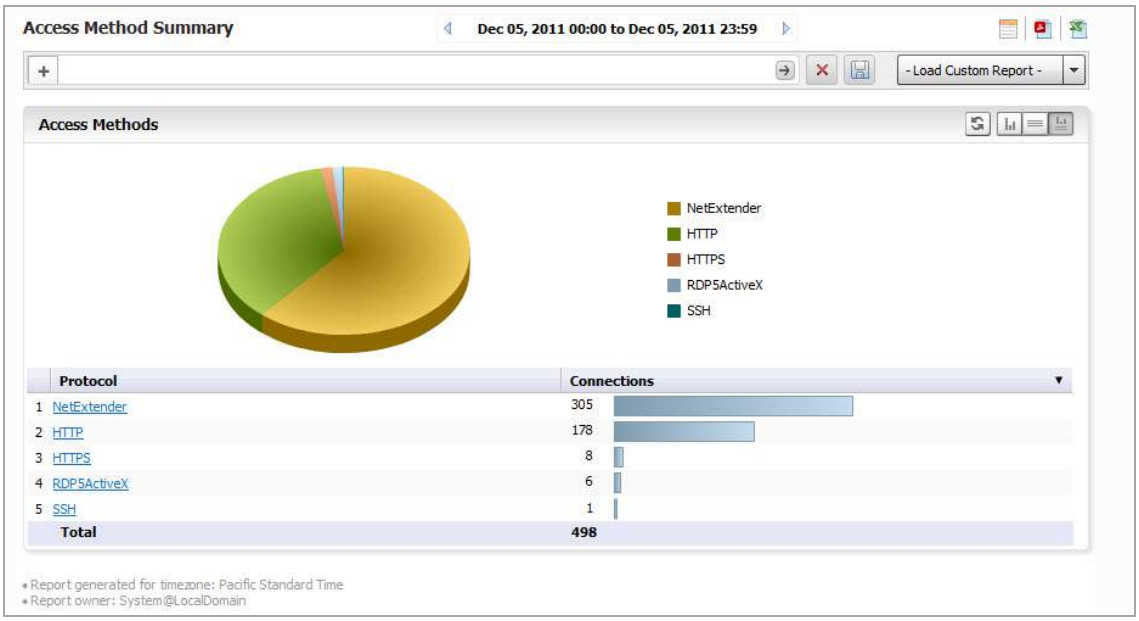
The Access Summary report provides an overview of the types of access protocols used. Clicking on a hyperlinked protocol entry takes you to the Log Analyzer view for more details.

To view the Summary Report, complete the following steps:

1 Click the **SMA** tab.

2 Select an SMA appliance.

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



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 display in the Log Analyzer report.

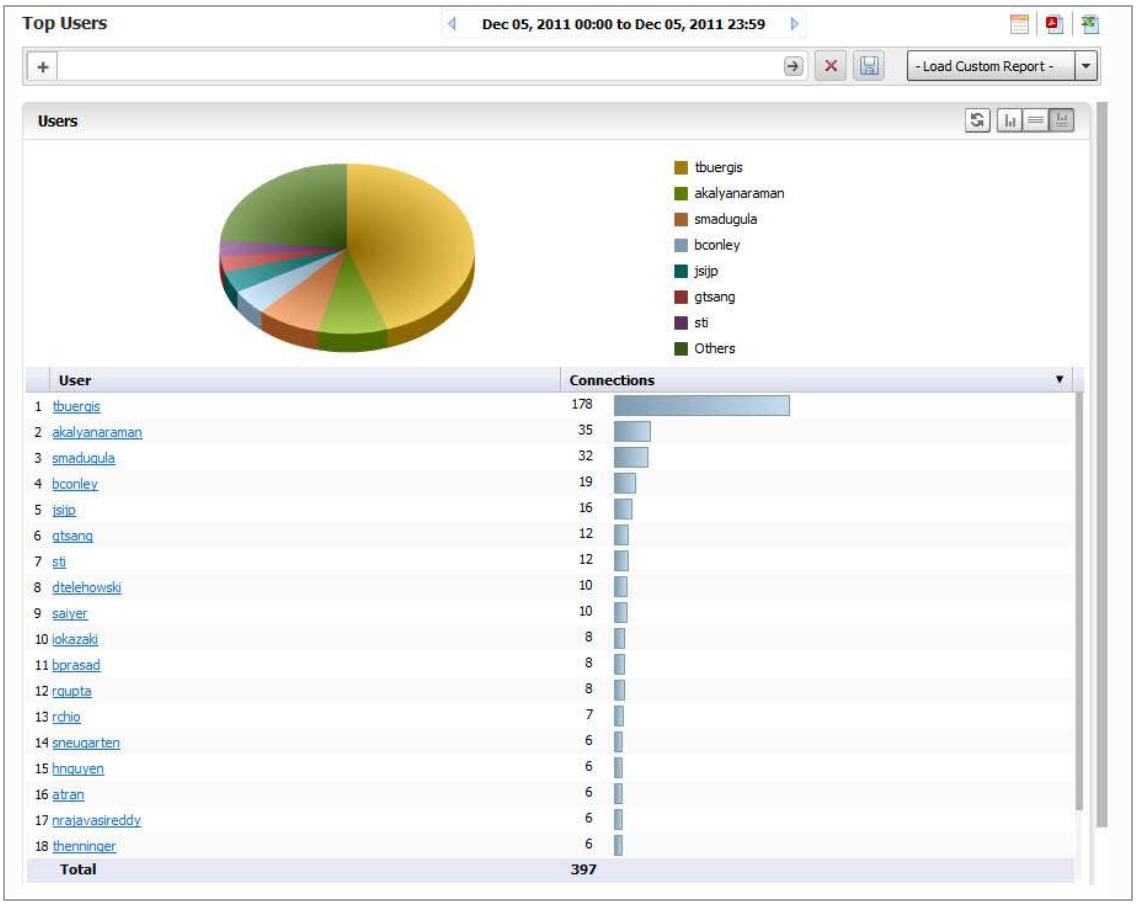
Viewing the Top Users Access Report

To view the Top Users Access Report, complete the following steps:

1 Click the **SMA** tab.

2 Select an SMA appliance.

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 are 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 SMA Authentication User Login Report

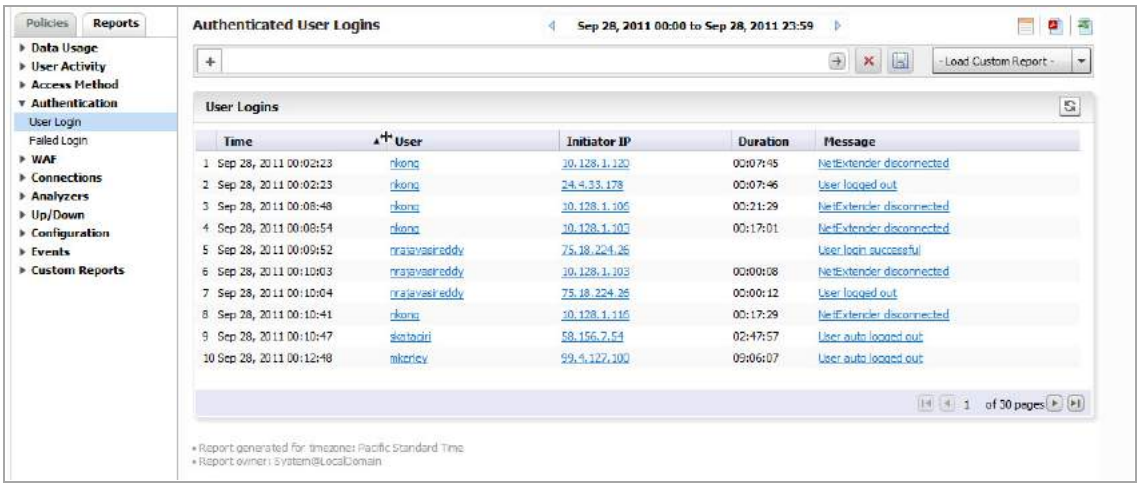
The Authentication Summary report shows an overview of user logins and login attempts and disconnections by time, user, IP address, type of connection/disconnection, and amount of time the connection was established. Authentication reports are only available at the unit level.

To view SMA Authentication User Login Reports, complete the following steps:

1 Click the **SMA** tab.

2 Select an SMA appliance.

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 SMA 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 SMA Authentication Failed Login Report

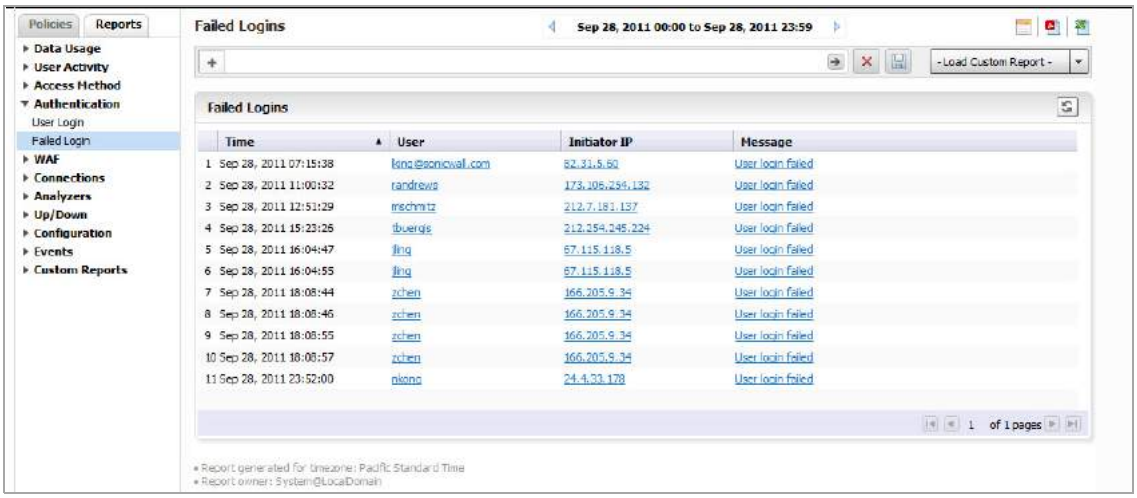
The Authentication Failed Login report shows an overview of user logins and login attempts and disconnections by time, user, IP address, type of connection/disconnection, and amount of time the connection was established. Authentication reports are only available at the unit level.

To view SMA Authentication Failed Login Reports, complete the following steps:

1 Click the **SMA** tab.

2 Select an SMA appliance.

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 SMA 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 the hyperlinks in these reports takes you to the Log Analyzer view, for more details.

To view reports, complete the following steps:

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

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

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.

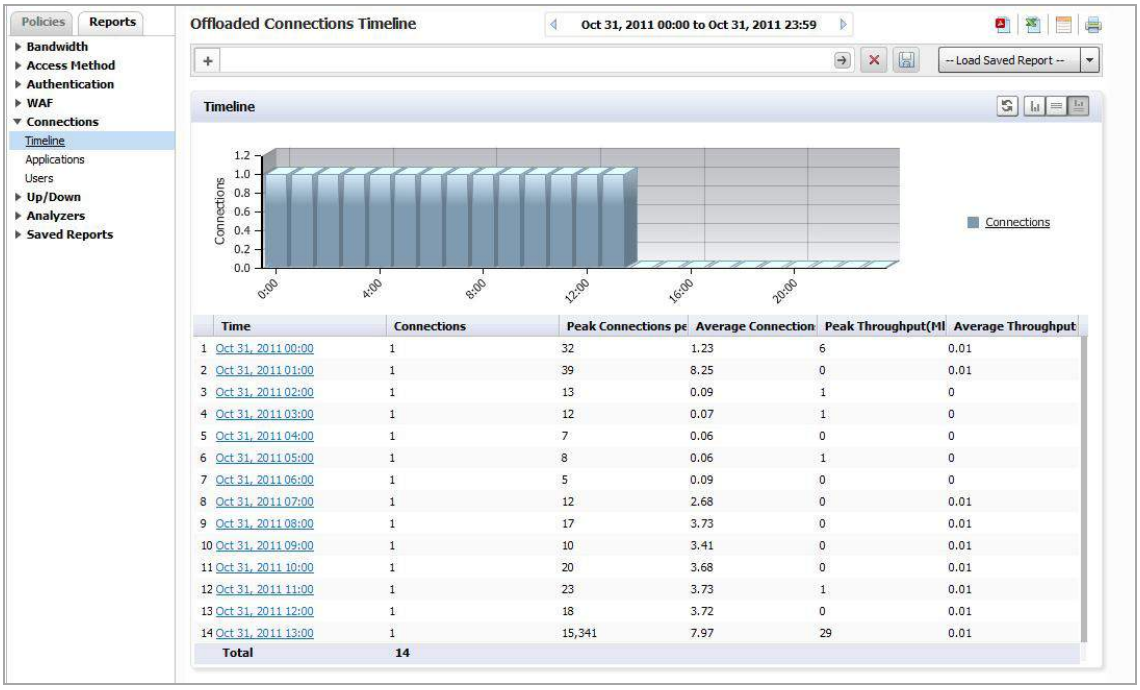
To view the Web Application Firewall Summary report, complete the following steps:

1 Click the **SMA** tab.

2 Select a SonicWall appliance.

3 Click **Connections > Timeline**.

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



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, complete the following steps:

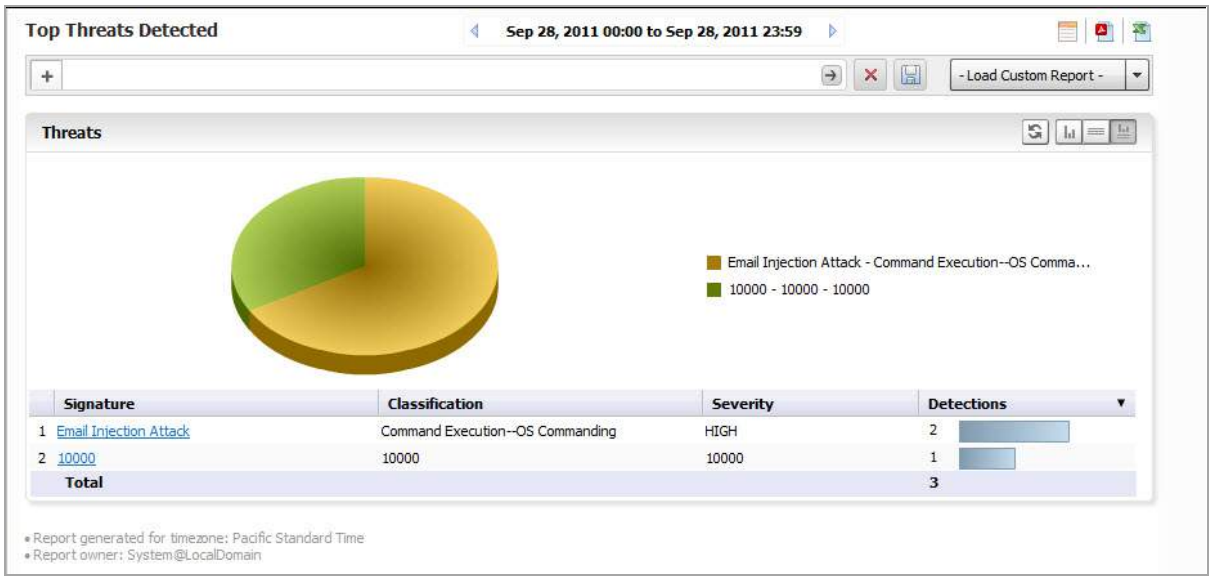
1 Click the **SMA** tab.

2 Select a SonicWall appliance.

3 Click the **Reports** tab.

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.



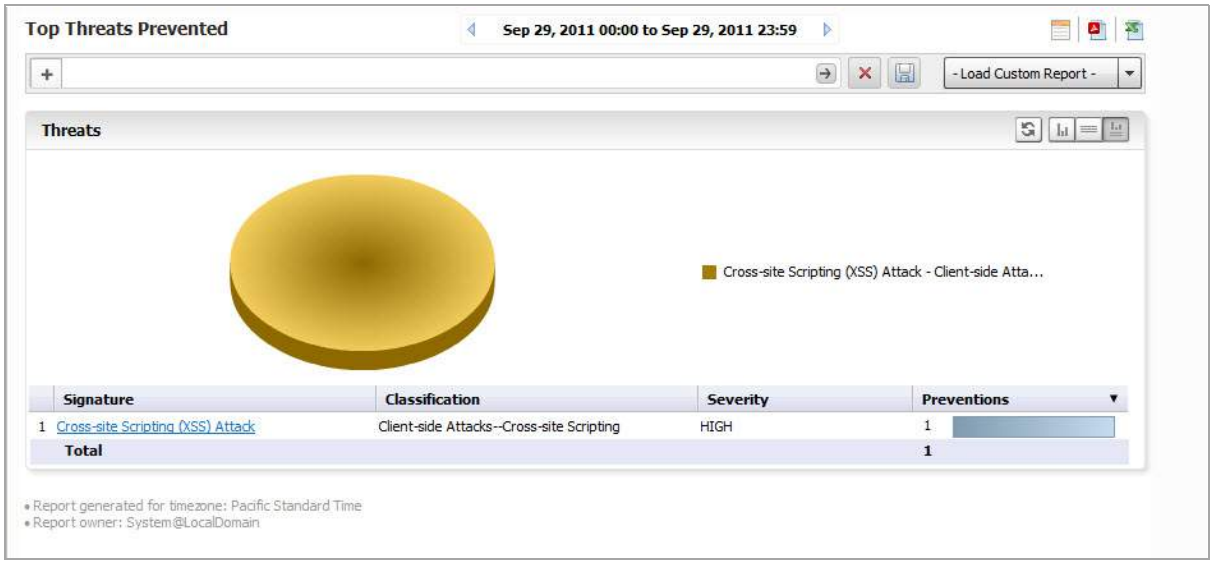
Click on the hyperlinks available in this report to go to the Log Analyzer.

Viewing WAF Top Threats Prevented

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

1. Click the **SMA** tab.
2. Select a SonicWall appliance.
3. Click on the **Reports** tab.
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, complete the following steps:

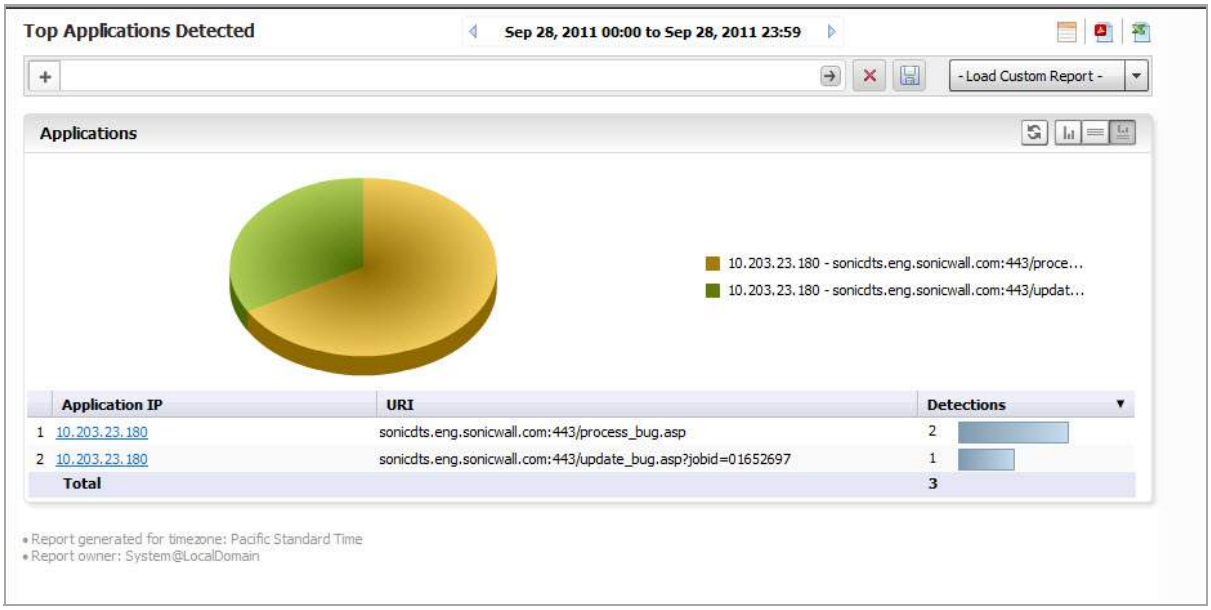
1 Click the **SMA** tab.

2 Select a SonicWall appliance.

3 Click the **Reports** tab.

4 Click **WAF > Applications Detected**.

The Top Applications Detected report lists applications with the most number of threats detected by the WAF process. It displays 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, complete the following steps:

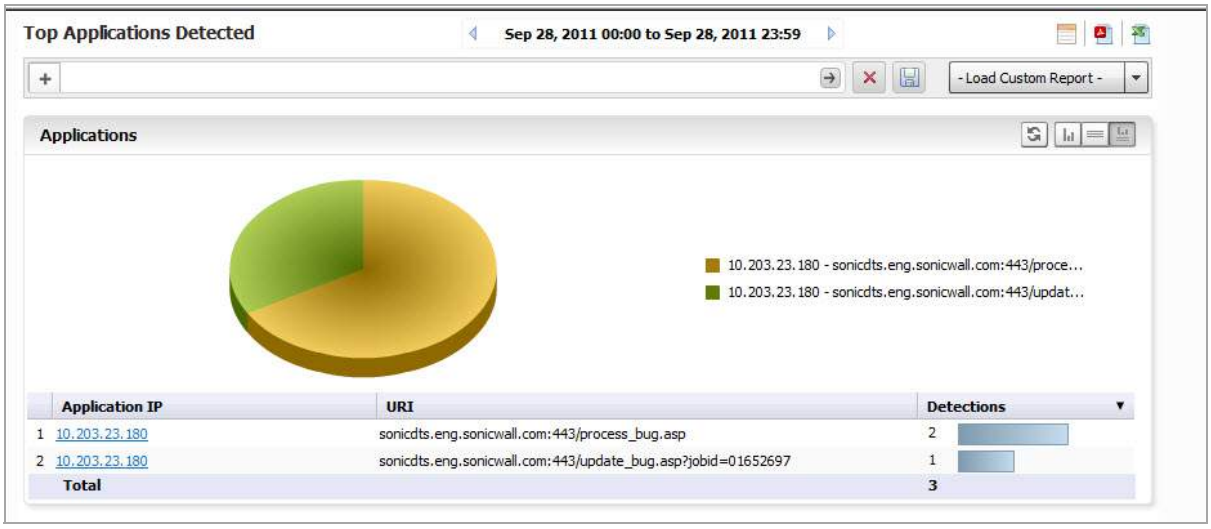
1 Click the **SMA** tab.

2 Select a SonicWall appliance.

3 Click the **Reports** tab.

4 Click **WAF > Applications Detected**.

The Top Applications Prevented report lists applications with the most number of threats prevented by the Web Application Firewall. It displays 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.

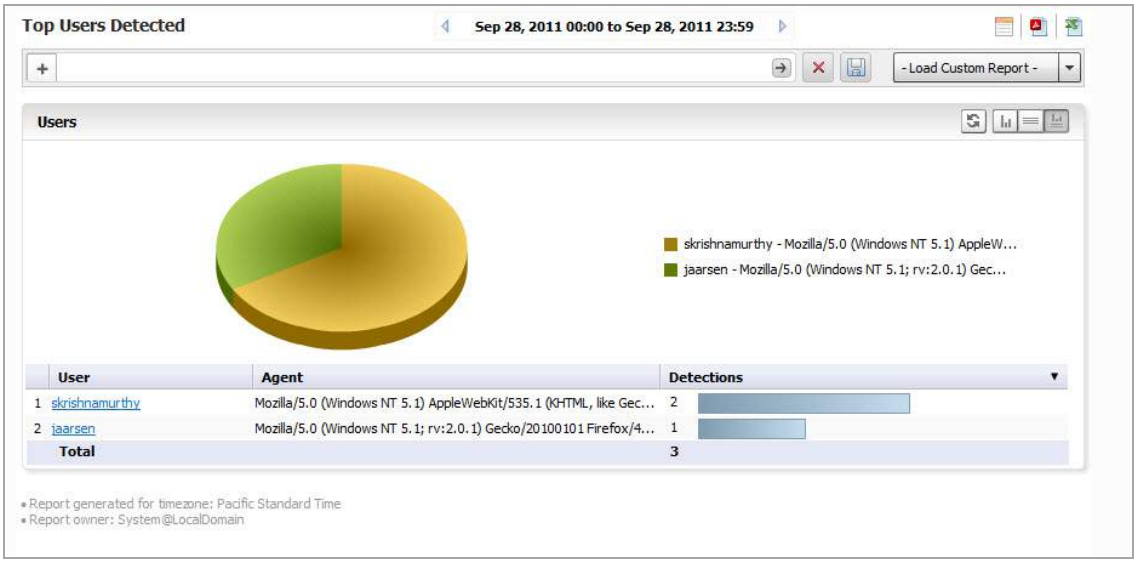
Viewing WAF Top Users Detected

The Top Users Detected report lists the top authenticated users from whom threats have been detected by the Web firewall. It displays 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, complete the following steps:

1. Click the **SMA** tab.
2. Select a SonicWall appliance.
3. Click the **Reports** tab.
4. Click **WAF > Users Detected**. The Top Users page displays.



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

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.

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 drop-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, complete the following steps:

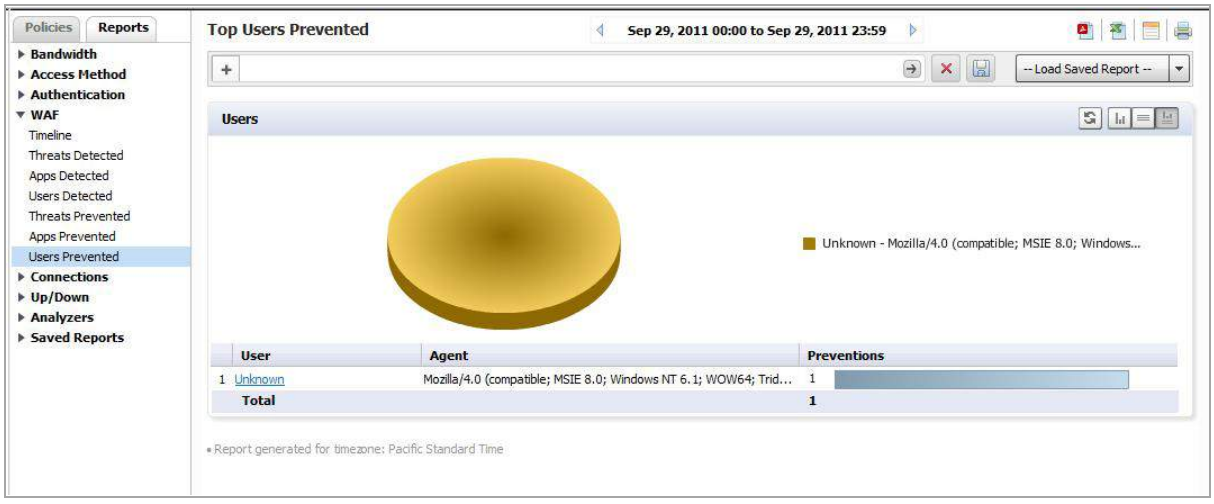
1 Click the **SMA** tab.

2 Select a SonicWall appliance.

3 Click the **Reports** tab.

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, complete the following steps:

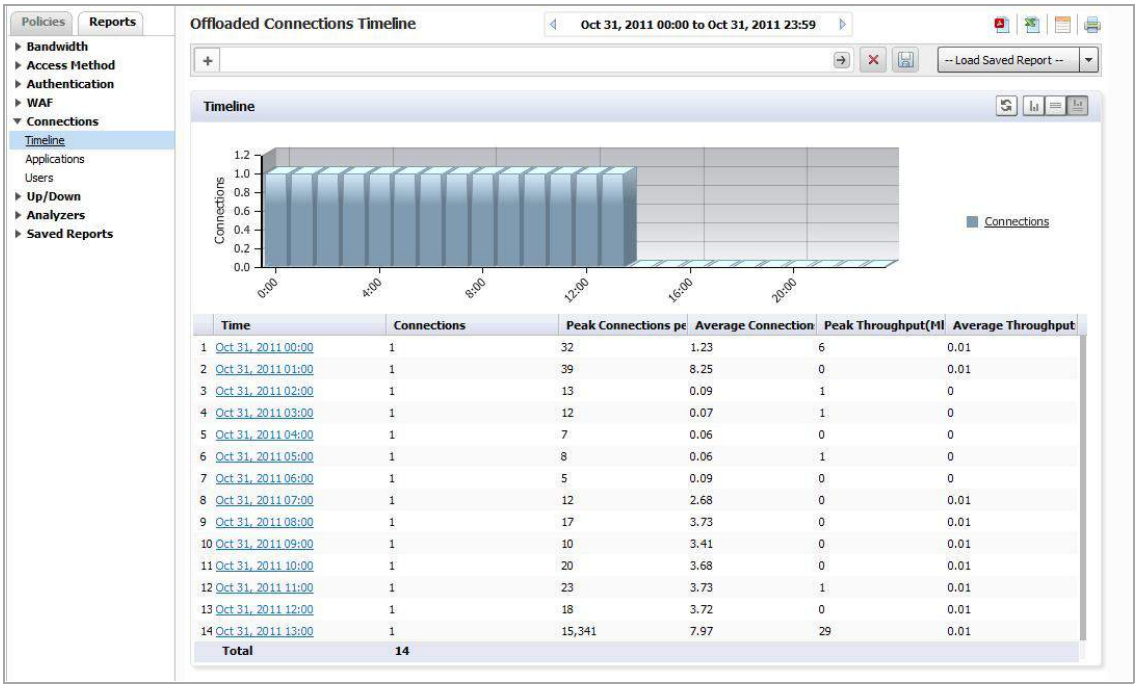
1 Click the **SMA** tab.

2 Select a SonicWall appliance.

3 Click the **Reports** tab.

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.

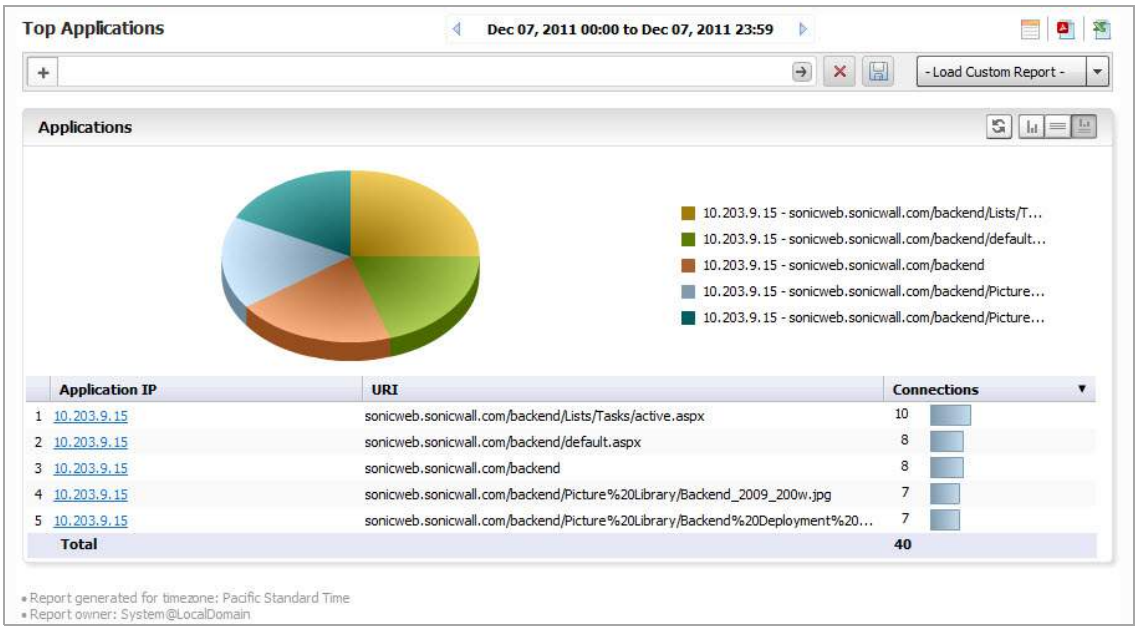
To view the report, complete the following steps:

1 Click the **SMA** tab.

2 Select a SonicWall appliance.

3 Click on the **Reports** tab.

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 drills down to the Top Applications, filtered by User Name.

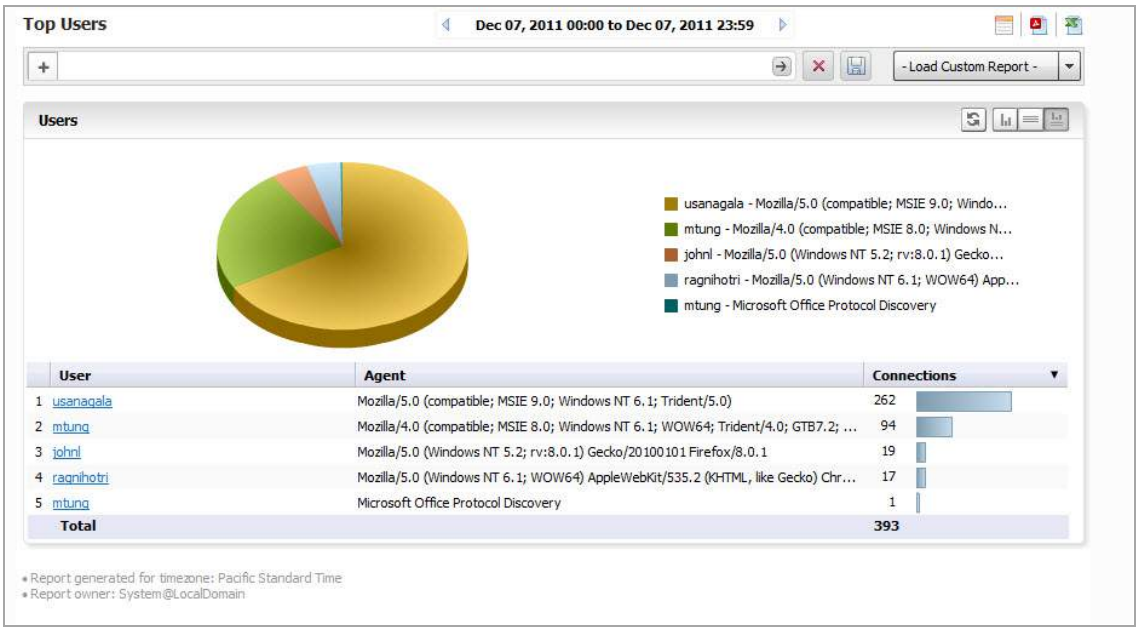
To view the report, complete the following steps:

1 Click the **SMA** tab.

2 Select a SonicWall appliance.

3 Click the **Reports** tab.

4 Click **Connections > Users**.



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

Viewing SMA Analyzer Logs

Topics:

Analyzer logs contain detailed information from the system logs on each transaction that occurred on the SMA 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, and so on. The Log Analyzer is only available at the individual unit level.

The SMA 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 SMA Reports takes you the Analyzer Log view of the information. Log information can be saved by using Save on the Filter Bar for a specific report. This report then appears in the list of Custom Reports.

For more information on the Log Analyzer, refer to Using the Log Analyzer on page 108.

Saving System Log Reports

To load the report for later viewing, either:

1 Click **Load Custom Report** and select from the drop-down list of saved Custom reports.

2 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 information is stored. For more information, see Configuring SMA Scheduled Reports on page 117 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 are saved. If saving to PDF, a maximum of 2500 rows are saved. If saving to Excel, a maximum of 10,000 rows are saved.

Viewing the Analyzer Log for an SMA Appliance

To view the Log, complete the following steps:

1 Click the **SMA** tab.

2 Select an SMA appliance.

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.

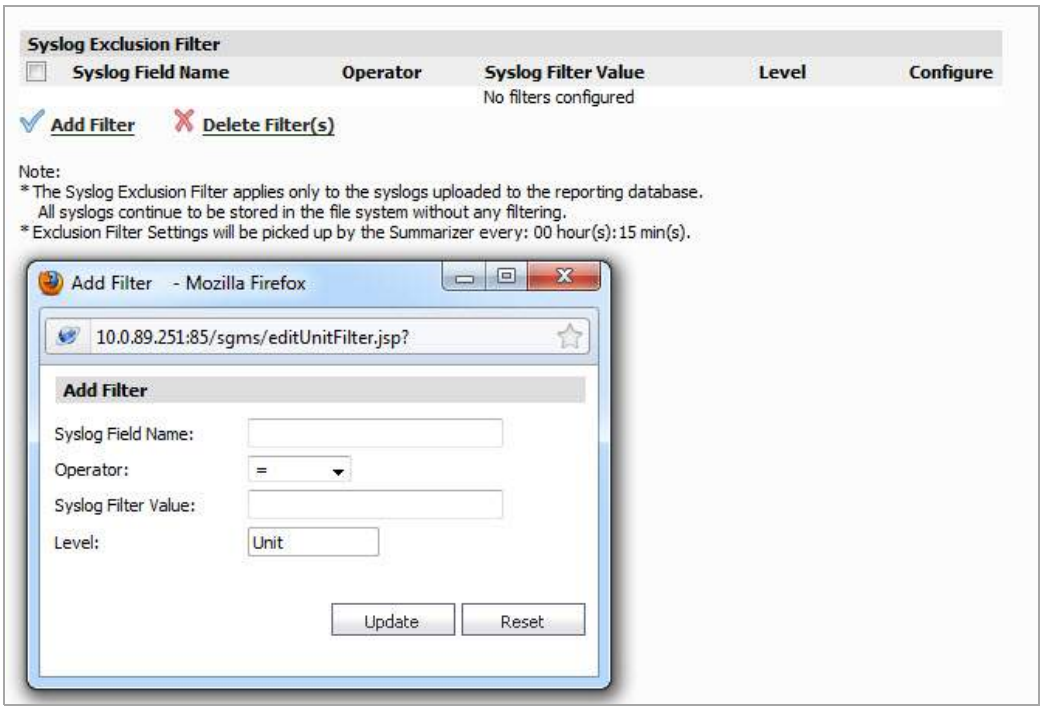
Use this screen to manage the volume of syslog uploaded to the reporting database. The factory default filters are configured to upload only the syslog needed to generate the reports. This can be fine tuned further, but it required advanced knowledge of the syslog and consequently should be performed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

To add a filter, complete the following steps:

1 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.

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



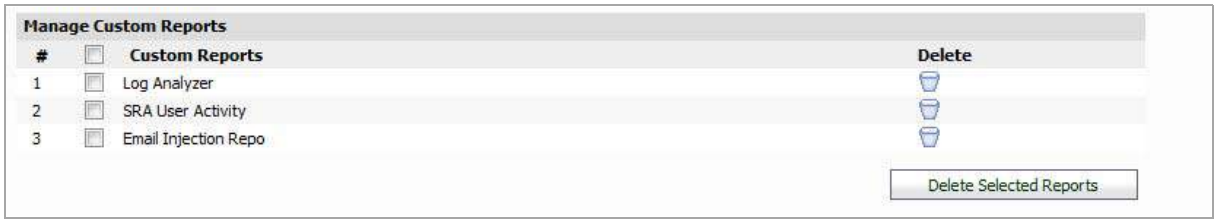
3 Specify the field you want to modify, and select an operator and value. Click **Update**.

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 drop-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 SMA 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 Custom Reports on page 108.

Part 4

Console

- Configuring Log Settings
- Configuring Console Management Settings
- Managing Reports in the Console Panel
- Using Diagnostics
- Granular Event Management
- Configuring User Settings
- Using Analyzer Help

7

Configuring Log Settings

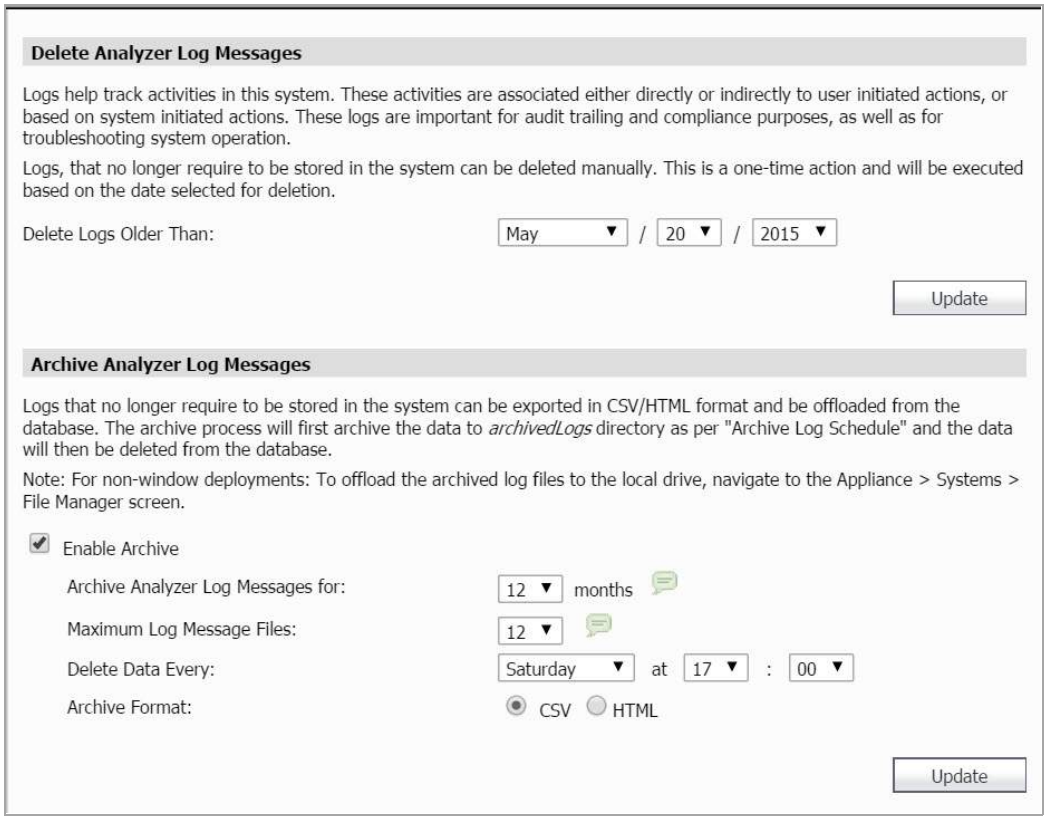
This chapter describes how to configure Log Settings. This includes adjusting settings on deleting log messages after a certain period of time, and setting criteria for viewing logs.

This chapter includes the following sections:

Configuring Log Settings

In the **Console > Log > Configuration** screen, you can delete or archive Analyzer log messages. The Archive process archives the data to the “archivedLogs” directory as per the Archive Log Schedule, before the data is deleted from the database.

NOTE: For UMH deployments, to offload the archived log files to a local drive, login to the /appliance management interface, then navigate to the **System > File Manager** page.



To configure Log settings, select between the following options:

- **Delete Logs Older Than** — Select the month, day, and year, and then click **Update**.

- **Enable Archive** — Select this check box to enable Analyzer log message archiving.
- **Archive Analyzer log messages for** — Select the number of months to archive log messages.
- **Maximum Log Message Files** — Select the maximum number of monthly archive files kept in the achivedLogs folder.
- **Delete Data Every** — Select a reoccurring day and time to delete data.
- **Archive Format** — Select the type of format to archive the Analyzer log messages. Choose between CSV or HTML.
- **Update** — Click **Update** after your settings are selected.

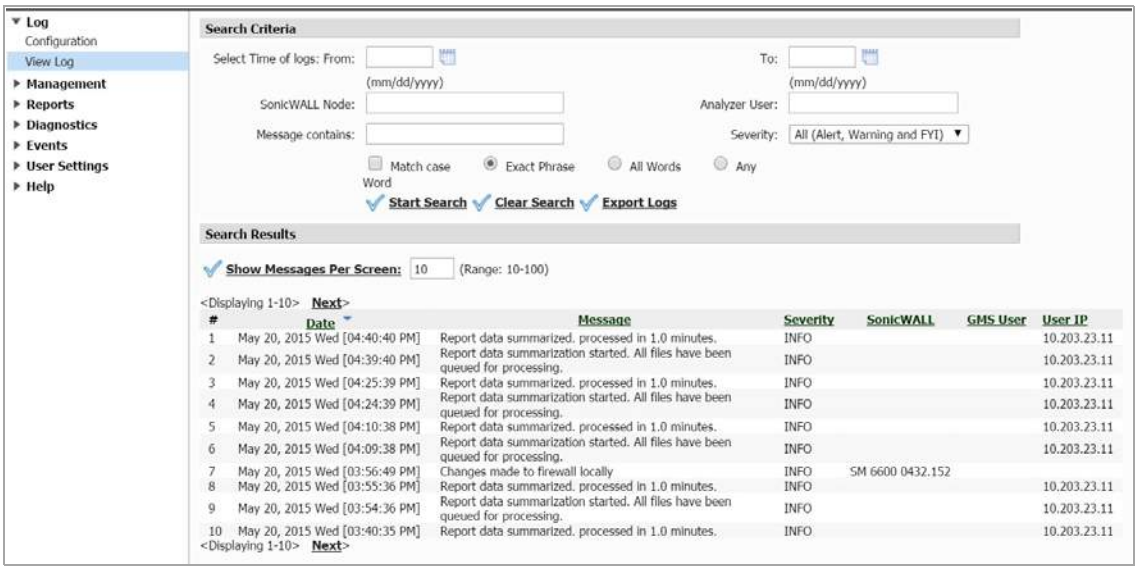
NOTE: The archive process first archives the data to the archivedLogs directory as per “Archive Log Schedule” and then the data is deleted from the database.

Configuring Log View Search Criteria

SonicWall Analyzer log keeps track of changes made within the Analyzer management interface, 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 SonicWall Analyzer log, complete 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 appear as you continue to type if log messages match your input.
- **Severity** — displays log entries with the matching severity level:
  - A**ll (Alert, Warning, and FYI)–where FYI mean "For Your Information"**
  - **Alert and Warning**
  - **Alert**
- Select the **Match case** check box to make the **SonicWall Node**, **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.

6 To jump to a specific message, enter the message number in the **Go to Message Number** field.

8

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 can configure email settings, set the system debug level, synchronize model codes information, and configure password security settings.

This section describes the following Settings topics:

GMS Settings

The GMS Settings allow you to show or hide the SMA tab. This section is only visible to administrators @LocalDomain, such as Super Admins.

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 cannot receive important email notifications, such as:

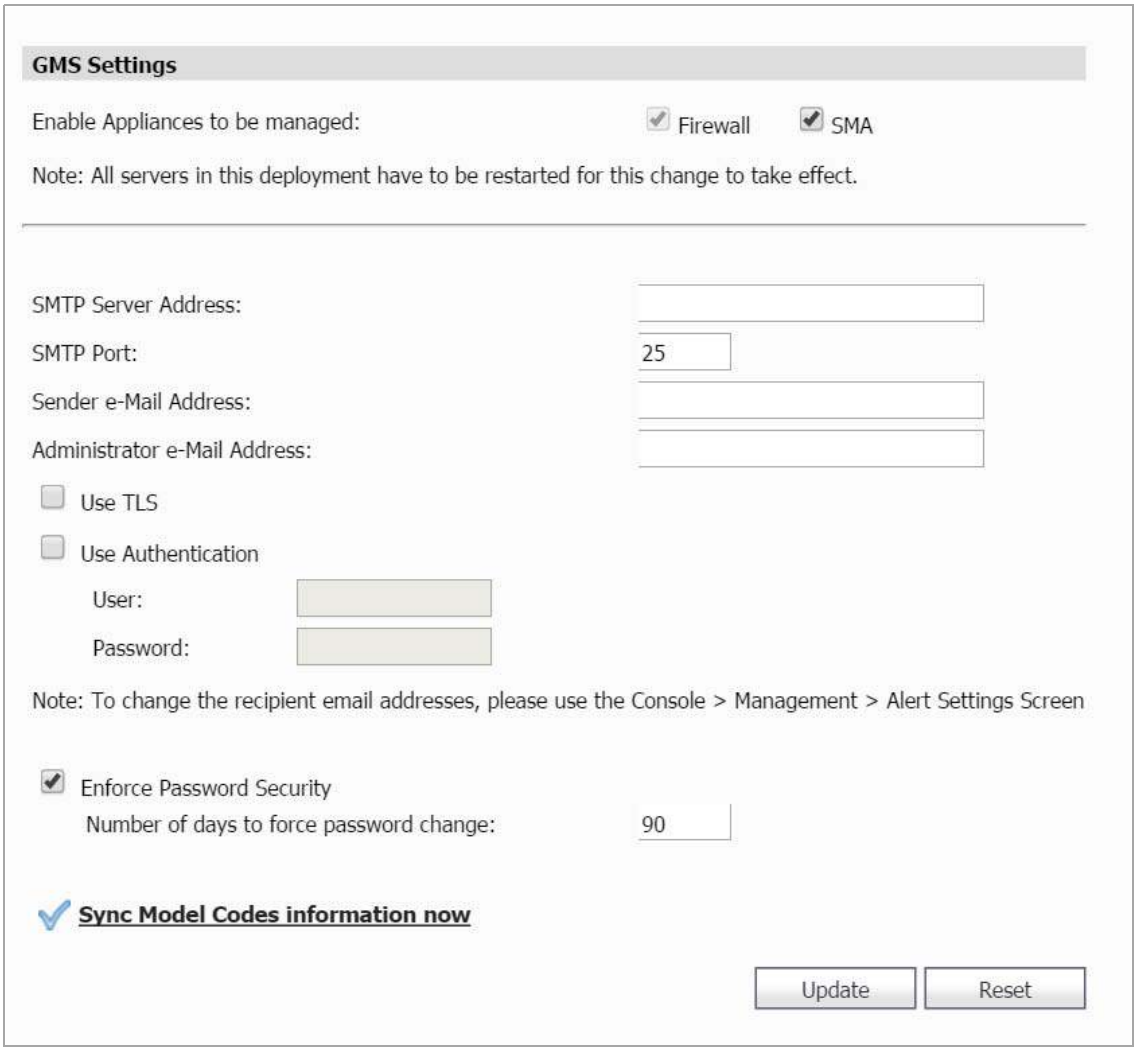
- System alerts for your SonicWall Analyzer deployment performance

- Availability of product updates, hot fixes, or patches
- Scheduled Reports

To configure these email settings, complete the following steps:

1 Click the **Console** tab.

2 Expand the **Management** tree and click **Settings**. The Settings page displays.



3 Enable or disable any SMA appliances to be managed. (Firewall is enabled by default). The deployed servers must be restarted after any changes are made in order for them to take effect.

4 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.

5 Click **Use TLS** if you would like to use Transport Layer Security (TLS) for your mail server connectivity, such as for Gmail or Office365. TLS ensures privacy between you and communicating applications on the Internet, and that no third-party can eavesdrop or tamper with your messages.

6 If the SMTP server in your deployment is set to use authentication, click **Use Authentication**. This option is necessary for all outgoing GMS 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.

7 Enter the email account name and domain that appears in messages sent from the SonicWall Analyzer into the **Sender e-Mail Address** field.

8 Enter the email account name and domain that appears in messages sent from SonicWall Analyzer into the **Administrator e-Mail Address** field. You can use User Authentication for this user by checking the box.

9 When finished in the Settings page, click **Update**. To clear the screen settings and start over, click **Reset**.

Configuring System Debug Level

SonicWall Analyzer provides the **System Debug level** option to control the debug messages sent to the log file.

To configure this setting, complete the following steps:

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

SonicWall Analyzer supports enforced password rotation for enhanced security compliance.

To enable and configure enforced password rotation, complete the following steps:

1 Select the **Enforce Password Security** check box.

2 In the **Number of days to force password change** field, enter a value. The default is 90. SonicWall Analyzer prompts 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 Reports

After the upgrade to Analyzer 8.0, 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 8.0 and pre-8.0 reports in the same session). Reports generated by pre 8.0 releases of SonicWall Analyzer are still available for viewing. Analyzer 8.0 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, complete the following steps:

1 Select **Show Legacy Reports**.

2 Log out of SonicWall Analyzer.

3 Log back in to 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 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, complete the following steps:

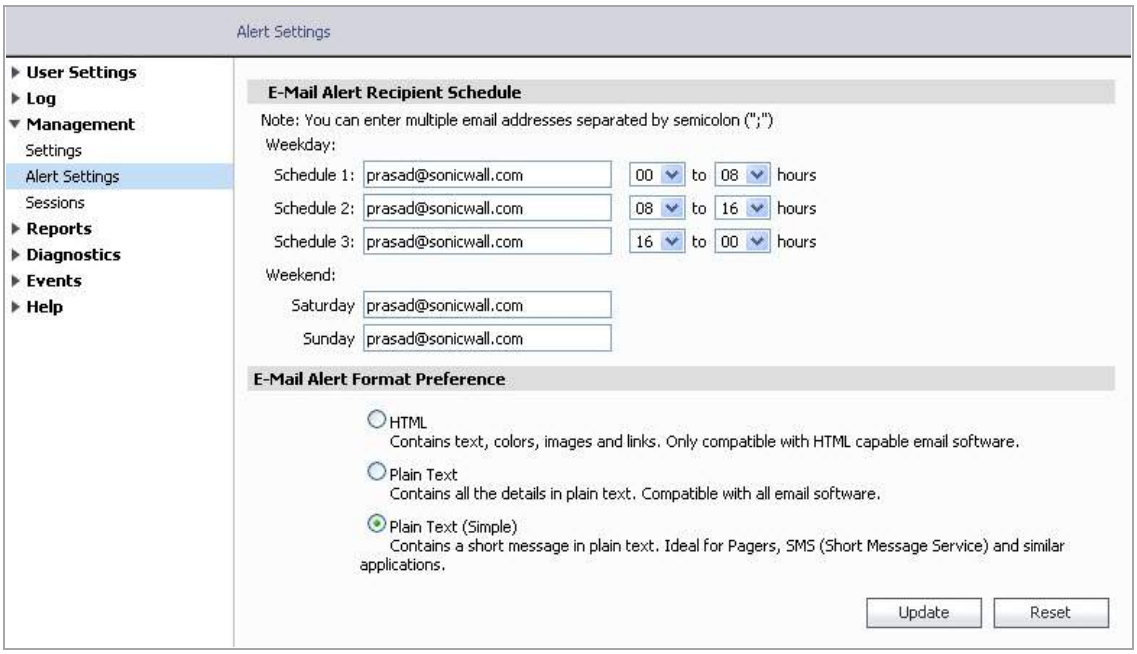
1 On the **Console > Management > Settings** page, click **Sync Model Codes information** now. A short time later the page is updated to display the synchronization status at the top.

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, complete 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 receive notifications and the times that they receive them:

- **Schedule 1** — Specifies who receives 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 receives 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 receives 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 receives 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 receives 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 is to 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

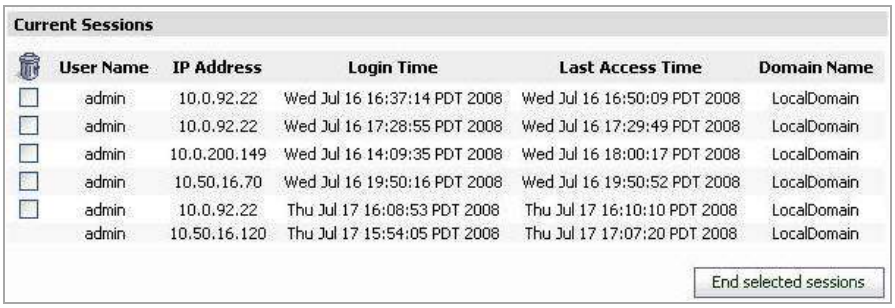
The Sessions page of the Management section of the Console allows you to view session statistics for currently logged in users and to end selected sessions.

Managing Sessions

On occasion, it might be necessary to log off other user sessions.

To do this, complete the following steps:

1 Click the **Console** tab, expand the **Management** tree and click **Sessions**. The Sessions page displays.

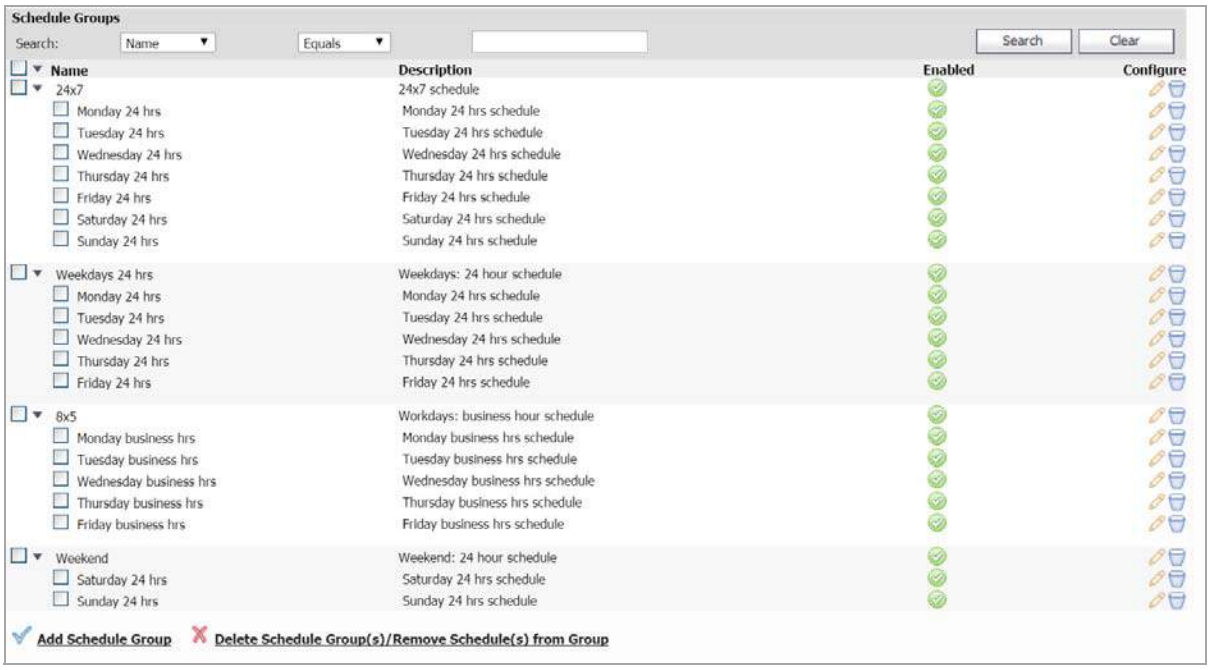


2 When more than one session is active, a check box is displayed next to each row. Select the check box of each user to log off and click **End selected sessions**. The selected users are logged off.

Configuring Management Schedules

The Schedules page of the Management section of the Console allows you to view schedule group statistics for currently logged in users. The Group Schedules table displays all your predefined and custom schedules. In the

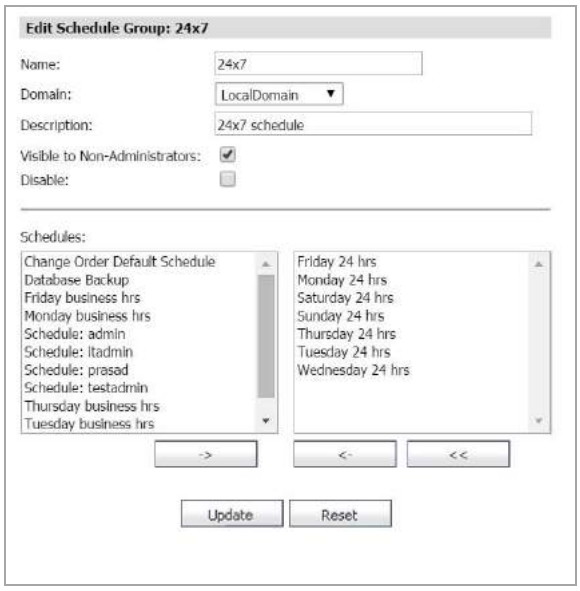
Group Schedules table, there are four default group schedules from which to choose: Daily 24x7, Weekdays 24x7, 8x5 Work Hours, and Weekend Hours.



A group schedule can include multiple day and time increments for rule enforcement with a single schedule. If a schedule includes multiple day and time entries, a right-arrow button appears next to the schedule name.

Clicking the **Expand** icon expands the schedule to display all the day and time entries for the schedule.

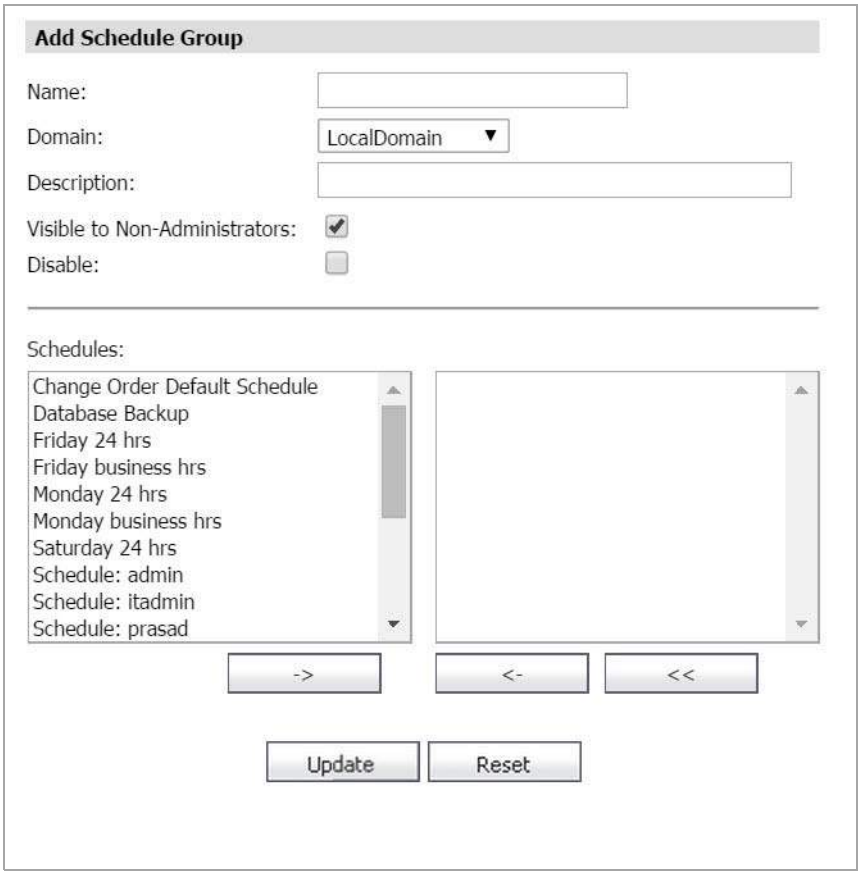
You can modify these group schedules by clicking the **Edit** icons in the Configure column to display the Edit Schedule Group window.



Adding Schedule Groups

To create a schedule group, complete the following steps:

1 On the **Console > Management > Schedules** page, click **Add Schedule Group**. The **Add Schedule Group** page is displayed.



2 Enter a descriptive name for the group schedule in the **Name** field.

3 Enter a group schedule description in the **Description** field.

4 Click **Visible to Non-Administrators** if you would like to make the schedule viewable by the public.

5 By clicking once on the desired Schedule time descriptions, use the arrow keys to move them into the right field. These are the parameter that will be used in your schedule group range.

6 Click **Update** to group the entries into one named schedule.

Deleting Schedule Groups

To delete a schedule group, complete the following steps:

1 Select the check box next to the name of the group you would like to delete.

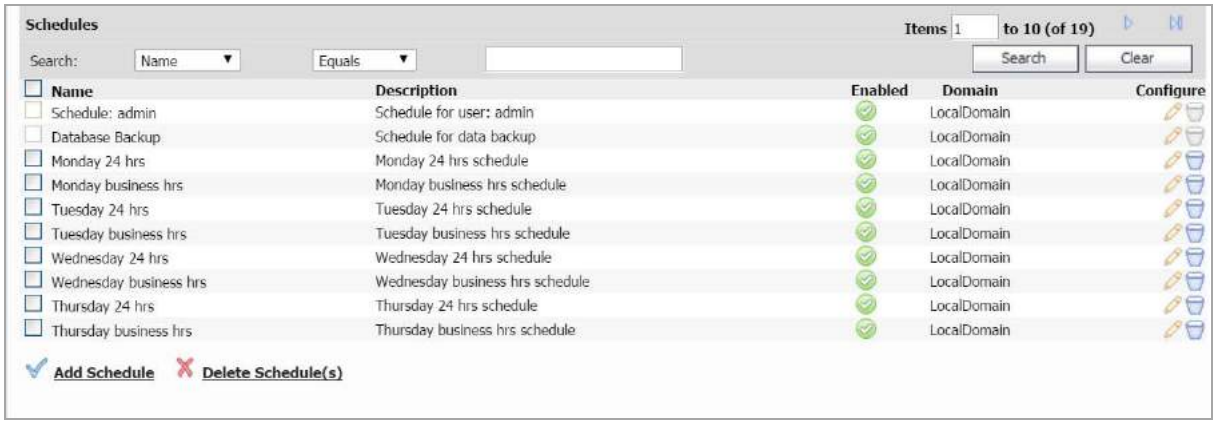
All subordinate check boxes are selected when you click the Schedule Name. Expand the group arrow if you would like to delete individual entries from the group.

2 Click **Delete Schedule Group(s)/Remove Schedule(s) from Group**.

3 Confirm the deletion by clicking **OK** on the window that appears.

Managing Schedules

The Schedules table displays all your predefined and custom schedules. In the Schedules table, there are several default schedules you can use or modify.

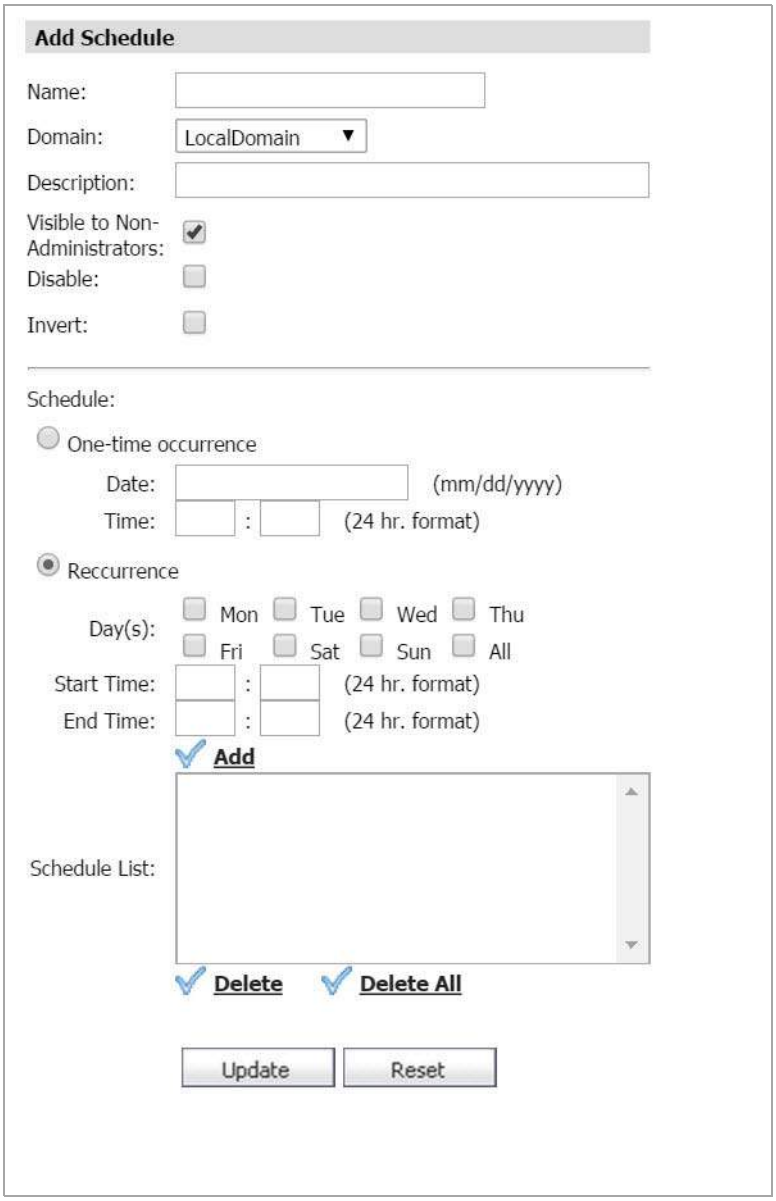


You can modify these schedules by clicking the **Edit** icons in the Configure column to display the **Edit Schedule** window.

Adding Schedules

To create a schedule, complete the following steps:

1 On the **Console > Management > Schedules** page, click **Add Schedule**. The **Add Schedule** page is displayed.



2 Enter a descriptive name for the schedule in the **Name** field.

3 Enter a schedule description in the **Description** field.

4 Click **Visible to Non-Administrators** if you would like to make the schedule viewable by the public.

5 Click **Disable** to take the schedule offline but still available for use later when activated.

6 Click **Invert** to

7 Select one of the following radio buttons for **Schedule**:

- **One-time occurrence** – For a one-time schedule at the configured **Date** and **Time**.

- **Recurrence** – For schedules that occur repeatedly during the same configured hours and days of the week, with no start or end date. When selected, the fields under **Recurring** become active, and the fields under **Once** become inactive.

8 For a One-time Occurrence, configure the starting date and time by entering the **Month**, **Day**, and **Year** (mm/dd/yyyy) and the **Hour**, and **Minute** in the fields. The time is represented in 24-hour format.

9 If the fields under **Recurrence**, select the check boxes for the days of the week to apply to the schedule or select **All**.

10 Under **Recurrence**, type in the time of day for the schedule to begin in the **Start Time** field. The time must be in the 24-hour format, for example, 17:00 for 5 p.m.

11 Under **Recurrence**, type in the time of day for the schedule to stop in the **End Time** field. The time must be in the 24-hour format, for example, 17:00 for 5 p.m.

12 Click **Add**.

13 Click **Update** to add the schedule to the **Schedule List**.

Deleting Schedules

You can delete custom schedules, but you cannot delete the default **Work Hours**, **After Hours**, or **Weekend Hours** schedules.

To delete individual schedule objects that you created, perform the following steps:

1 To delete existing days and times from the **Schedule List**, select the row and click **Delete Schedule(s)**. Or, to delete all existing schedules, click the check box next to **Name** and then click **Delete Schedule(s)**.

9

Managing Reports in the Console Panel

This chapter 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 two GB database for raw syslog data everyday. Be very careful when selecting how much raw information to store.

Configuring the Data Deletion Schedule Settings

Syslog files sent from SonicWall appliances are stored on the system, 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 and SMA appliances.

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

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 is 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 **Update** to the right of this field.

Configuring Data Storage

To set the amount of time that reporting data and raw syslog data is stored, complete the following steps:

1 Click the Summarizer at: drop-down menu, then select the desired summarizer IP address.

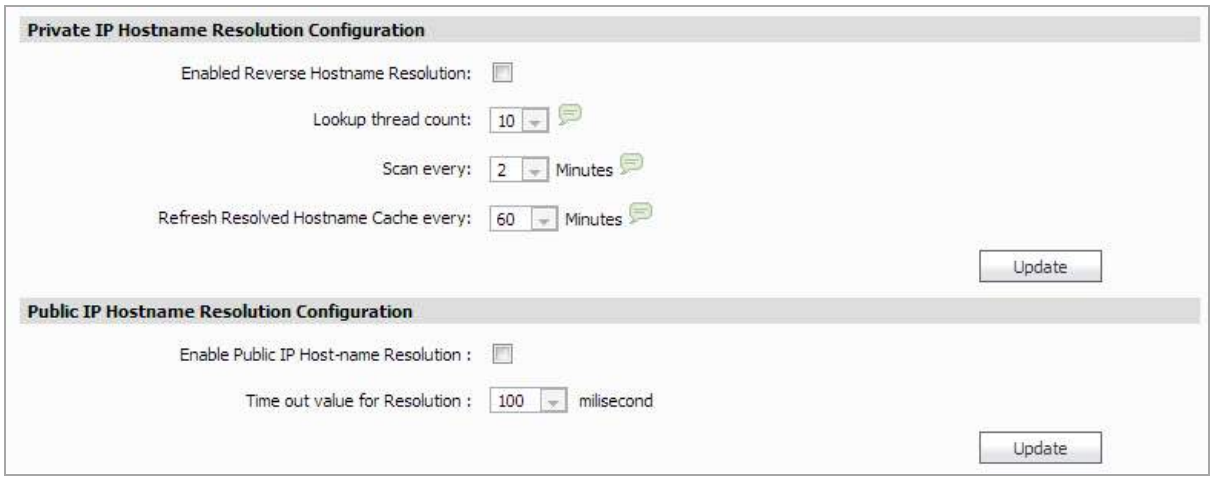
2 Click the **Keep Reporting Data for** drop-down menu, then select the number of months to archive the data. Reporting data can be archived for a minimum of one month and a maximum of 36 months.

3 Click the **Keep Raw Syslog Data Files for** drop-down menu, then select the number of months to archive the data files. To disable the archiving of raw syslog data files, set the value to zero. The maximum amount of time to store raw syslog data files is 36 months.

TIP: If you would like to store data for longer than 36 months, you can create scheduled scripting to move data that has been processed and stored in "//syslog/ArchivedSyslog/*.zip …" to a mapped network shared folder for long-term storage.

Configuring Hostname Resolution

Hostname Resolution in the **Reports > Summarizer** page is configured for source IP addresses with missing hostnames while inserting the data in the database. This means that the reports shows both the initiator IP address and the initiator hostname in the reports whenever applicable.



- **Enabled Reverse Hostname Resolution** — Reverse hostname resolution is disabled by default, enable this option for Analyzer to lookup for missing hostnames.

  NOTE: Enabling hostname lookup increases the time taken to process syslogs. All syslogs that need resolution are processed separately in parallel to normal syslog processing. This might slow down summarizer and increase memory and consume more CPU cycle. Also the memory and CPU are also be impacted further by changing the default configurations of Lookup thread count, Scan every, Refresh Resolved Hostname Cache every. Any changes to the Hostname Resolution Configuration take effect during the next summarizer run.

- **Refresh Resolved Hostname Cache every** — The hostname that is looked up for an IP address is cached. This time indicates how long the hostname is kept in the cache, after that, it again looks up the hostname for that IP address.
- **Scan Every** — Analyzer dumps syslogs with missing hostnames to a particular folder. This time indicates how long it waits to scan the folder for new files.
- **Lookup thread count** — Signifies how many threads are processing the lookup in parallel. The larger the number, the faster the processing.

  NOTE: Increasing this number also increases the load on the summarizer instance.

- **Update** — Click this button when you are finished configuring the settings.
- **Enable Public IP Host-name Resolution** — Public IP hostname resolution is disabled by default, enable this option for Analyzer to lookup for missing public IP hostnames.
- **Time out value for resolution** — Select the timeout period (in milliseconds) if the hostname is not resolved.

Configuring the Packet Data Viewer

In **Console > Reports > Summarizer**, you can enable or disable the Packet Data Viewer for signature alerts by clicking the check box.

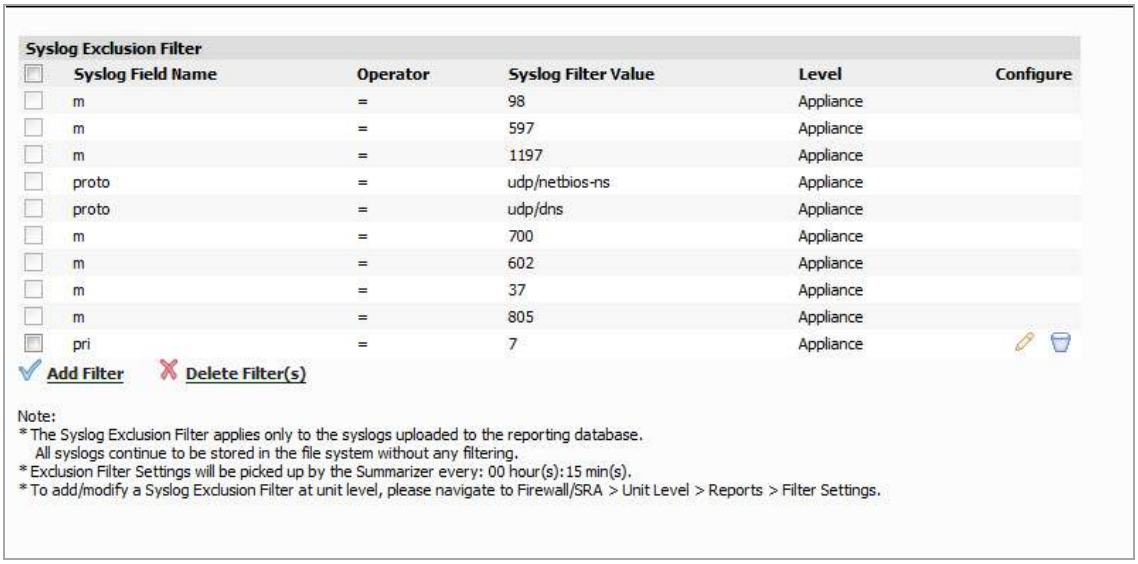
Syslog Exclusion Filter

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.

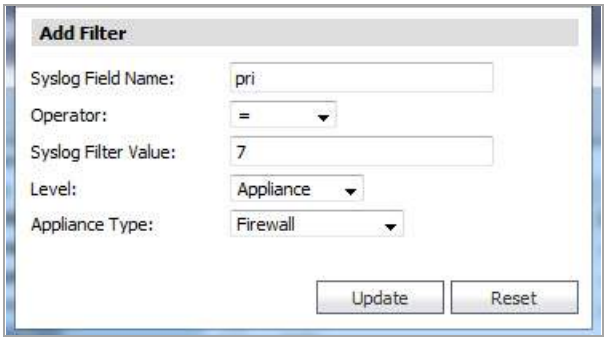
The Syslog Exclusion Filters function in a manner similar to applying an exclusion filter to a single Firewall or SMA appliance, but are applied to all Analyzer appliances, or all appliances in a Firewall or SMA group.

To add a filter, complete the following steps:

1 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 are prompted for the type of appliance: Firewall or SMA. If you select Agent, you are prompted to select from a list of SGMS agents.

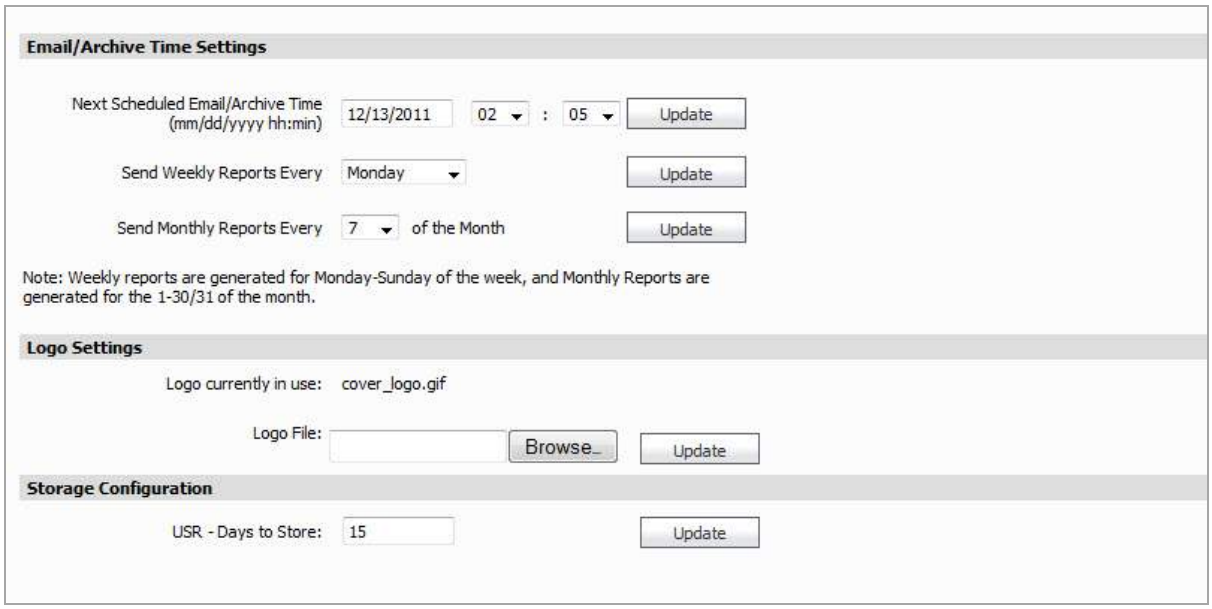
4 Click **Update**.

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, complete 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 are 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 Using the Universal Scheduled Reports Application on page 31.

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-8.0 releases of SonicWall Analyzer are still available for viewing, but require careful management. SonicWall Analyzer 8.0 Reporting is not compatible with earlier versions, but reports generated by earlier versions are still accessible under the current reporting structure.

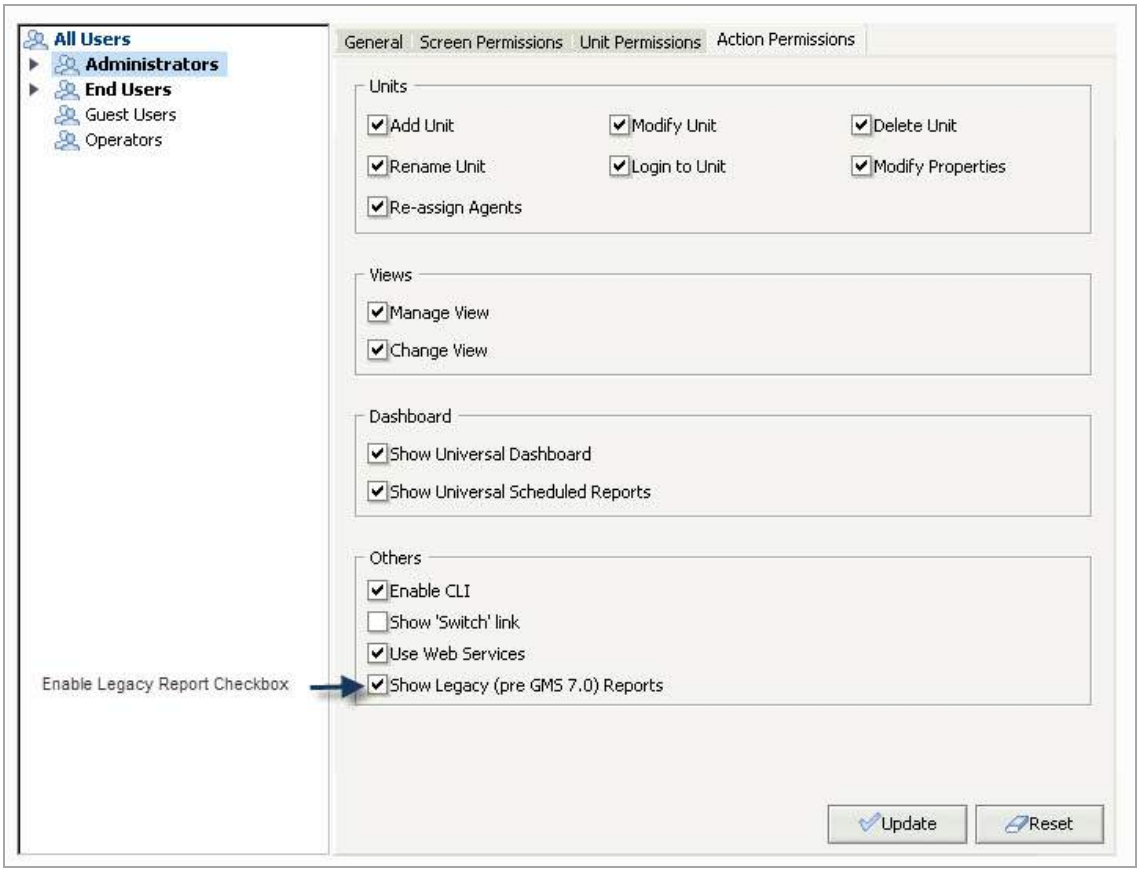
Because it is not possible to view both 8.0 and pre-8.0 reports in the same session, we advise creating a separate Login for accessing Legacy reports. This allows switching back and forth, as you can only view 8.0 or pre-8.0 reports in a session. By creating a separate login, you can switch between viewing modes.

1 Create a new User or Administrator login. An Administrator login (with a name like Admin_Legacy) is recommended, as this login has full privileges. For more information on configuring Legacy reports for new user, refer to the Console Management section.

2 Log in to the **Management > Users > Action Permissions** tab.

3 Set flag in the check box for **Show Legacy Reports**.

NOTE: This check box is only available if SonicWall Analyzer 7.0 Reports exist in the system.

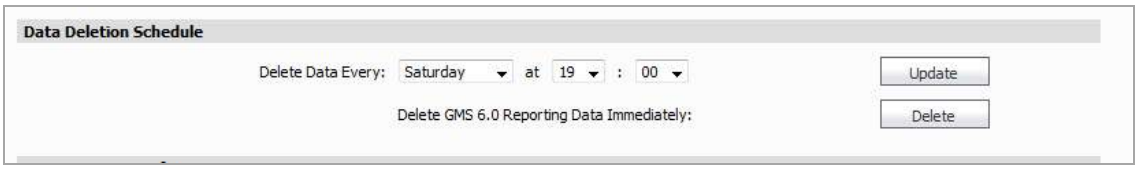


4 Log out, log back in using the new Login created in Step 1.

If Legacy Reports are no longer needed, you can delete them.

5 Go to **Reports > Summarizer**.

6 Under the **Data Deletion Schedule**, you see a box for **Delete 6.0 Reporting Data Immediately**. Click **Delete** to delete the Legacy reports.



NOTE: If you delete pre-8.0 reporting data, the Legacy data check boxes under the Action Permissions and Summarizer tabs are no longer available, going forward.

10

Using Diagnostics

This chapter describes the diagnostic information that SonicWall Analyzer provides and summarizer status information.

This chapter includes the following sections:

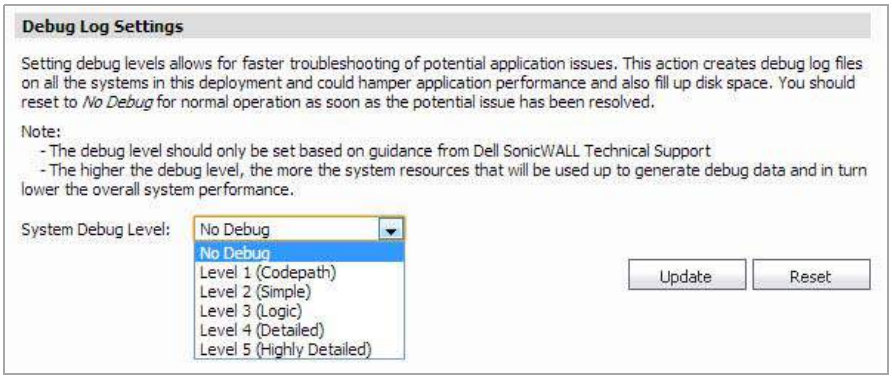
Configuring Debug Log Settings

Setting debug levels allows for faster troubleshooting of potential application issues. This action creates debug log files on all the systems in this deployment and could hamper application performance and also fill up disk space. You should reset to “No Debug” for normal operation as soon as the potential issue has been resolved.

NOTE: The debug level should only be set based on guidance from SonicWall Technical Support.The higher the debug level, the more the system resources that are used up to generate debug data and in turn lower the overall system performance.

To set the debug level when instructed by SonicWall Technical Support, complete the following steps:

1 Click the **Console** tab, expand the **Diagnostics** tree and click **Debug Log Settings**. The Debug Log Settings page displays.



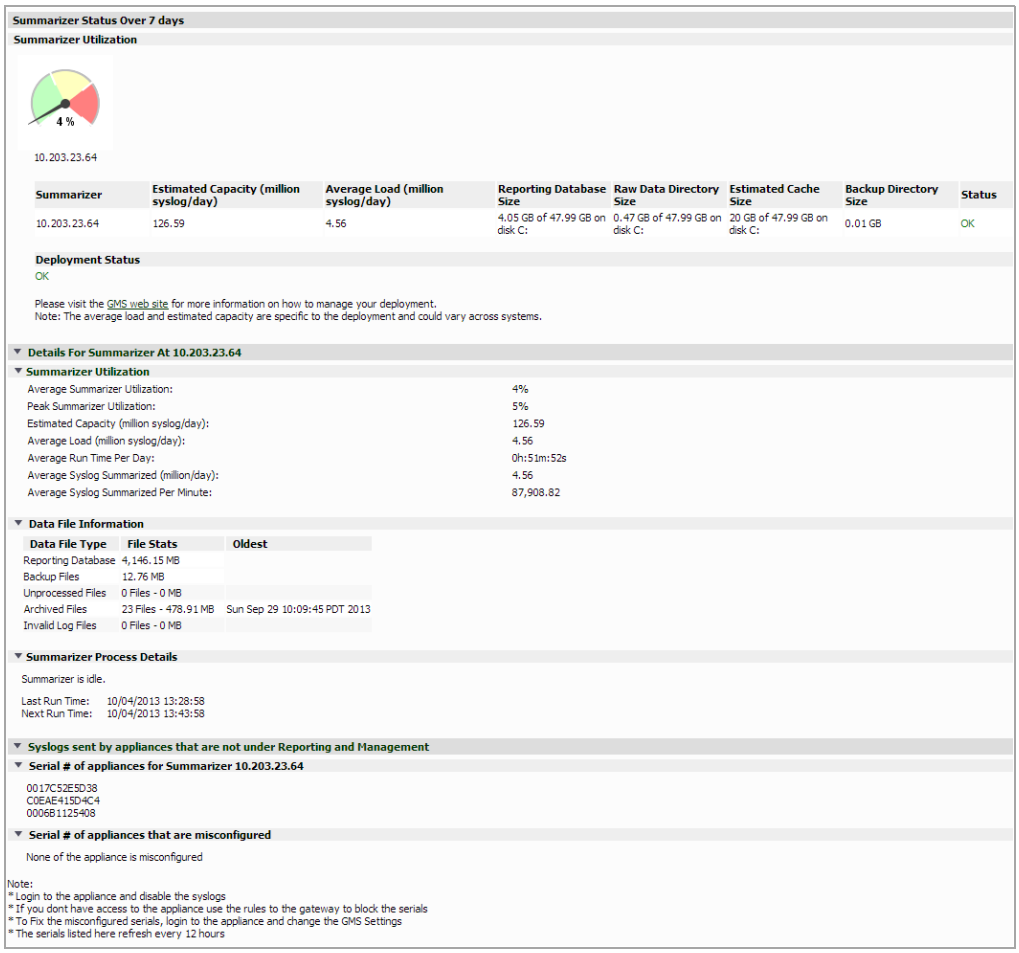
2 Click the **System Debug Level** drop-down, then select one of the following:

- **Level 1 (Codepath)**
- **Level 2 (Simple)**
- **Level 3 (Logic)**
- **Level 4 (Detailed)**
- **Level 5 (Highly Detailed)**

3 Click **Update**.

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 seven days.

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

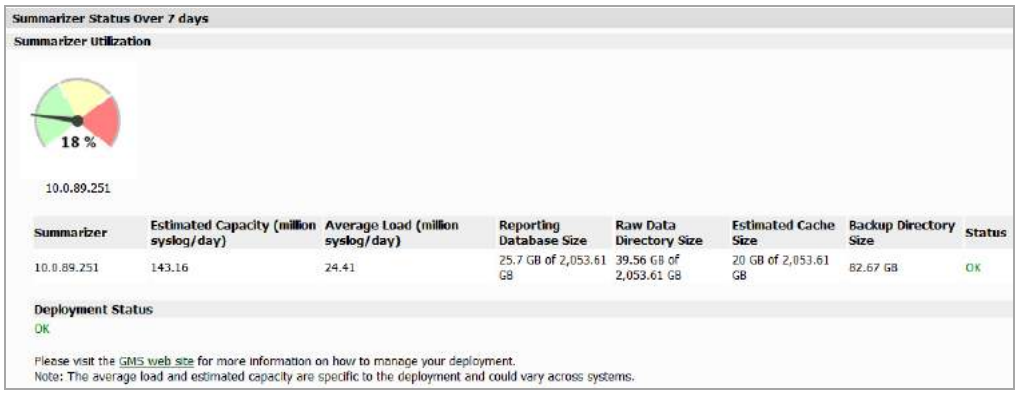
To reach the Summarizer Status screen, navigate to the **Console** panel of Analyzer and then to **Diagnostics > Summarizer Status**.

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 on page 159
- Details for Summarizer at <IP Address> on page 159
- Syslogs sent by appliances that are not under Reporting and Management on page 161

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 percent of capacity.
    - **Low Disk Space**: There is less that 5GB of space left on the disk.

Deployment Status

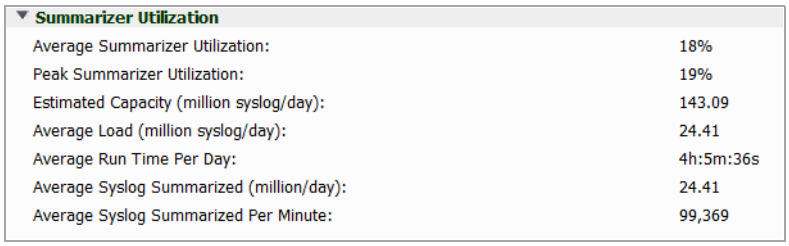
The Deployment Status tells you how the deployment should be sized if it is not performing well. You might need to reassign some units to a different agent, add another agent, or add more disk space.

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.



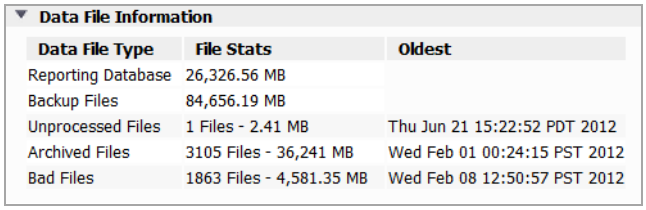
Summarizer Utilization	
Average Summarizer Utilization:	18%
Peak Summarizer Utilization:	19%
Estimated Capacity (million syslog/day):	143.09
Average Load (million syslog/day):	24.41
Average Run Time Per Day:	4h:5m:36s
Average Syslog Summarized (million/day):	24.41
Average Syslog Summarized Per Minute:	99,369

- **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.



Data File Information

Data File Type	File Stats	Oldest
Reporting Database	26,326.56 MB	
Backup Files	84,656.19 MB	
Unprocessed Files	1 Files - 2.41 MB	Thu Jun 21 15:22:52 PDT 2012
Archived Files	3105 Files - 36,241 MB	Wed Feb 01 00:24:15 PST 2012
Bad Files	1863 Files - 4,581.35 MB	Wed Feb 08 12:50:57 PST 2012

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:

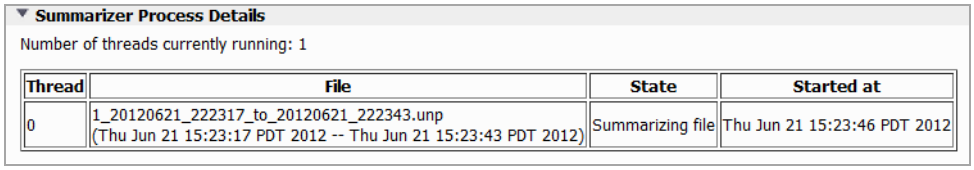
  - **Reporting Database Files**: The files in the reporting database.
  - **Backup Files**: The backup snapshot.
  - **Unprocessed Files**: The data files in the summarizer's processing queue.
  - **Archived Files**: The processed data files.
  - **Bad Files**: Data files with processing errors.
- **File 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.

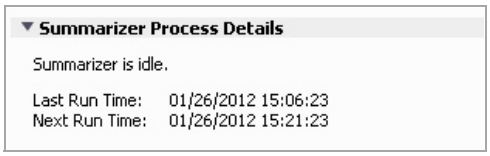
Summarizer Process Details

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.



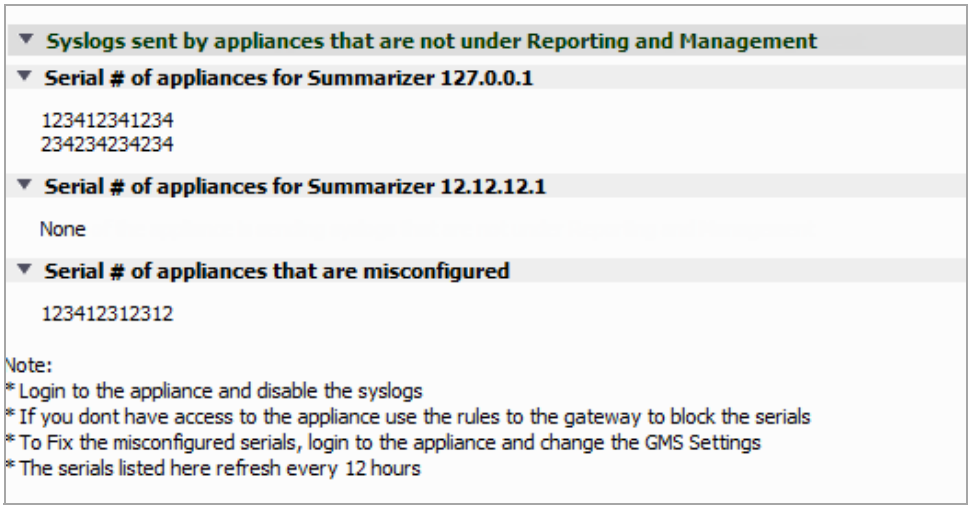
If the summarizer is currently idle, the page displays the last run time and next run time.



Syslogs sent by appliances that are not under Reporting and Management

Appliances that are no longer managed by Analyzer might still send syslog messages, impacting the performance of the summarizer. The syslogs from such appliances are dropped and not stored in archivedSyslogs or badSyslogs folders.

This feature displays a list (refreshed every 12 hours) of the appliances that are still sending syslogs messages even though they are no longer managed Analyzer, as well as appliances that are incorrectly configured:



If your Analyzer has a list of appliances in these fields, try the following to correct the issue:

- Log in to the appliance and disable the syslogs.
- If you do not have access to the appliance, use the rules to the gateway to block the serial numbers.
- To fix the misconfigured appliances, log in to the appliance and change the Analyzer settings.

11

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.

- **Severities: Severity is used to tag an alert as Critical, Warning, Information, or a custom severity level. You can create your own preferred severities and assign the order of importance to them from lowest to highest. When using a custom severity, you must define it before creating a threshold that uses it.**
- **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 panel also provides an **Events > Alert Settings** screen where you can enable or disable alerts.

You can enable or disable an alert at the global or unit level in 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.

Benefits

Granular Event Management offers a significant improvement in control over the way different events are handled. You now have more flexibility when deciding where and when to send alerts, and you can configure event thresholds, severities, schedules, and alerts from a centralized location in the management interface rather than configuring these on a per-unit basis.

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 163.

Using Granular Event Management

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

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	Event > Alert Settings	Database Info

GEM Predefined Default Objects (Continued)

Panel	Screens	Predefined Default Objects
Console	**Events > Schedule**	**Schedule Groups:**
		• Database Size Status
		• System Files Backed-Up Status
		• Disk Space Utilization Status

About Alerts

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

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

- **Firewall panel**: Alert settings for Reporting
- **Console panel**: Alert settings for the Analyzer application

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 section:

- Configuring Events on the Console tab on page 165

Configuring Events on the Console tab

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

See the following sections:

- Configuring Event Thresholds on page 165
- Configuring Event Schedules on page 166
- Enabling or Disabling Alerts on the Console Panel on page 169

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:

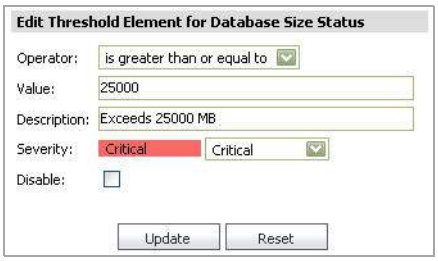
- Editing an Threshold Element on page 165
- Enabling/Disabling Thresholds and Threshold Elements on page 166

Editing an Threshold Element

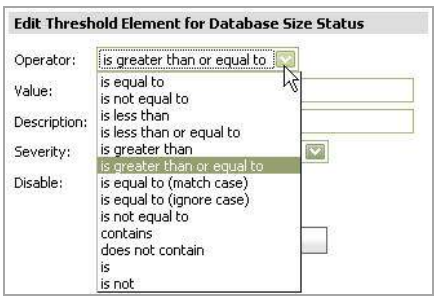
To edit an existing element of a Threshold, complete the following steps:

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:



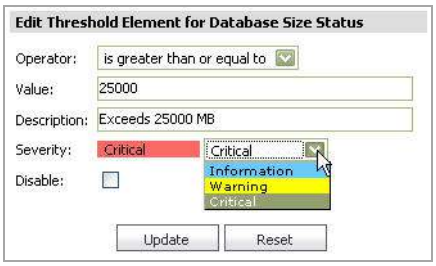
2 In the **Operator** field, select from the drop-down menu the type of operator to apply to your threshold element.



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 on page 166.

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.

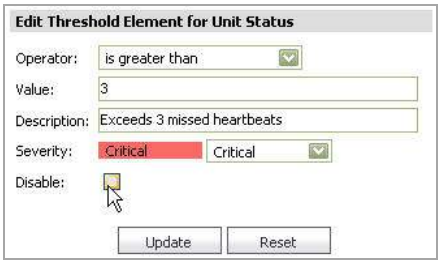
To enable or disable Thresholds and/or their elements, complete the following tasks:

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 **Edit** , which is on the element level.

3 Select **Disable** to disable the element or de-select **Disable** 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 **Visible to Non-Administrators** is selected.

The following tasks are described in this section:

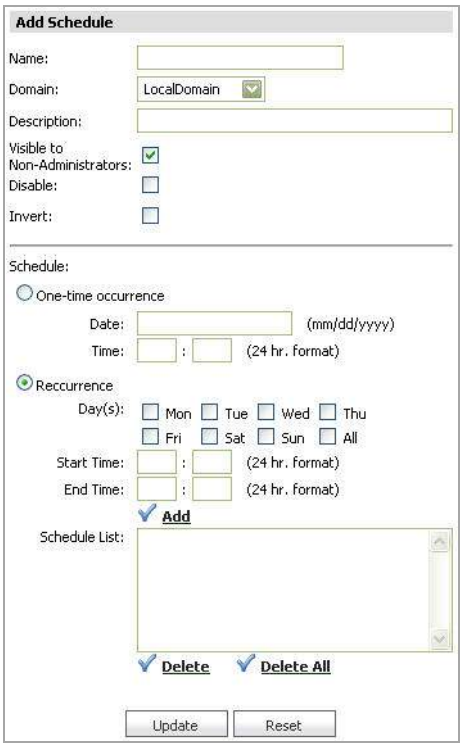
Adding an Event Schedule

In **Events > Schedules** you can add, delete, or configure schedules. You 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 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, complete 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** field, click the drop-down list and select a name. This function is for Super Admins only.
4. In the **Description** field, add a description for the schedule.
5. Select **Visible to Non-Administrators** if you want the schedule to be visible and usable by non-administrators.
6. To temporarily disable a schedule, select **Disable**.
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 Group on page 168.

Adding an Event Schedule Group

You can combine several schedules into a schedule group on the **Events > Schedule** screen.

To add a schedule group, complete the following steps:

1 On the **Events > Schedule** screen, click **Add Schedule Group**.

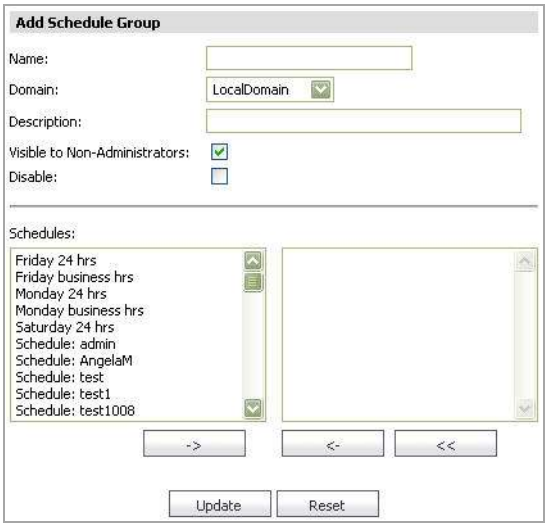
2 Enter the name of your schedule group in the **Name** field.

3 Enter a description of your schedule group in the **Description** field.

4 Click **Visible to Non-Administrators** to allow this schedule group to be viewed and used by non administrators.

5 Click **Disable** 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 on page 168.

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 message displays when this action is performed.

To delete an event schedule, schedule group, or remove a schedule from a schedule group, complete the following steps:

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 are 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 **Delete Schedule Group(s)/Remove Schedules from Group**.

5 To delete the selected schedule(s), click **Delete Schedule(s)**.

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 or click the arrow to display more information about the alert. You can enable or disable these alerts by selecting or clearing the check box in the **Enable** column for the alert, then clicking the Enable/Disable Alert(s) link.

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.

To add an alert, complete the following steps:

1 Navigate to the **Events > Alert Settings** page.

2 Click the **Add Alert** link.

3 Enter a name and description for your alert.

4 Enable **Visible to Non-Administrators** if you want your Alert to be visible to non-administrators.

5 Enable the **Disable** check box 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.

To configure an Alert Type, complete the following steps:

1 Click the **Alert Type** drop-down list and select an alert type.

Most of the Alert Types require you to edit content. Editing Contents allows you to pick additional information, in a granular fashion, on which the alerting has to be performed.

NOTE: When an alert type is selected, a description for that alert is displayed in the Alert Type panel.

2 Click the **Edit Content** link. The Edit contents for alert type: Data usage (Daily) pop-up window displays.

3 Click the **Threshold** drop-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 **Update**. To reset the settings, click **Reset**.

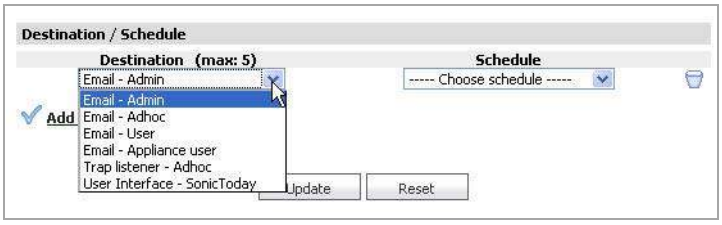
Destination / Schedule

In the Destination / Schedule panel you can add up to five destinations and set a schedule for each.

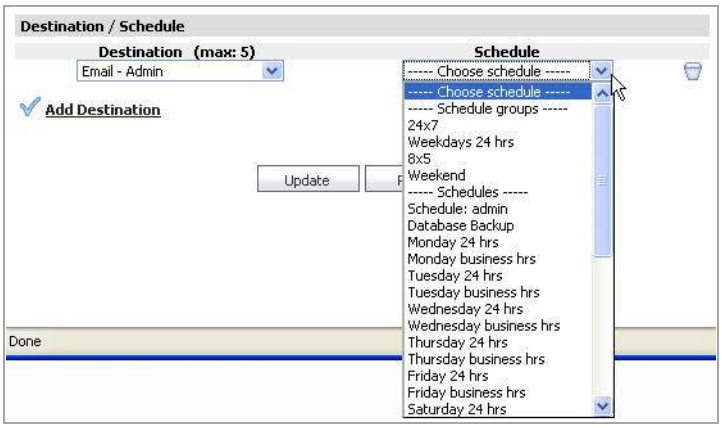
To add a destination and set a schedule, complete the following steps:

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** drop-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

To enable or disable an alert, complete the following steps:

Enabling a Alert

1 Select **Enabled** of the alert(s) you wish to enable.

2 Click **Enable/Disable Alert(s)** link. A confirmation window displays. Click **OK** to enable/disable.

Disabling an Alert

1 Deselect **Enabled** of the alert(s) you wish to disable.

2 Click the **Enable/Disable Alert(s)** link. A confirmation window displays. Click **OK** to enable/disable.

Deleting Alerts

To delete an alert, complete the following steps:

1 Select the check box(s) of the Alert(s) you wish to delete.

2 Click the **Delete Alert** link. A confirmation window displays.

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.

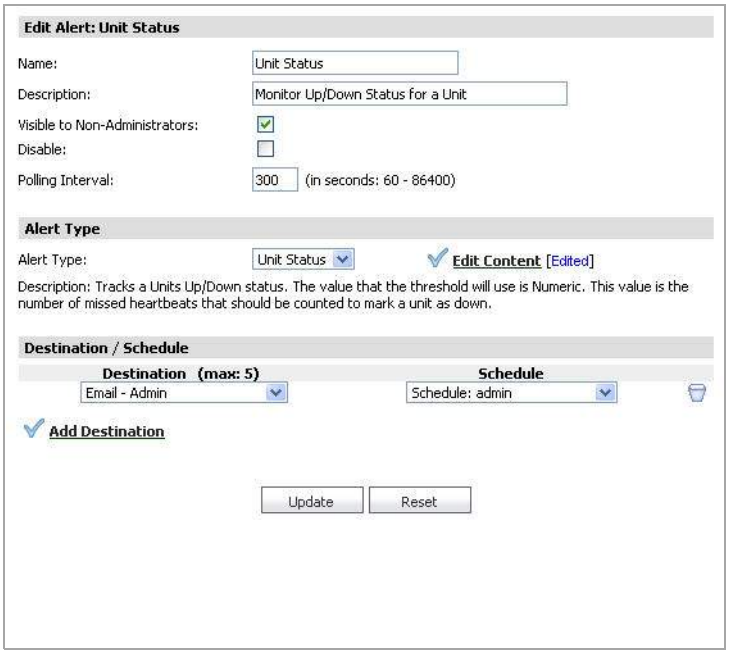
Editing Alerts

After an alert is created, you can go back and edit it at any time.

To edit an alert, complete the following steps:

1 Click the **Configure** icon of the alert you wish to edit.

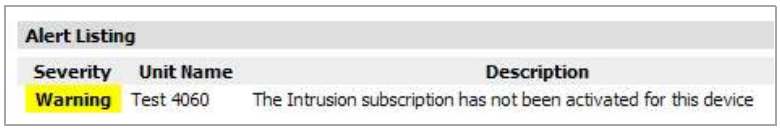
The **Edit Alert** page displays.



2 Refer to the section Add Alert on page 170 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 the panel. Select a global view or unit to view current alerts for your selection.



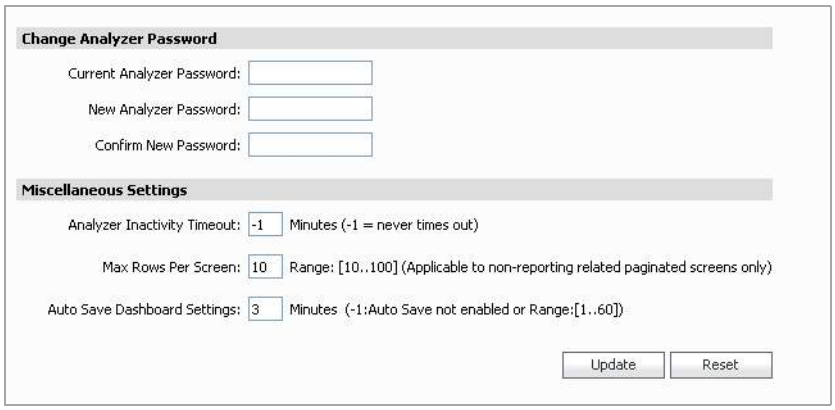
Alert Listing

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

12

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 that provides a way to change the Analyzer administrator password, the Analyzer inactivity Timeout, and pagination settings.



To configure the user settings that are available in the Console panel on the User Settings > General page, complete the following steps:

1 Enter the existing SonicWall Analyzer password in the **Current Password** field.

2 Enter the new SonicWall Analyzer password in the **New Password** field.

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

> **NOTE:** Password fields are grayed out for users on a Remote Domain.

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

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.

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 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.

13

Using Analyzer Help

To access the Analyzer online help, click **Help** in the top-right corner of the Analyzer user interface.

SonicWall Analyzer online help provides context-sensitive conceptual overviews, configuration examples, and trouble shooting tips.

This contains the following sections:

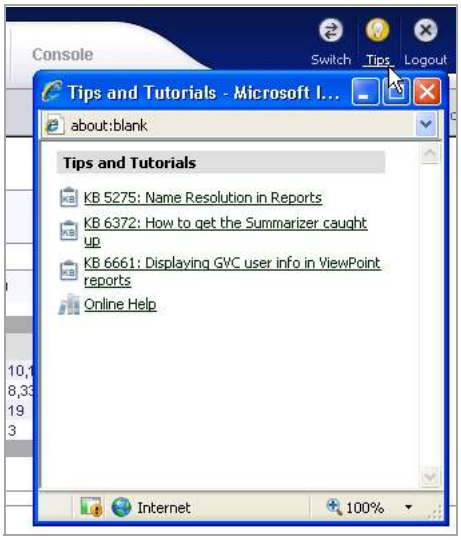
About Analyzer

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 Analyzer.

To access the Analyzer online help, click **Help** 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 corner of the window. Tips, tutorials, and online help are displayed for this topic.

Part 5

UMH

- Using the UMH System Interface

14

Using the UMH System Interface

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

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

- **System > Status**
- **System > Licenses**
- **System > Administration**
- **System > Settings**
- **System > Diagnostics**
- **System > Backup/Restore**

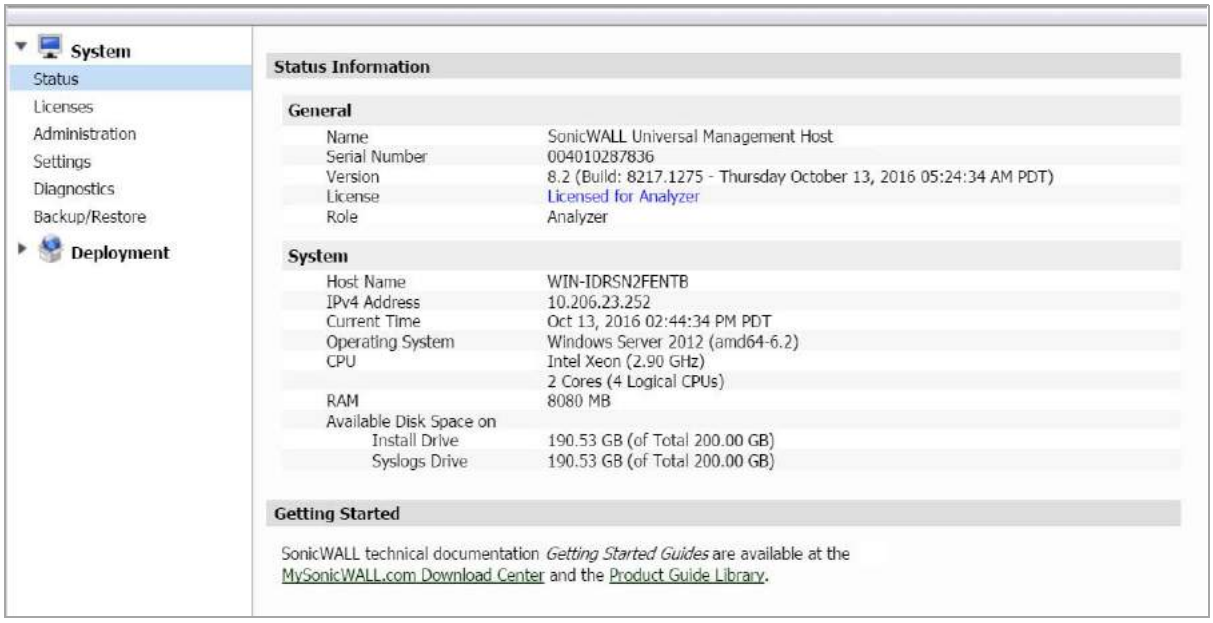
NOTE: Microsoft Windows deployments can skip these settings as they only apply to Virtual Appliance deployments.

This section includes the following subsections:

Overview of the UMH System Interface

The SonicWall Analyzer UMH system interface is used for system management of the 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 SonicWall Analyzer application interface, click **Switch** 

in the top right corner of the interface.

Viewing Online Help and Tips

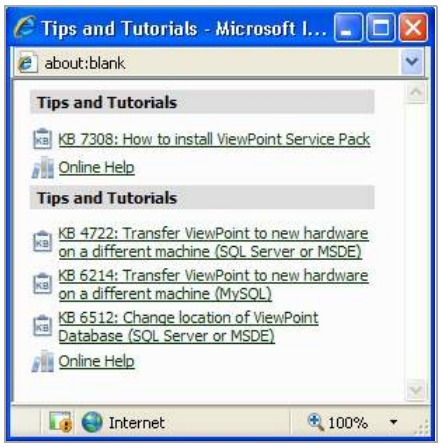
To display context sensitive help for the current page, click **Help** 

in the top right corner of the interface.

Help can change to the **Tips** button 

if the current page has any context sensitive tips or video tutorials.

Clicking **Tips** displays dynamic links for white papers, videos, knowledge base articles, other references, and Online Help.



Logging Out of the UMH System Interface

To log out of the SonicWall Analyzer UMH system interface, click **Logout** 

in the top right corner of the interface.

Configuring UMH System Settings

This section describes the tasks you can do on the System pages of the SonicWall Analyzer UMH system interface. The SonicWall Analyzer UMH system interface contains similar configuration settings for Microsoft Windows and Virtual Appliance deployments. The 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**

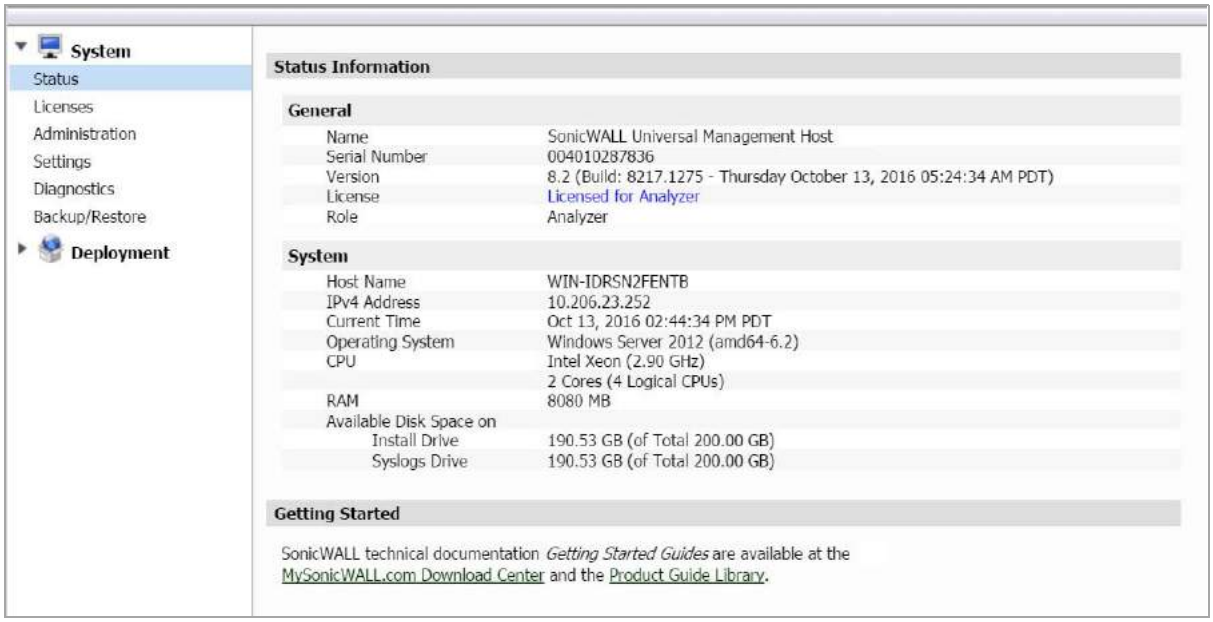
See the following sections:

- Switching to the Application Interface on page 178
- Viewing Online Help and Tips on page 178
- Logging Out of the UMH System Interface on page 179
- Viewing System Status on page 180
- Managing System Licenses on page 180
- Upgrading from Analyzer to GMS on page 181
- Configuring System Time Settings (Virtual Appliance) on page 191
- Configuring System Administration Settings on page 191
- Managing System Settings on page 192
- Using System Diagnostics on page 193

- Using System File Manager (Virtual Appliance) on page 195
- Using System Backup/Restore on page 196
- Using System Shutdown (Virtual Appliance) on page 198

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 SonicWall Analyzer instance, the software version, licensing status, and the system role. For 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.

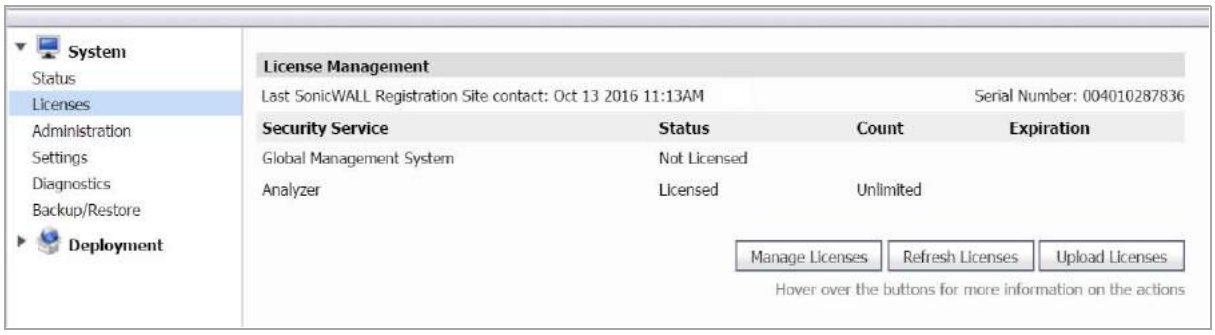
At the bottom of the page, a link is provided to access the *Getting Started Guide* that takes you to the Online Help table of contents.

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 shows the status of your SonicWall GMS Free Trial, if activated. If you choose to upgrade to SonicWall GMS, this page shows 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 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.

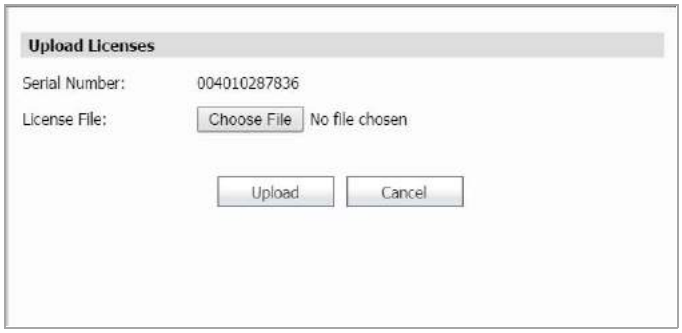
The Expiration column indicates the expiration date of the license. If no date is shown, the license is perpetual, and does not expire.



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

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

To upload a new license, click **Upload Licenses** 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, **Try GMS Free - 30 Days** 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 on page 182
- Enabling the GMS Free Trial from the UMH Interface on page 184
- Completing the Free Trial Upgrade on page 185
- Configuring Appliances for Analyzer Management on page 187
- Purchasing a SonicWall GMS Upgrade on page 189

Enabling the GMS Free Trial from Analyzer

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

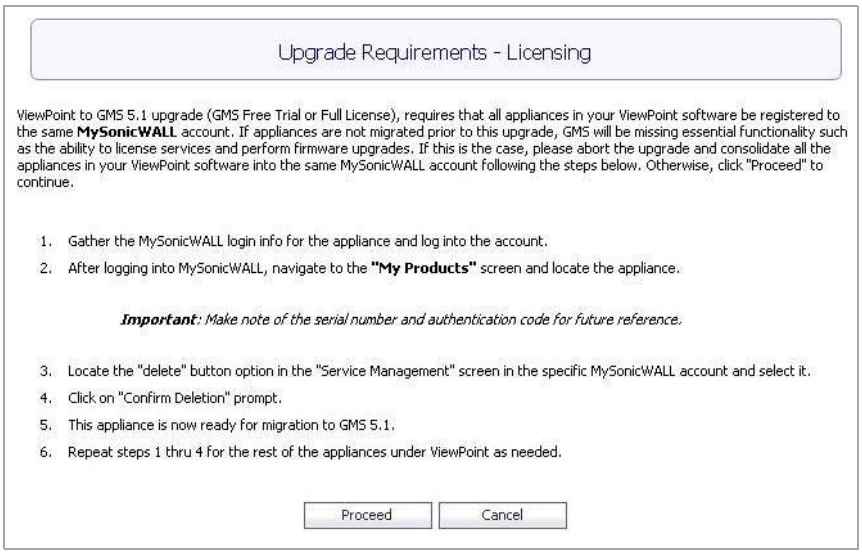
To find out how many devices your SonicWall Analyzer installation is handling, log in to MySonicWall and navigate to the **My Products** page. Click on the link for your SonicWall Analyzer installation to get to the **Service Management** page, and scroll to the bottom. You see the list of appliances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

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

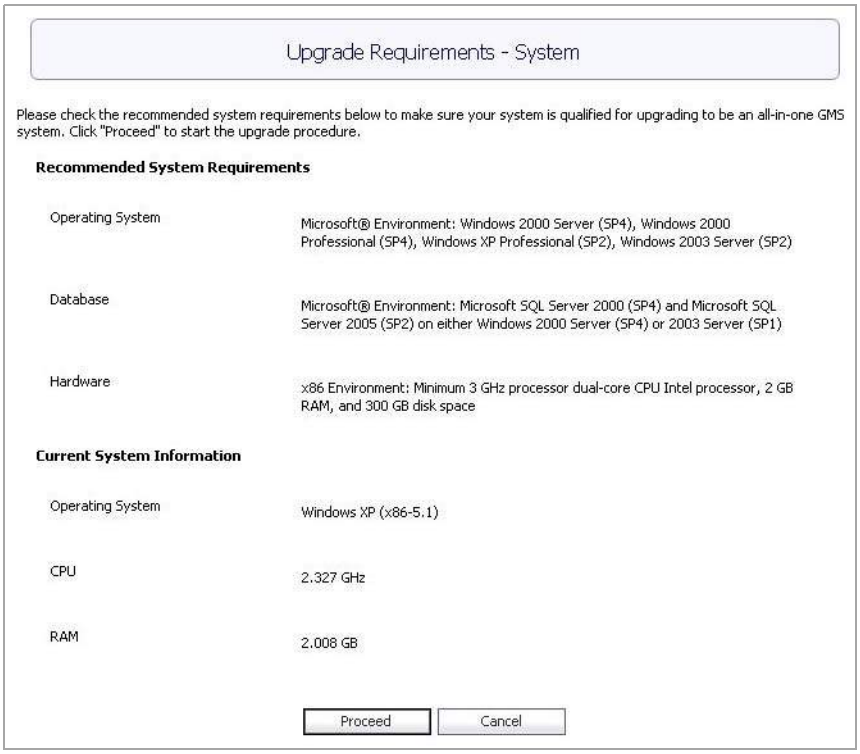
1 In the SonicWall Analyzer management interface, click **Try GMS Free - 30 Days** next to the tabs at the top of the page.

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,

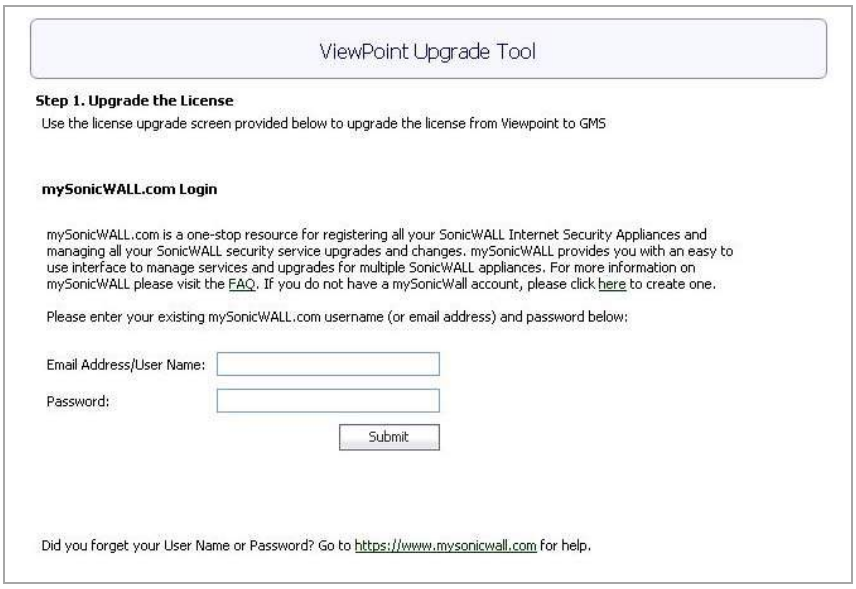
ensure that all appliances under Analyzer reporting are registered to the same MySonicWall account. Follow the steps provided in the screen, and then click **Proceed**.



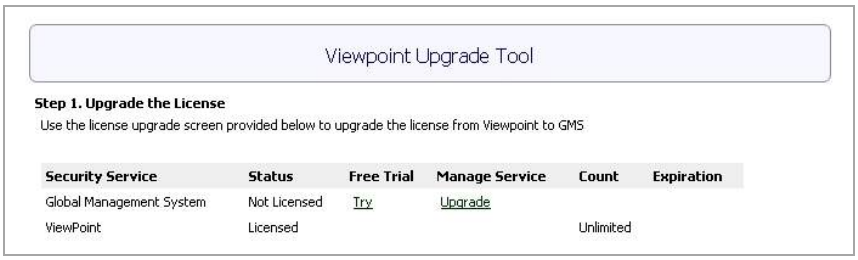
3 The **Upgrade Requirements – System** screen displays the recommended operating system, database, and hardware system requirements. Click **Proceed**.



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.



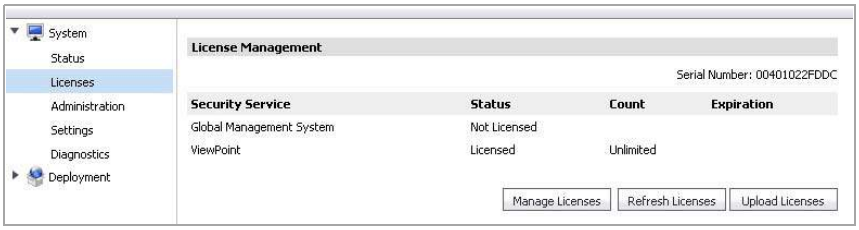
6 From this point, the upgrade process continues with the same steps for access from either the SonicWall Analyzer interface or the Universal Management Host interface.

Continue the procedure by completing the following section.

Enabling the GMS Free Trial from the UMH Interface

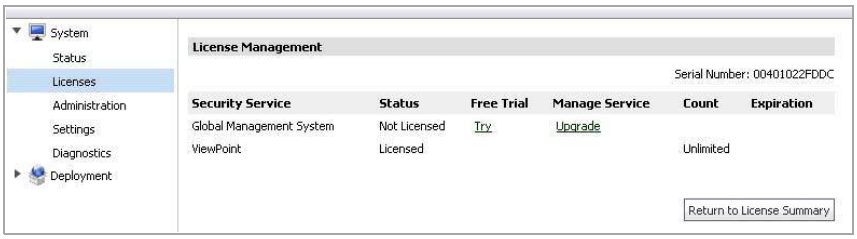
To enable the 30-day Free Trial of SonicWall GMS from the Universal Management Host interface on your SonicWall Analyzer system, complete the following steps:

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.

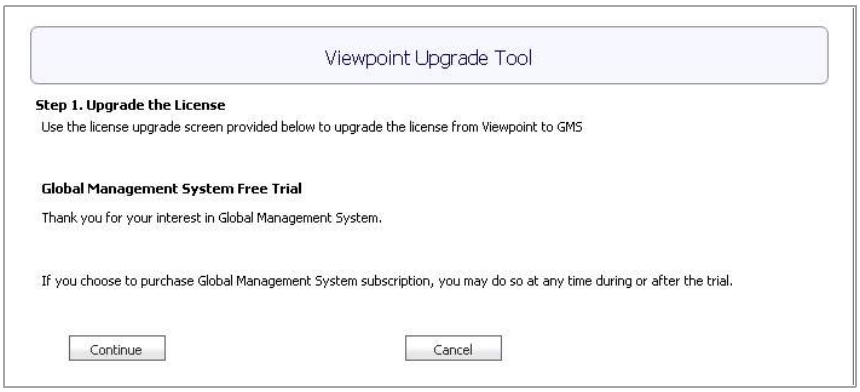
Completing the Free Trial Upgrade

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:

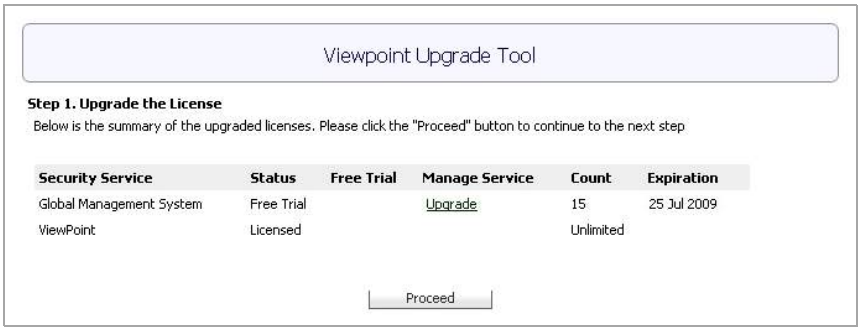
- Enabling the GMS Free Trial from Analyzer on page 182
- Enabling the GMS Free Trial from the UMH Interface on page 184

To continue the upgrade, complete the following steps:

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



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 **Upgrade** 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 in step 2 of the upgrade process. This page displays two sections:

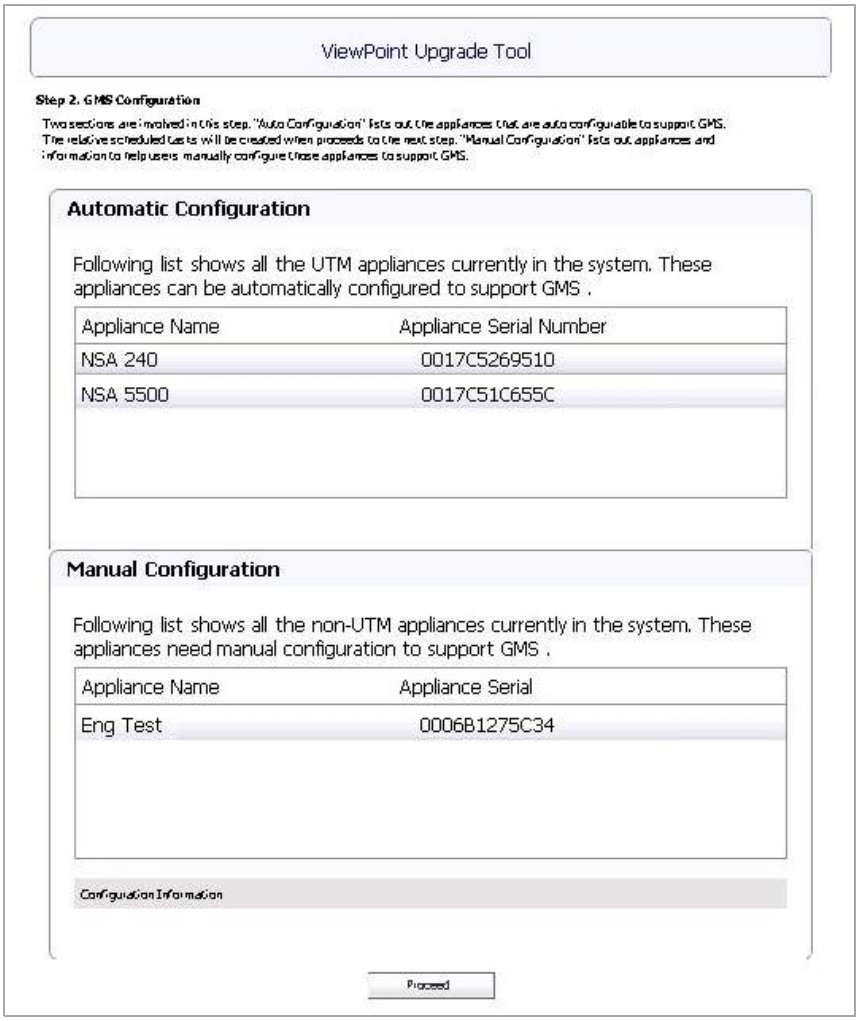
Automatic Configuration

Contains a list of SonicWall firewall or CSM appliances in your Analyzer installation. These appliances are automatically configured for SonicWall GMS management.

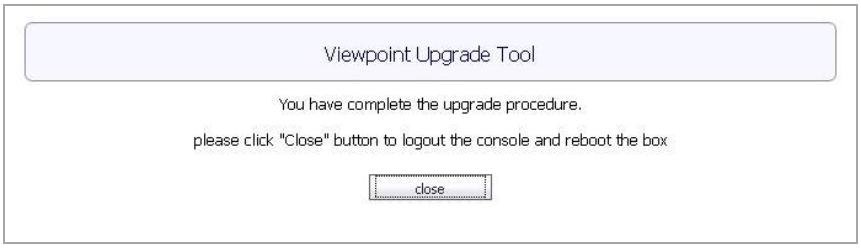
Manual Configuration

Contains a list of SonicWall or SSL-VPN appliances in your Analyzer installation. You must manually configure these appliances for SonicWall GMS management. See Configuring Appliances for Analyzer Management on page 187 for detailed instructions on enabling SonicWall GMS management on these appliances.

4 When ready, click **Proceed**.



5 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.

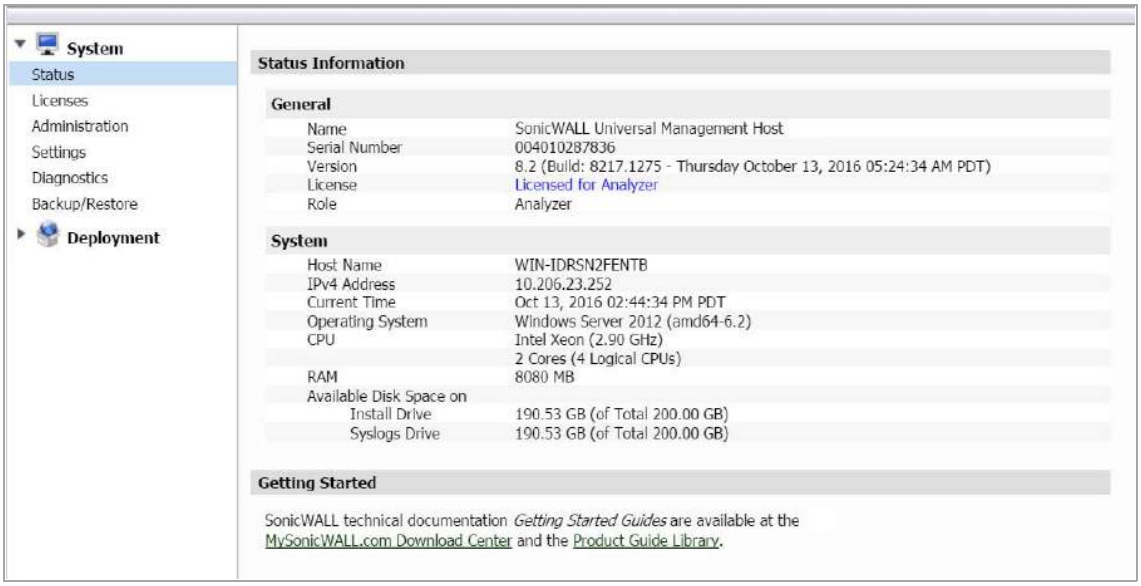


6 The Analyzer login page appears and requests that you reboot the system. Reboot the system. If a reboot is not done, you could encounter problems with the correct IP Address appearing.

7 After rebooting, log in with your Analyzer credentials.

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

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



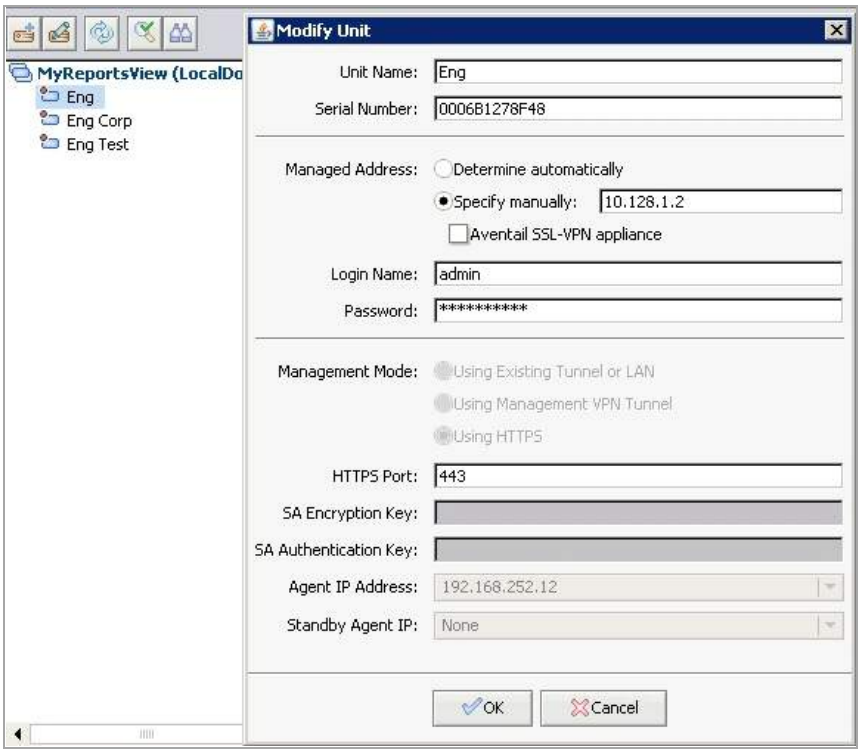
Configuring Appliances for Analyzer Management

To manually configure the appliances listed in the Manual Configuration section of the Analyzer Upgrade Tool page, complete the following steps for each appliance:

1 In the SonicWall Analyzer management interface, click the tab at the top of the page that corresponds to the type of appliance, such as **SSL-VPN**.

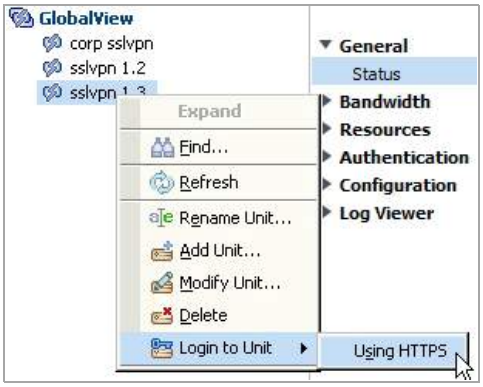
2 In the left pane, right-click one of the listed appliances and select **Modify Unit**.

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.

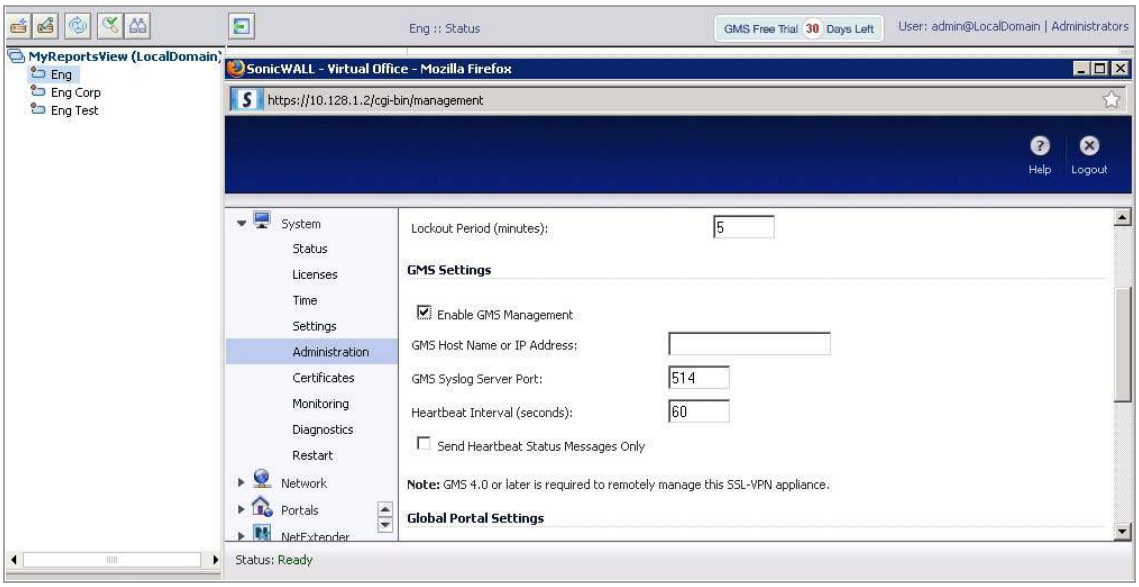


4 Click **Cancel**.

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 **Enable GMS Management**, 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 **Accept** at the top of the appliance interface screen.

10 Click **Logout** 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

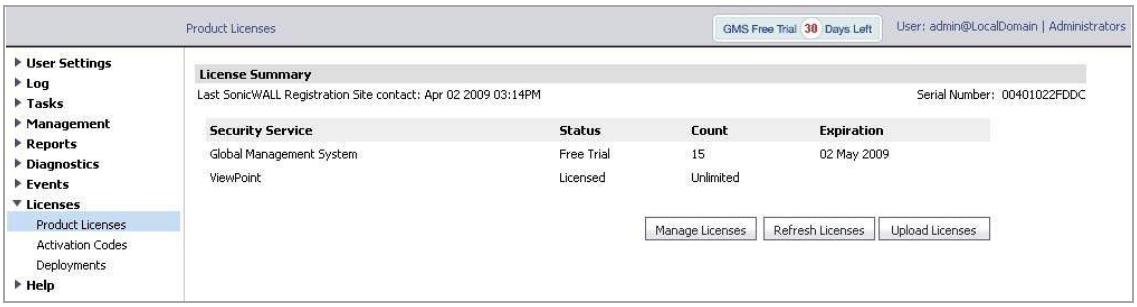
You can purchase an upgrade to SonicWall GMS at any time during the 30-day Free Trial.

To purchase the SonicWall GMS license, complete the following steps:

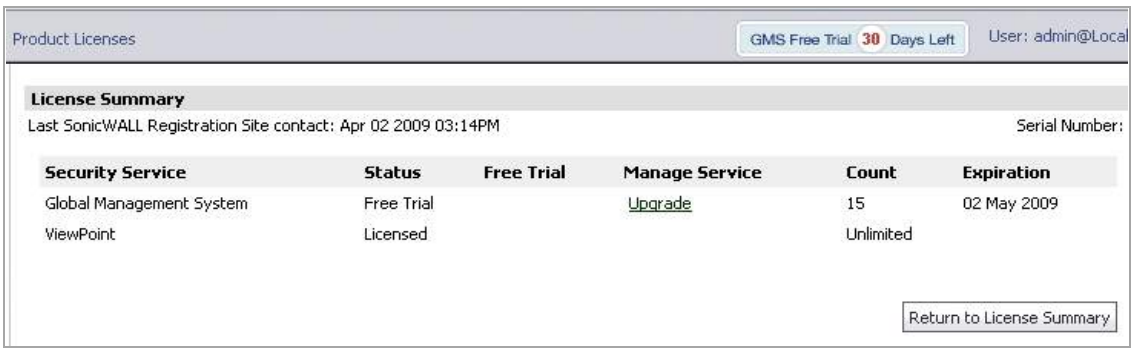
1 In the SonicWall GMS interface, click **GMS Free Trial X Days Left**, where **X** is the number of days left in the Free Trial.

2 On 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 **Upgrade**.



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.

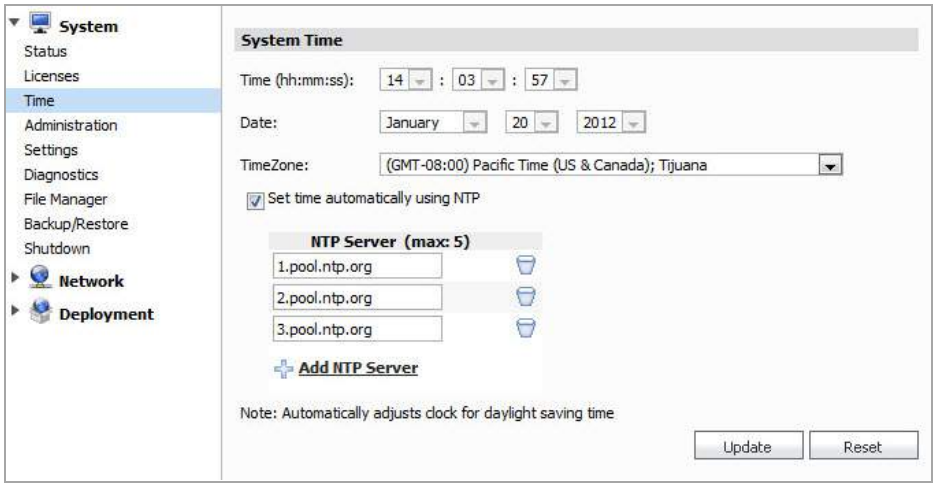
6 Enter a descriptive name for the SonicWall GMS installation into the Friendly Name field. This name appears in your MySonicWall account.

7 If your SonicWall Analyzer installation currently handles more than 10 appliances, when you upgrade to SonicWall GMS, you 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.

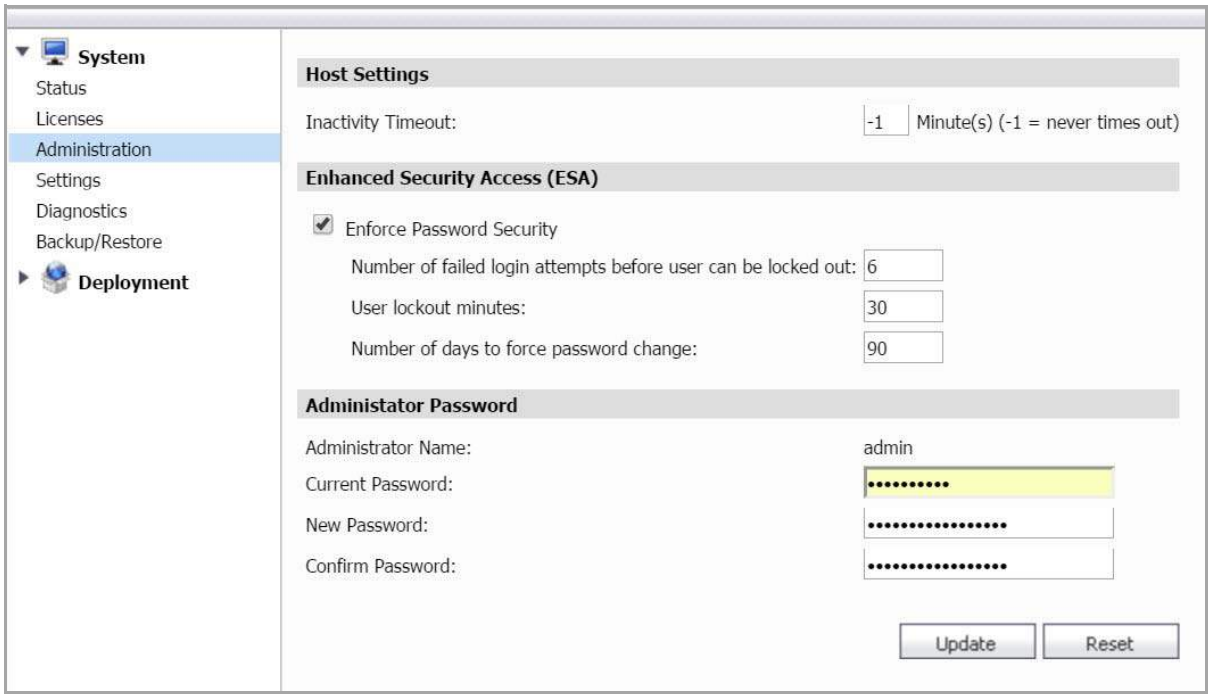


To manually select the time, under **Systems Time** select the Time, Date, and Time zone.

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

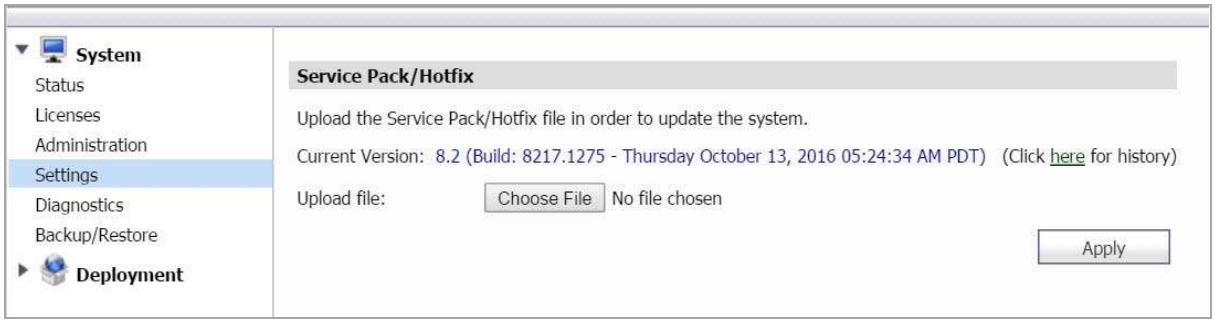
Under **Enhanced Security Access**, you can configure the number of failed login attempts before the admin account is locked out, and the number of minutes that the lockout lasts. You can also configure the number of days before the admin account password must be changed.

Under **Administrator Password**, you can change the administrator password for the 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**.

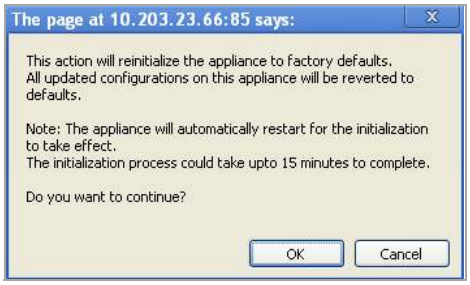
Managing System Settings

The **System > Settings** page provides a way to upload new 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.

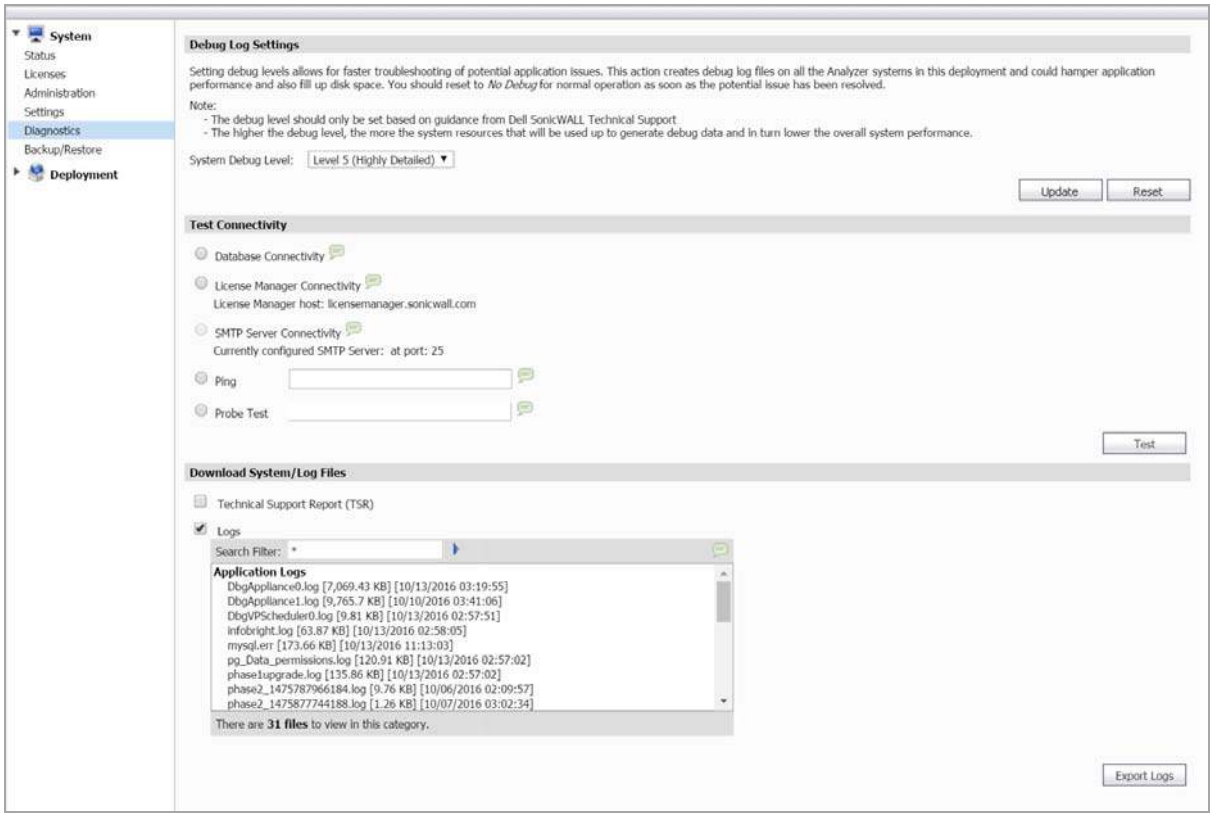
The Reinitialize Appliance to Factory Settings section allows the administrator to reset all UMH system settings to factory defaults. Click **Reinitialize** to reset to factory defaults. A pop-up message displays for the administrator to confirm this process.



Click **OK**, the system reboots and the reinitialization process takes 10-15 minutes to complete. After the reinitialization process is complete, the administrator needs to log back in 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:

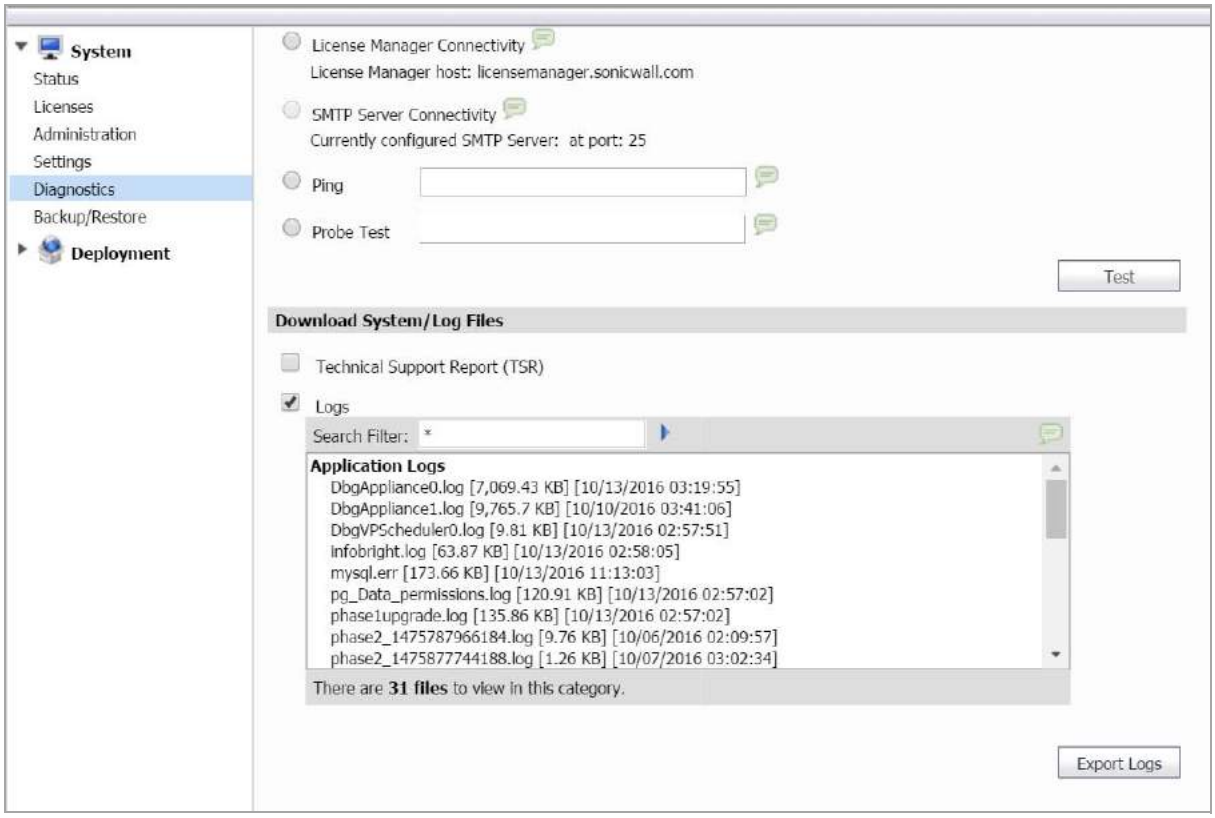
- No Debug
- Level 1 (Codepath)
- Level 2 (Simple)
- Level 3 (Logic)
- Level 4 (Detailed)
- Level 5 (Highly Detailed)

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.

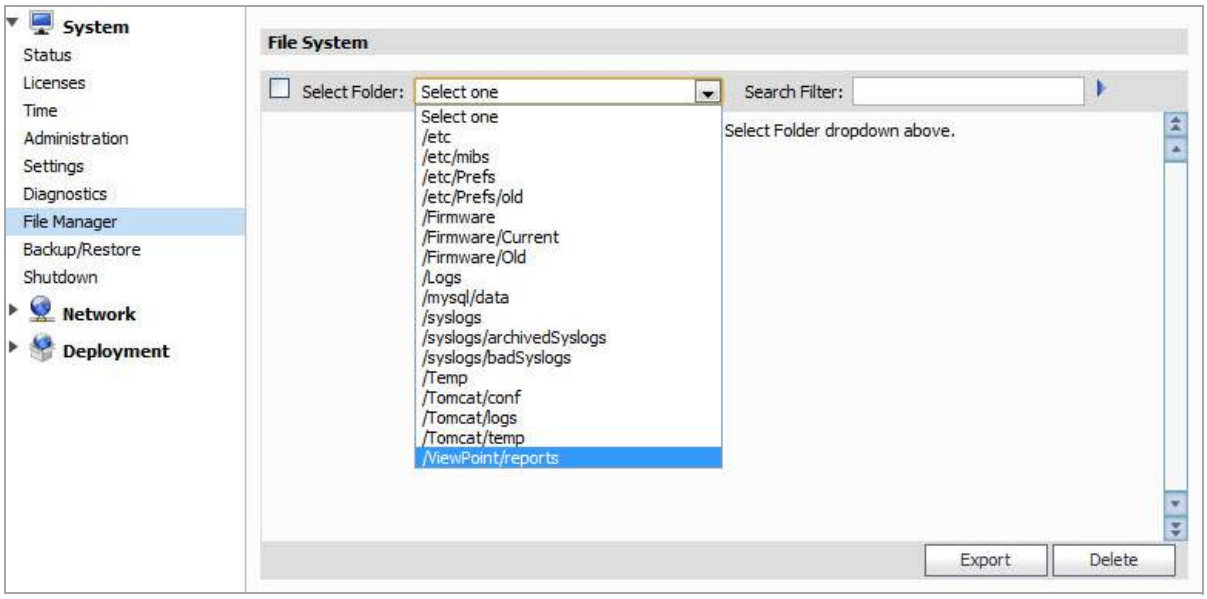
In the **Download System/Log Files** section, you can enter a filter, or search value, into either of the **Search Filter** fields, and then press **Enter**, to locate log entries of interest. Click **Export Logs** to save the log files to a file on your computer.



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

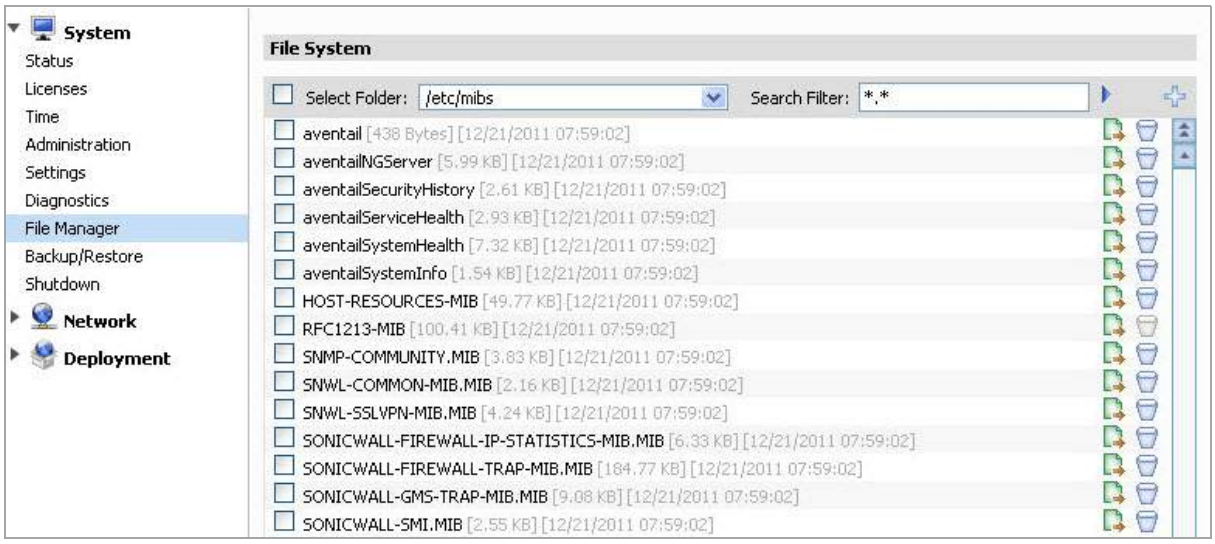
Using System File Manager (Virtual Appliance)

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

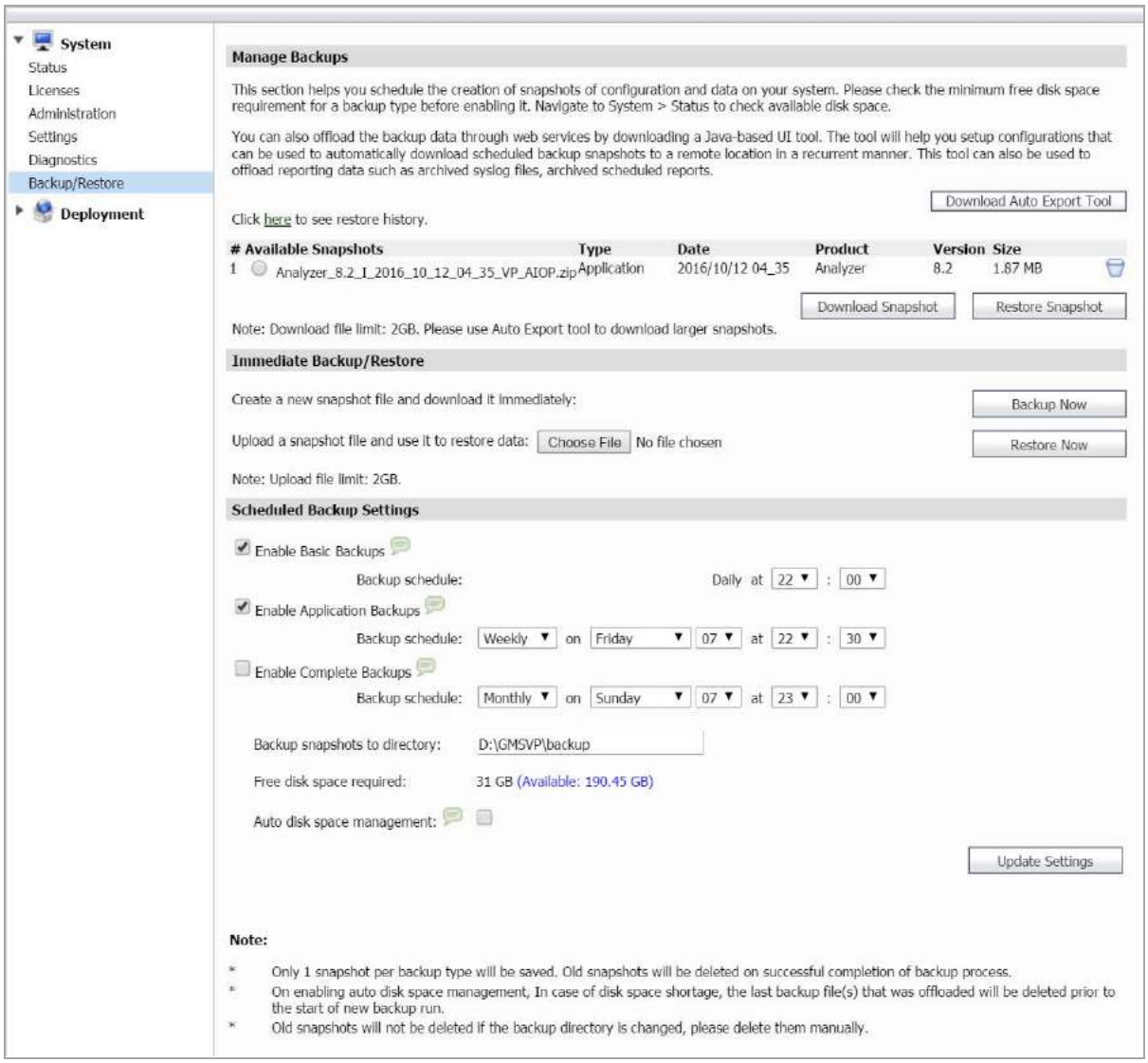
Administrators can also use the file manager to import files, such as, third-party MIB files to the directory folder for multiple-vendor solution interoperability. To import or to upload a file, select a folder from the drop-down menu. The page refreshes and displays the contents of the selected folder. In the top-right corner of the page, click the plus icon to upload a file. Next, click **Choose File** to open the file management dialog box. In the file management dialog box, navigate to the file you would like to upload and click **Open**. The selected file is now displayed next to **Choose File**. Click **Upload** 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 off-load the backup/reporting data through web services by downloading a Java-based UI tool. This tool helps you setup configurations that can be used to automatically download backup snapshots to a remote location in a reoccurring schedule.



Manage Backups

Manage backups

Name	Description
Download Auto Export Tool	Helps you setup configurations that can be used to automatically download scheduled backup snapshots to a remote location in a recurrent manner. It also allows the user to offload reporting data such as archived syslog files and archived scheduled reports to a remote location
Click here to see restore history link	Displays the restored snapshots.
Available Snapshots list	Displays all the available snapshots with type, date, product, version, and size information for each.
Download Snapshot	Downloads a snapshot of the current system configurations.
Restore Snapshot	Restores a backup snapshot, the snapshot is uploaded to your local storage and then used to restore data.

Immediate Backup/Restore

Immediate Backup/Restore

Name	Description
Backup Now	Creates a new basic, application, or complete snapshot file.
Choose File	Selects a snapshot file from your local file system to upload to the Analyzer server.
Restore Now	Restores using the selected snapshot file.

Scheduled Backup Settings

Scheduled Backup Settings

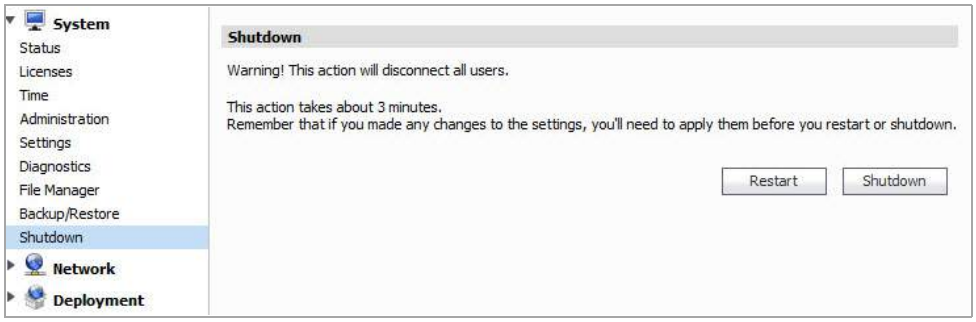
Name	Description
Enable Basic Backups check box	Backs up files that are essential for the system configuration and addUnit.xml files on a daily basis.
Daily At drop down lists	Selects the hour and minute for the backup schedule.
Enable Application Backups check box	Backs up basic data, database, firmware images, and HM recordings on a monthly or weekly schedule.
Backup Schedule: drop down lists	Selects the week or month, day, hour, and minute for the backup schedule.
Enable Complete Backups check box	Backs up application backup data, reporting database, and archived scheduled reports from the default archive directory on a monthly or weekly schedule.
Backup Schedule drop down lists	Selects the month or week, day, hour, and minute for the backup schedule.
Backup Snapshots to Directory text field	Backs up snapshots to the directory that is entered into the text field.

Scheduled Backup Settings (Continued)

Name	Description
Free disk space required	Indicates the space required to perform the backup, and how much space is available for use on the resource. If available disk space is less than the estimated free disk space required, the backup process will not start. However, if the auto disk space management feature is enabled, the backup process deletes the previous backup files to free the disk space required for the backup process to begin if the following conditions are satisfied:
Auto disk space management	Select to allow Analyzer to manage the disk space and backup requirements. Auto disk space management is a configurable option provided for you to automate recovering disk space by deleting previous backup files in case of a disk space shortage for the backup process. If there is sufficient disk space for the backup process to run, this feature does not have any impact.
Update Settings	Updates the current configured settings.

Using System Shutdown (Virtual Appliance)

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



Configuring UMH Network Options (Virtual Appliance)

This section describes the tasks you can do on the Network pages of the SonicWall Analyzer UMH system interface.

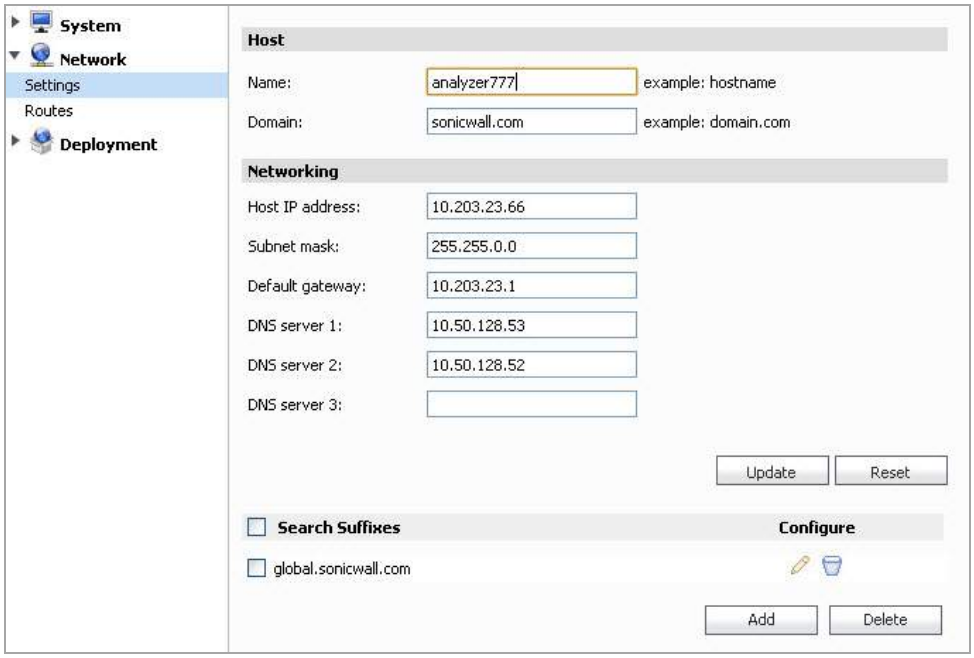
See the following sections:

- Configuring Network Settings (Virtual Appliance) on page 199
- Configuring Network Routes (Virtual Appliance) on page 199

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 **Update** to apply the host and networking settings changes. Click **Reset** 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 **Add** to include multiple search suffixes, and to remove Search Suffixes, click the check box next to the Search Suffixes list, and click **Delete**.

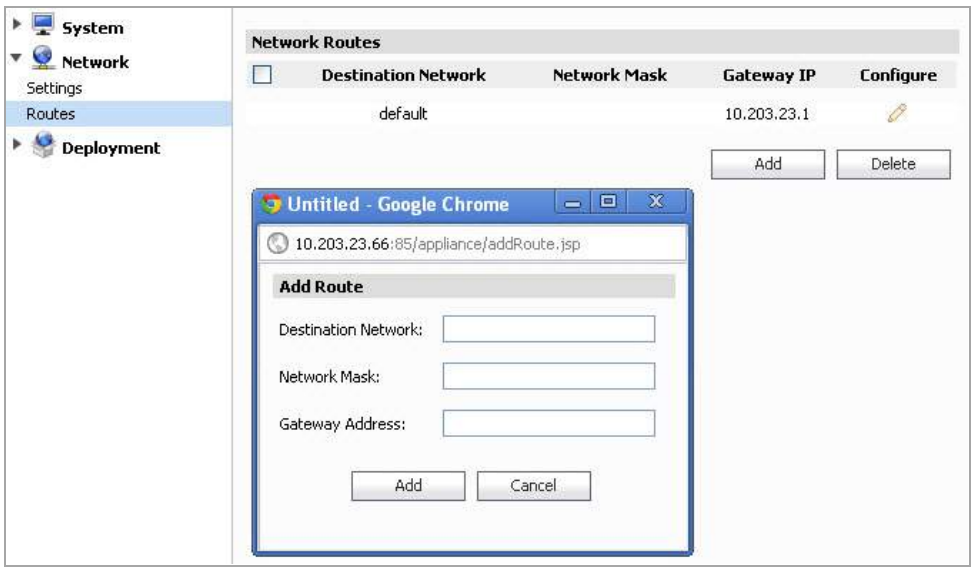


Configuring Network Routes (Virtual Appliance)

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 **Add**. To edit the default network route, click the configure icon. When multiple network routes are added to the list, selecting the check box at the

top-left corner of the page selects all the added network routes. Click **Delete** to remove a network route from the list.

NOTE: The default network route cannot be deleted.



Configuring UMH Deployment Options

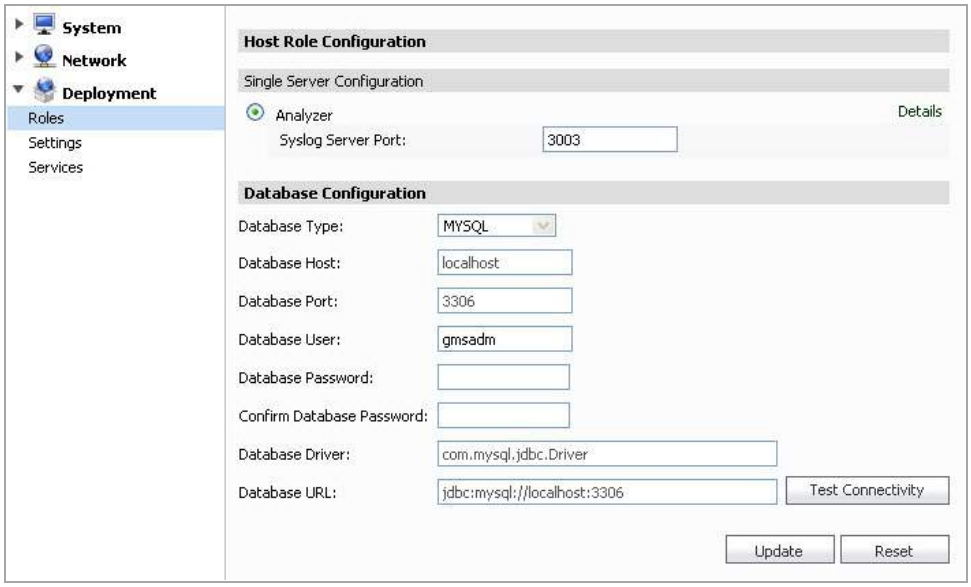
This section describes the tasks you can do on the Deployment pages of the SonicWall Analyzer UMH system interface.

See the following sections:

- Configuring the Deployment Role on page 201
- Configuring Deployment Settings on page 201
- Configuring Web Server Settings on page 202
- Configuring SMTP Settings on page 203
- Configuring SSL Access on page 203
- Controlling Deployment Services on page 204

Configuring the Deployment Role

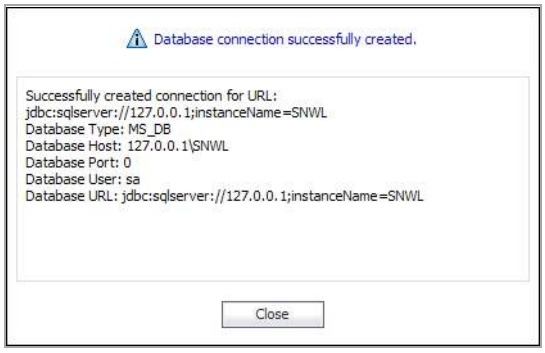
In a SonicWall Analyzer installation, the **Deployment > Roles** page provides a way to configure the syslog port and the database settings, and to test database connectivity.



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

Under Database Configuration, to provide credentials with which SonicWall Analyzer accesses 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 **Test Connectivity**. A pop-up message displays the database connectivity status.

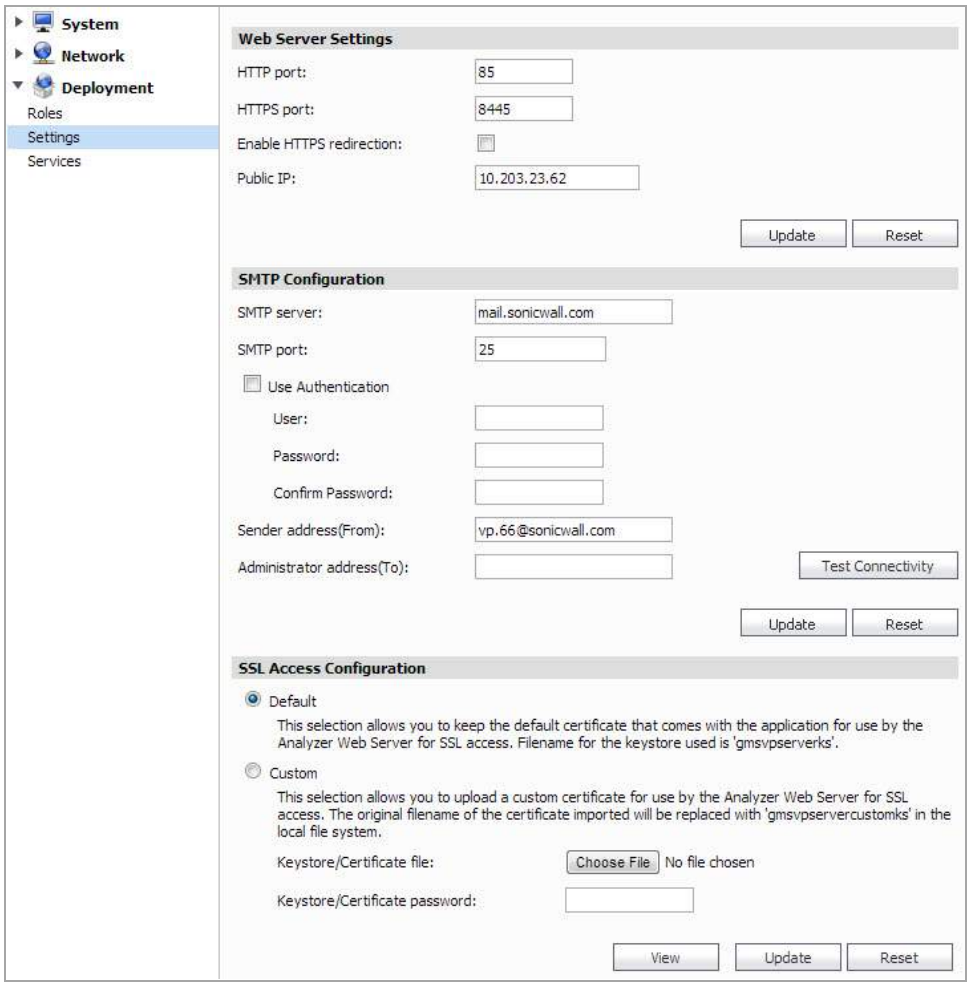


When finished, click **Update** to apply the changes. To revert the fields on the page to their default settings, click **Reset**.

Configuring Deployment Settings

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

The **Deployment > Settings** page is identical in both the UMH management interfaces.



See the following sections:

- Configuring Web Server Settings on page 202
- Configuring SMTP Settings on page 203
- Configuring SSL Access on page 203
- Controlling Deployment Services on page 204

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 SonicWall Analyzer, type the port number into the **HTTP Port** field. The default port is 85.

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 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 **Enable HTTPS Redirection** 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 **Update**.

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, complete the following steps:

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 Click **Use TLS** if you would like to use Transport Layer Security (TLS) for your mail server connectivity, such as for Gmail or Office365. TLS ensures privacy between you and communicating applications on the Internet, and that no third-party can eavesdrop or tamper with your messages.

4 If the SMTP server in your deployment is set to use authentication, click the **Use Authentication** check box. 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.

5 Type the email address from which mail is sent into the **Sender address** field.

6 Type the email address of the system administrator into the **Administrator address** field.

7 To test connectivity to the SMTP server, click **Test Connectivity**.

8 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, complete the following steps:

1 Navigate to the **Deployment > Settings** page under **SSL Access Configuration** section.

2 Select **Default** to keep, or revert to, the default settings, where the default GMS Web Server certificate with 'gmsvpserverks' keystore is used.

3 Select **Custom** to upload a custom keystore certificate for GMS SSL access.

4 In the **Keystore/Certificate** file field, click **Browse** to select your certificate file.

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

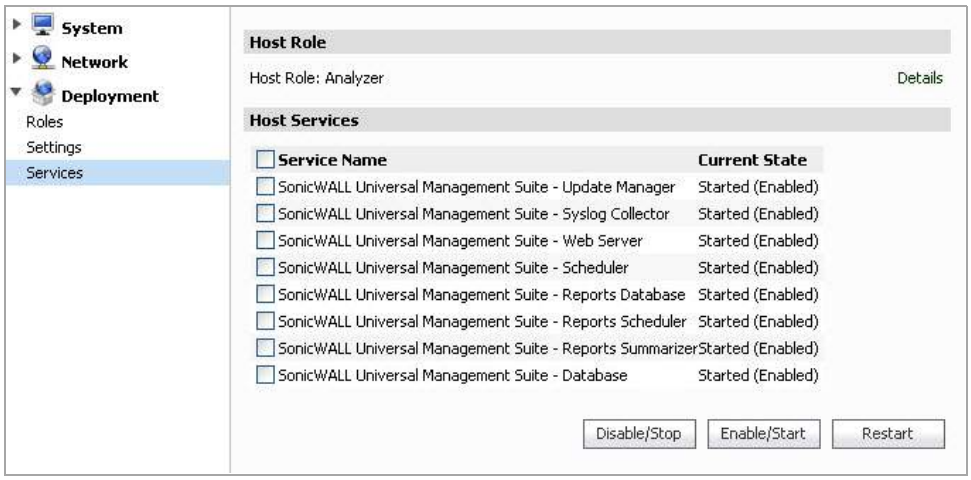
5 Type the password for the keystore certificate into the **Keystore/Certificate password** field.

6 Click **View** to display details about your keystore certificate.

7 Click **Update** 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 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 check box for that service and then click **Disable/Stop**.

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

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

Part 6

Appendices

- Upgrading
- License Agreements

A

Upgrading

This appendix is designed to help you upgrade SonicWall Analyzer. If you have not used SonicWall Analyzer before, you might want to familiarize yourself with SonicWall Analyzer concepts and features.

This appendix contains the following sections:

Upgrading to Analyzer 8.3

This section provides procedures for upgrading an existing SonicWall Analyzer 8.0 or newer installation to Analyzer 8.3. Analyzer can be configured for a single server or in a distributed environment on multiple servers. Analyzer 8.1 can be installed as a fresh install or as an upgrade from Analyzer 8.0. If you wish to perform a fresh install of Analyzer 8.3, refer to the *SonicWall Analyzer Getting Started Guide* that relates to your Analyzer deployment.

Upgrading Considerations

CAUTION: If you are upgrading to 8.3 and still have CDP appliances under management, those appliances will automatically be removed from Analyzer.

CAUTION: If you have a Windows-32 bit Analyzer Server currently in your deployment, you must first migrate or decommission those servers, before upgrading to 8.3.

Consider the following before upgrading to Analyzer 8.3:

- "The 40GB Analyzer Virtual Appliance should be installed in non-production environments only. Examples of non-production environments include those for Proof of Concept (POC), pilot, and demo deployments. Only the 250GB and 950GB virtual appliances are supported in production environments. It is not possible to upgrade a 40GB virtual appliance to a 250GB or 950GB virtual appliance. You need to download the 250GB or 950GB virtual appliance if you are planning to use this software now or in the future for a production environment.
- In non-production environments, the amount of syslog data collected by the virtual appliance may exceed the 40GB limit, in which case SonicWall will be unable to support the 40GB virtual appliance.
- You must disable the User Account Control (UAC) feature on Windows before running the Analyzer installer. In addition, disable Windows Firewall or your personal firewall before running this installer.
- Analyzer can only be configured for a single server.

Upgrading Procedure

To upgrade to Analyzer 8.3, complete the following steps:

1 Navigate to www.mysonicwall.com.

2 Download the Analyzer 8.3 software.

`sw_gmsvp_win_eng_8.3.xxxx.yyyy.exe`

3 After the file has downloaded, double-click the file and follow the onscreen instructions. The Installer detects any previous installations of Analyzer. Click **Install** to proceed with the installation.

4 If you see a Windows Security Alert for Java, click **Unblock**. The installer displays a progress bar as the files are installed. Wait a few minutes for the installer to finish installing.

5 After the files are installed, whether or not the system has a Personal Firewall such as 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 if you plan to use HTTPS Management mode for managing remote appliances (instead of Analyzer Management Tunnel or Existing Tunnel modes). Click **OK**. Be sure to adjust the settings as recommended.

6 After the version file is installed, reboot the system to complete the installation.

Upgrading the Analyzer virtual appliance

The Analyzer Virtual Appliance can be upgraded from 8.2 to 8.3. To upgrade the Analyzer Virtual Appliance from a version earlier than 7.2, you need to upgrade to major versions of Analyzer until you reach 7.2, then you can upgrade to Analyzer 8.3. For SonicWall Analyzer Virtual Appliance deployments, upgrading from the Analyzer 8.0 release to the Analyzer 8.3 release can be performed on the **System > Settings** page.

In a distributed environment, shut down all Analyzer servers except the one that is running the database. Then upgrade the Console/AIOP first and then the other servers. You must upgrade all Analyzer servers in your deployment to the same version of SonicWall Analyzer 8.3. You cannot have some servers running version 8.2 and others running 8.3.

For a fresh install of the Analyzer 8.3 64-bit Virtual Appliance, refer to the *SonicWall Analyzer Virtual Appliance Getting Started Guide*.

To upgrade, complete the following:

1 Download the Analyzer 8.3 file from www.mysonicwall.com to your workstation:

`sw_gmsvp_vm_eng_8.3.xxxx.yyyy.gmsvp-updater.64bit.sh`

2 Log in to the /appliance (System) interface of the Analyzer server.

3 Navigate to the **System > Settings** page.

4 Click **Browse**, navigate to the location where you saved the above file, and select it.

5 Click **Apply** to begin the firmware upgrade installation.

The Virtual Appliance reboots at the end of the installation process.

Upgrading SonicWall ViewPoint 6.0 to Analyzer 8.3

The SonicWall Analyzer cannot be directly upgraded from ViewPoint 6.0 to Analyzer 8.3, but it can be upgraded from Analyzer 7.0. To upgrade the 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 8.3.

To upgrade major versions of SonicWall Analyzer, use the Universal Management Suite installer and complete the following steps:

1 Log on to your 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 might 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 SonicWall Services bind for capturing syslog and SNMP packets, and Web port settings.

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

7 The Important Registration Information screen provides the URL for access to the SonicWall 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**

NOTE: To register for a SonicWall Analyzer installation, log in to the Universal Management Host system interface, then click **Register** in the top-right corner. The License Management page displays, enter the word "ANALYZER" in the Serial Number field and leave the Authentication Code fields blank. Enter a name into the Friendly Name field, then click **Submit**. For complete instructions, refer to the latest *SonicWall Analyzer Getting Started Guide* for your deployment.

8 Click **Next**.

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

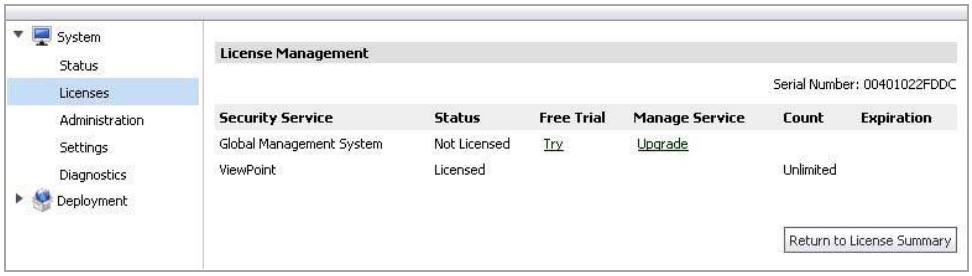
In the SonicWall Analyzer login page, enter the same credentials for **User** and **Password** that you had in your earlier version prior to the upgrade.

Upgrading from Analyzer to GMS

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, **Try GMS Free - 30 Days** 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 SonicWall GMS Free Trial and purchasing the SonicWall GMS upgrade license, see the following sections:

- Enabling the GMS Free Trial from Analyzer on page 209
- Enabling the GMS Free Trial from the UMH Interface on page 212
- Completing the Free Trial Upgrade on page 212
- Configuring Appliances for GMS Management on page 215
- Purchasing a SonicWall GMS Upgrade on page 217

Enabling the GMS Free Trial from Analyzer

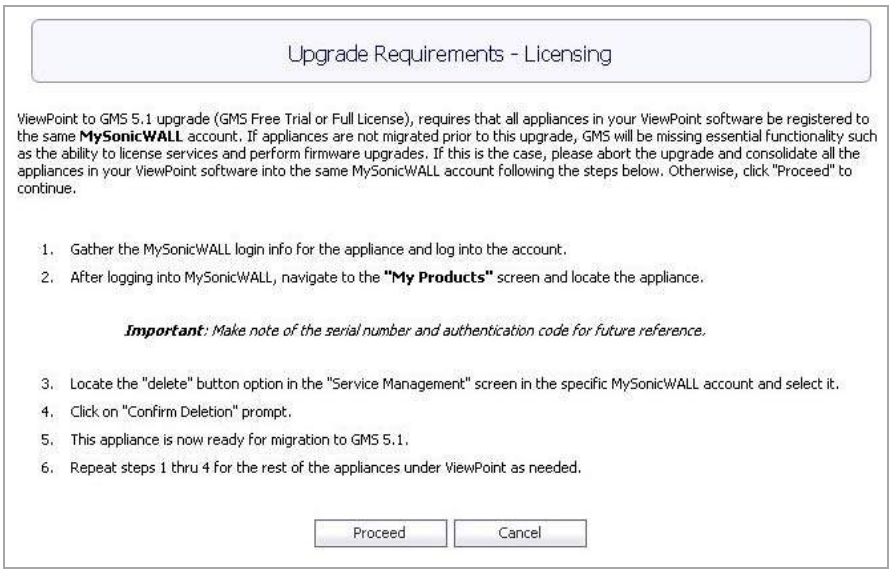
When five or more devices are connected to SonicWall Analyzer reporting, **Try GMS Free - 30 Days** appears next to the tabs at the top of the Analyzer management interface.

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 see the list of appliances under **Associated Products**.

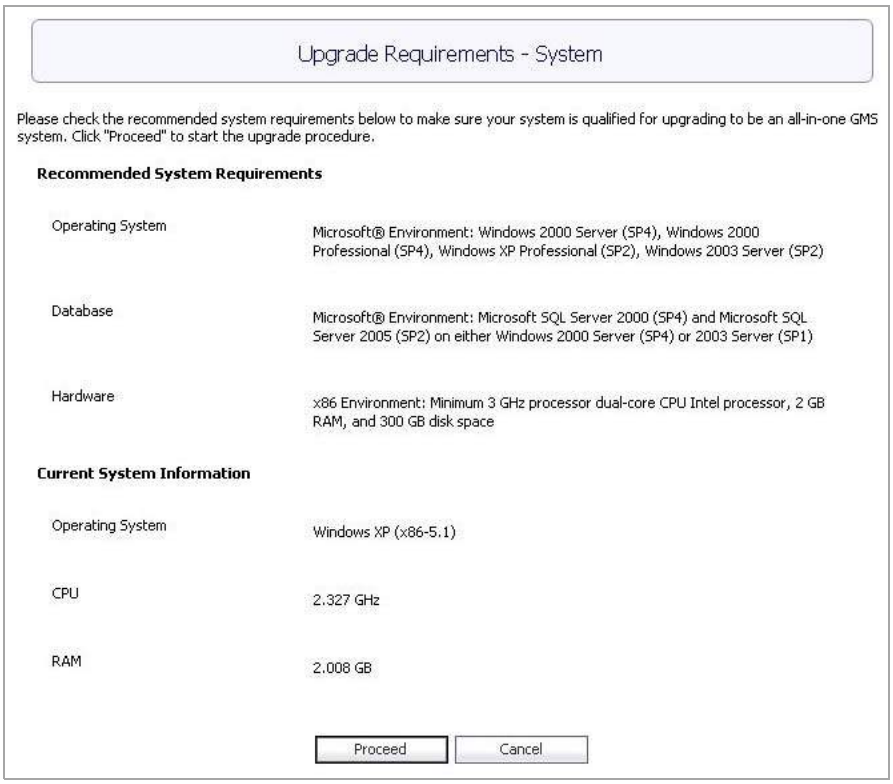
To enable the 30-day SonicWall GMS Free Trial from the Analyzer management interface, complete the following steps:

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

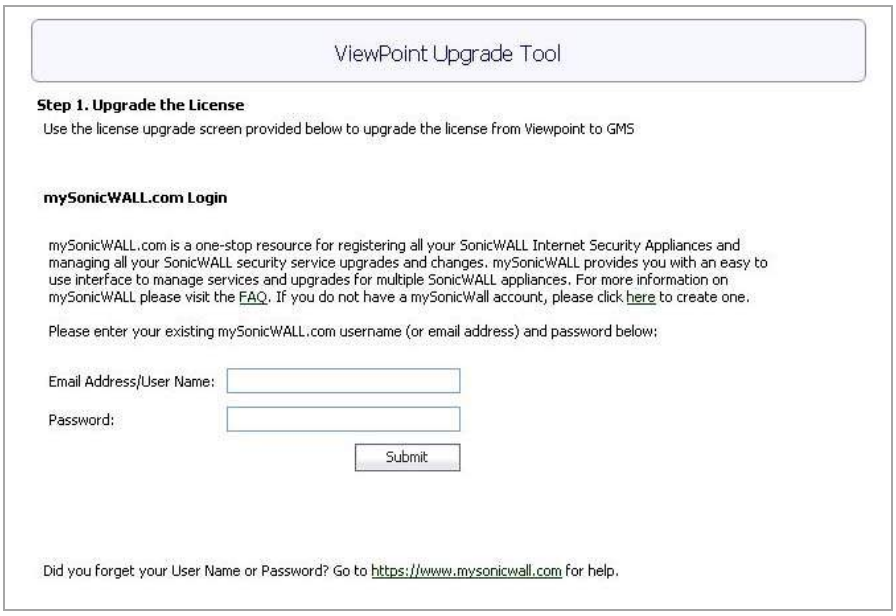
2 The Analyzer Upgrade Tool launches and guides you through the process of installing the Free Trial or Upgrade. The tool displays the **Upgrade Requirements – Licensing** screen. Before migrating to GMS, ensure that all appliances under Analyzer reporting are registered to the same MySonicWall account.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



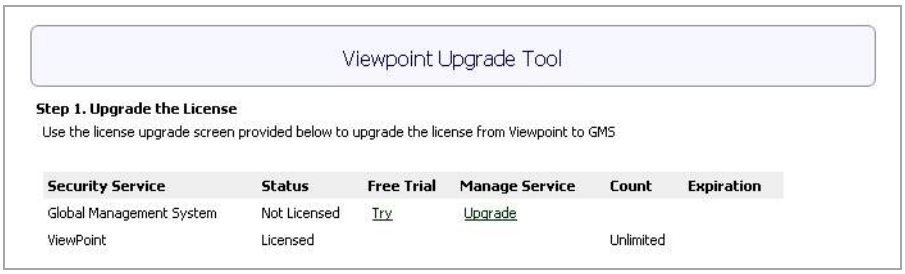
3 The **Upgrade Requirements – System** screen displays the recommended operating system, database, and hardware system requirements. Click **Proceed**.



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, complete the steps in Completing the Free Trial Upgrade on page 212.

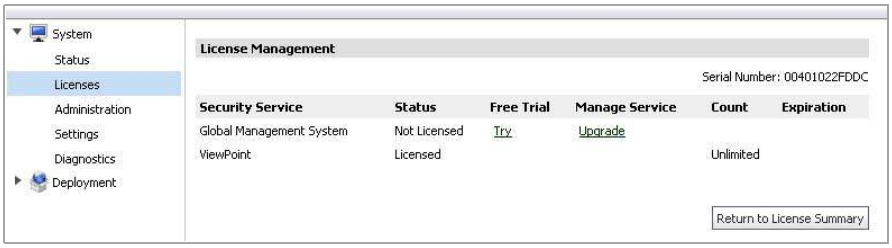
Enabling the GMS Free Trial from the UMH Interface

To enable the 30-day Free Trial of SonicWall GMS from the Universal Management Host interface on your SonicWall Analyzer system, complete 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, complete the steps in Completing the Free Trial Upgrade on page 212.

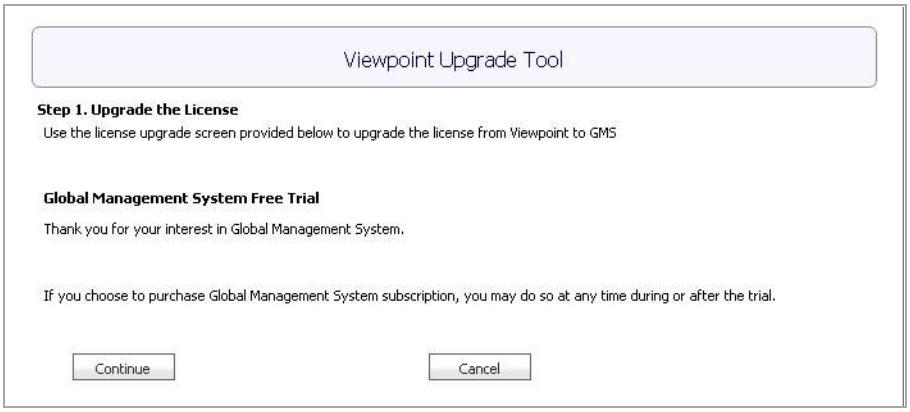
Completing the Free Trial Upgrade

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:

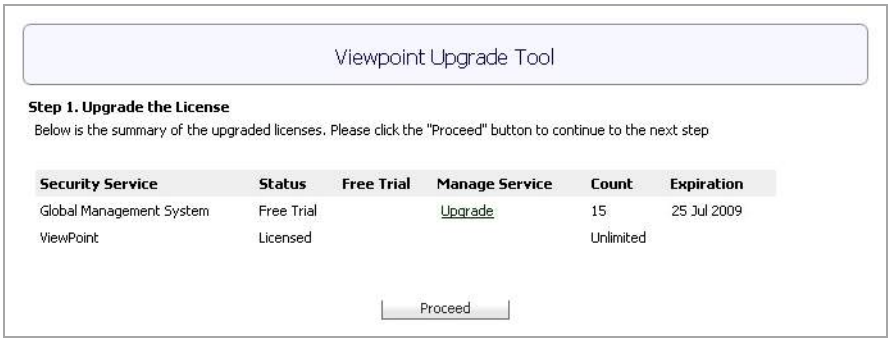
- Enabling the GMS Free Trial from Analyzer on page 209
- Enabling the GMS Free Trial from the UMH Interface on page 212

To continue the upgrade, complete the following steps:

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



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**.

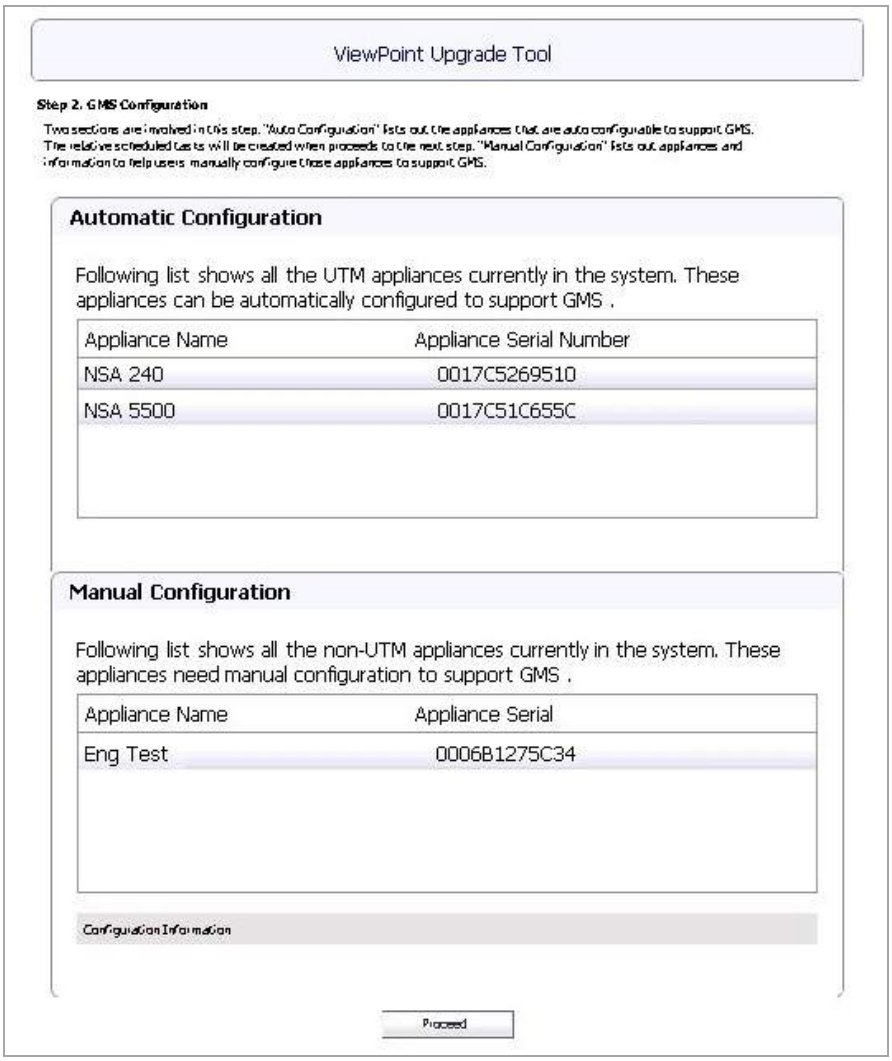


3 In the next Analyzer Upgrade Tool page, you begin the configuration for GMS in step 2 of the upgrade process. This page displays two sections:

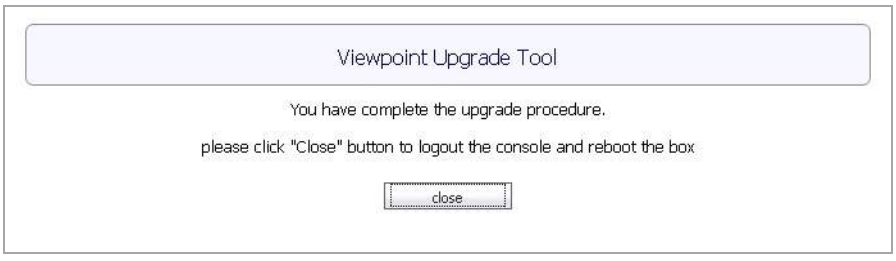
Automatic Configuration – Contains a list of SonicWall firewall or CSM appliances in your Analyzer installation. These appliances are automatically configured for GMS management.

Manual Configuration – Contains a list of SonicWall or SSL-VPN appliances in your Analyzer installation. You must manually configure these appliances for GMS management. See Configuring Appliances for GMS Management on page 215 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.

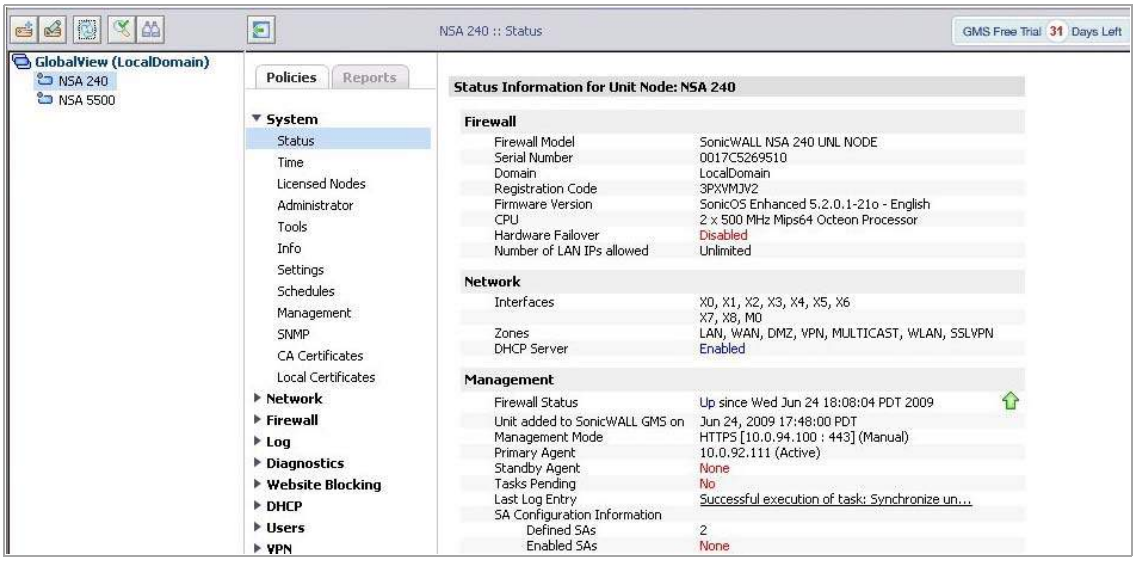


5 The GMS login page appears and requests that you reboot the system. Reboot the system. If a reboot is not done, you might encounter problems with the correct IP Address appearing.

6 After rebooting, log in with your Analyzer credentials.

When you log in, you 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.



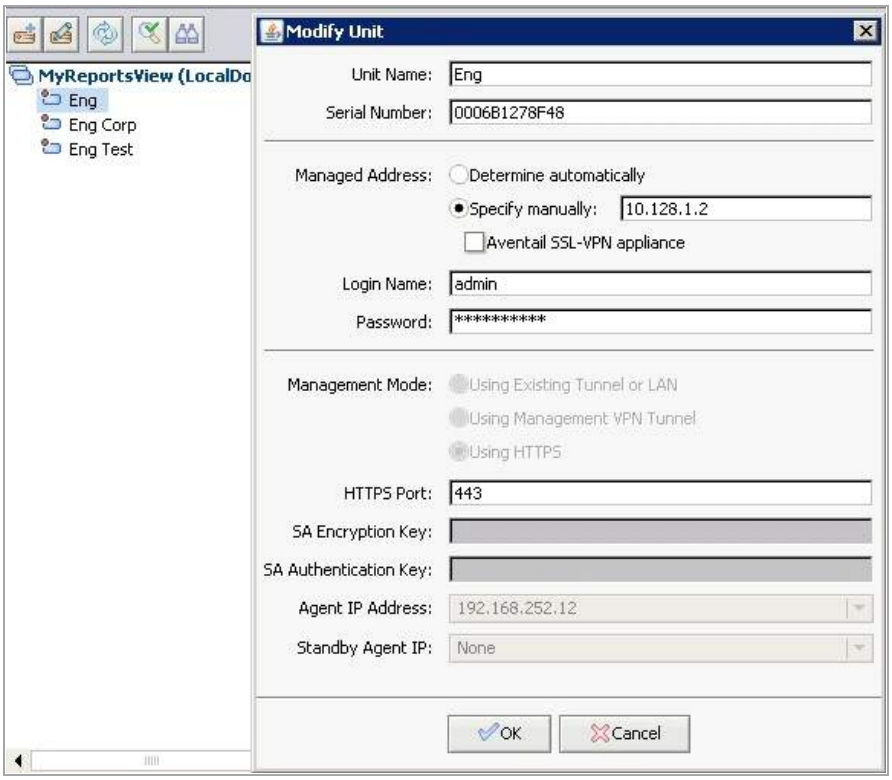
Configuring Appliances for GMS Management

To manually configure the appliances listed in the Manual Configuration section of the Analyzer Upgrade Tool page, complete 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**.

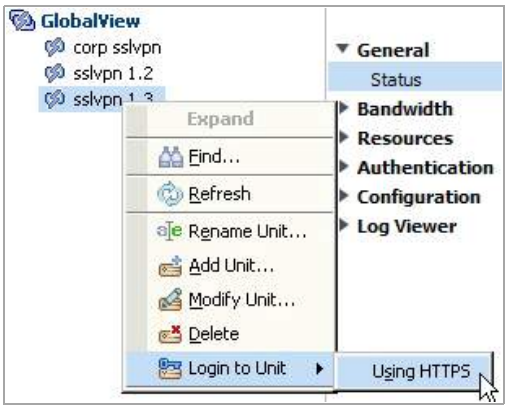
2 In the left pane, right-click one of the listed appliances and select **Modify Unit**.

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.

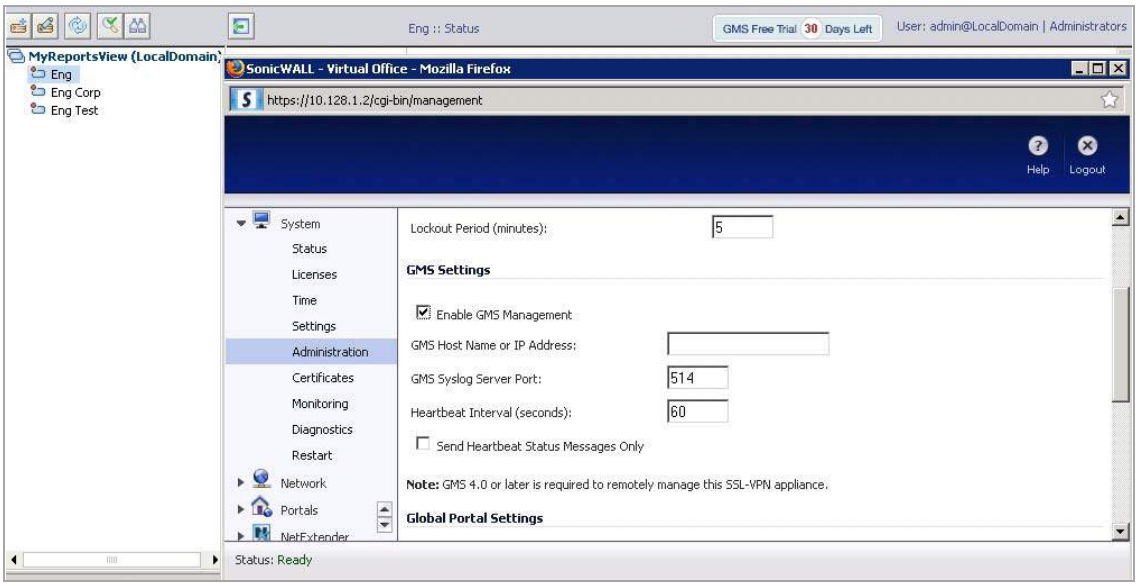


4 Click **Cancel**.

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** check box, 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 **Accept** at the top of the appliance interface screen.

10 Click **Logout** 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.

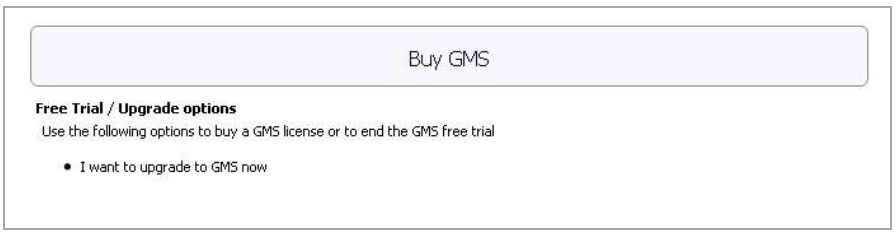
Purchasing a SonicWall GMS Upgrade

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

To purchase the SonicWall GMS license, complete the following steps:

1 In the GMS interface, click **GMS Free Trial X Days Left**, 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 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 appears in your MySonicWall account.

7 If your Analyzer installation currently handles more than 10 appliances, when you upgrade to GMS, you 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 might need to complete. Select from the following:

- It is highly recommended that you regularly back up the SonicWall Analyzer data. For more information, see Backing up SonicWall Analyzer Data on page 219.
- 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 219.
- If you are reinstalling SonicWall Analyzer, preserving the previous configuration settings can save a lot of time. To reinstall SonicWall Analyzer using an existing SonicWall Analyzer database, see Reinstalling SonicWall Analyzer Using an Existing Database on page 219.
- If you need to uninstall SonicWall Analyzer from a server, it is important to do it correctly. To uninstall SonicWall Analyzer, see Uninstalling SonicWall Universal Management Suite and Its Database on page 220.

Backing up SonicWall Analyzer Data

SonicWall Analyzer stores its configuration data in the SGMSDB database. It is important to back up this database and the individual 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 Infobright with Postgres (IB-PG) 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 SonicWall Analyzer services for database backup. However, make sure that the backup occurs when SonicWall Analyzer activity is the lowest and that the backup operation schedule does not clash with the SonicWall Analyzer scheduler.

NOTE: It is also recommended to regularly back up the entire contents of the SonicWall Analyzer directory, the `sgmsConfig.xml` file.

Changing the SQL Server Authentication Mode

SonicWall Analyzer requires the Mixed Mode authentication mode.

To change the authentication mode from Windows Mode to Mixed Mode, complete the following steps:

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

Reinstalling SonicWall Analyzer Using an Existing Database

If you need to reinstall SonicWall Analyzer, but want to preserve the settings in an existing SonicWall Analyzer database, complete the following steps:

1. Install a new database, using the same username and password that you used for the existing SonicWall Analyzer database.

2 Install SonicWall Analyzer using this new database.

3 Stop all 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 SonicWall Analyzer database.

5 Restart the 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 220.
- To uninstall SonicWall Universal Management Suite databases from Microsoft SQL Server 2000, see MS SQL Server 2000 on page 220.

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.

B

License Agreements

You can view the End User License Agreement and all Third-Party Product Licenses in the **Console > Help > About** screen of the Analyzer user Interface.

This appendix details the following licensing agreements:

End User Software License Agreement

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THIS PRODUCT. BY DOWNLOADING, INSTALLING OR USING THIS PRODUCT, YOU ACCEPT AND AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. FOR DELIVERIES OUTSIDE THE UNITED STATES OF AMERICA, PLEASE GO TO HTTPS://WWW.SONICWALL.COM/LEGAL/EUPA.ASPX TO VIEW THE APPLICABLE VERSION OF THIS AGREEMENT FOR YOUR REGION. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT OR THE APPLICABLE VERSION OF THIS AGREEMENT FOR YOUR REGION, DO NOT DOWNLOAD, INSTALL OR USE THIS PRODUCT.

This SonicWall End User Product Agreement (the "Agreement") is made between you, the Customer ("Customer" or "**You**") and the Provider, as defined below.

1. **Definitions**. Capitalized terms not defined in context shall have the meanings assigned to them below:

(a) "Affiliate" means any legal entity controlling, controlled by, or under common control with a party to this Agreement, for so long as such control relationship exists.

(b) "Appliance" means a computer hardware product upon which Software is pre-installed and delivered.

(c) "Documentation" means the user manuals and documentation that Provider makes available for the Products, and all copies of the foregoing.

(d) "Maintenance **Services**" means Provider's maintenance and support offering for the Products as identified in the Maintenance Services Section below.

(e) "Partner" means the reseller or distributor that is under contract with Provider or another Partner and is authorized via such contract to resell the Products and/or Maintenance Services.

(f) "Provider" means, (i) for the US, Europe, Middle East, Africa, Latin America, and Taiwan, SonicWall Inc., with its principal place of business located at 4 Polaris Way, Aliso Viejo, CA 92656 USA and (ii) for Asia (other than Taiwan) SonicWall International Ltd. City Gate Park Mahon, Cork, Ireland.

(g) "Products" means the Software and Appliance(s) provided to Customer under this Agreement.

(h) "Software" means the object code version of the software that is delivered on the Appliance and any other software that is later provided to Customer as well as any new versions and releases to such software that are made available to Customer pursuant to this Agreement, and all copies of the foregoing.

2. **Software License.**

(a) **General**. Subject to the terms of this Agreement, Provider grants to Customer, and Customer accepts from Provider, a non-exclusive, non-transferable (except as otherwise set forth herein) and non-sublicensable license to access and use the quantities of each item of Software purchased from Provider or a Partner within the parameters of the license type ("License **Type(s)"**) described below in the quantities purchased ("License"). Except for MSP Licenses (as defined below), Customer shall only use the Software to support the internal business operations of itself and its worldwide Affiliates.

(b) **License Types.** The License Type for the Software initially delivered on the Appliance is "per ***Appliance"***. Software licensed per Appliance may be used only on the Appliance on which it is delivered, but without any other quantitative limitations. Software that is purchased on a subscription, or periodic basis is licensed by User or by Managed Node. A "User" is each person with a unique login identity to the Software. A "Managed **Node"** is any object managed by the Software including, but not limited to firewalls, devices, and other items sold by Provider.

(c) **Software as a Service.** When Customer purchases a right to access and use Software installed on equipment operated by Provider or its suppliers (the "SaaS ***Software"***), (i) the License for such SaaS Software shall be granted for the duration of the term stated in the order (the "SaaS ***Term"***), as such SaaS Term may be extended by automatic or agreed upon renewals, and (ii) the terms set forth in the SaaS Provisions Section of this Agreement shall apply to all access to and use of such Software. If any item of Software to be installed on Customer's equipment is provided in connection with SaaS Software, the License duration for such Software shall be for the corresponding SaaS Term, and Customer shall promptly install any updates to such Software as may be provided by Provider.

(d) **MSP License.**

"Management ***Services***" include, without limitation, application, operating system, and database implementation, performance tuning, and maintenance services provided by Customer to its customers (each, a "Client") where Customer installs copies of the Software on its Clients' equipment or provides its Clients access to the Products. Customer shall be granted a License to use the Software and the associated Documentation to provide Management Services (the "MSP ***License"***). Each MSP License is governed by the terms of this Agreement and any additional terms agreed to by the parties.

If the Product is to be used by Customer as a managed service provider, then Customer shall ensure that (i) Customer makes no representations or warranties related to the Products in excess of SonicWall's representations or warranties contained in this Agreement, (ii) each Client only uses the Products and Documentation as part of the Management Services provided to it by Customer, (iii) such use is subject to the restrictions and limitations contained in this Agreement, including, but not limited to those in the Export Section of this Agreement, and (iv) each Client cooperates with Provider during any compliance review that may be conducted by Provider or its designated agent. At the conclusion of any Management Services engagement with a Client, Customer shall promptly remove any Appliance and Software installed on its Client's computer equipment or require the Client to do the same. Customer agrees that it shall be jointly and severally liable to Provider for the acts and omissions of its Clients in connection with their use of the Software and Documentation and shall, at its

expense, defend Provider against any action, suit, or claim brought against Provider by a Client in connection with or related to Customer's Management Services and pay any final judgments or settlements as well as Provider's expenses in connection with such action, suit, or claim.

(e) **Evaluation/Beta License.** If Software is obtained from Provider for evaluation purposes or in beta form, Customer shall be granted a License to use such Software and the associated Documentation solely for Customer's own non-production, internal evaluation purposes (an "Evaluation ***License***"). Each Evaluation License shall be granted for an evaluation period of up to thirty (30) days beginning (i) five (5) days after the Appliance is shipped or (ii) from the date that access is granted to the beta Software or the SaaS Software, plus any extensions granted by Provider in writing (the "Evaluation Period"). There is no fee for an Evaluation License during the Evaluation Period, however, Customer is responsible for any applicable shipping charges or taxes which may be incurred, and any fees which may be associated with usage beyond the scope permitted herein. Beta Software licensed hereunder may include pre-release features and capabilities which may not be available in SonicWall's generally available commercial versions of the Software. SonicWall retains the right during the term of the Evaluation License to modify, revise, or remove SonicWall beta software from Customer's premises. Customer acknowledges that SonicWall owns all modifications, derivative works, changes, expansions or improvements to beta software, as well as all reports, testing data or results, feedback, benchmarking or other analysis completed in whole or in part in conjunction with usage of beta software. NOTWITHSTANDING ANYTHING OTHERWISE SET FORTH IN THIS AGREEMENT, CUSTOMER UNDERSTANDS AND AGREES THAT EVALUATION AND BETA SOFTWARE IS PROVIDED "AS IS", WHERE IS, WITH ALL FAULTS AND THAT SONICWALL DOES NOT PROVIDE A WARRANTY OR MAINTENANCE SERVICES FOR EVALUATION OR BETA LICENSES, AND SONICWALL BEARS NO LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES RESULTING FROM USE (OR ATTEMPTED USE) OF THE EVALUATION OR BETA SOFTWARE THROUGH AND AFTER THE EVALUATION PERIOD AND HAS NO DUTY TO PROVIDE SUPPORT TO CUSTOMER FOR SUCH SOFTWARE. BETA SOFTWARE MAY CONTAIN DEFECTS AND A PRIMARY PURPOSE OF LICENSING THE BETA SOFTWARE IS TO OBTAIN FEEDBACK ON THE BETA SOFTWARE'S PERFORMANCE AND THE IDENTIFICATION OF DEFECTS. CUSTOMER IS ADVISED TO SAFEGUARD IMPORTANT DATA, TO USE CAUTION AND NOT TO RELY IN ANY WAY ON THE CORRECT FUNCTIONING OR PERFORMANCE OF THE BETA SOFTWARE AND/OR ACCOMPANYING MATERIALS.

(f) **Use by Third Parties.** Customer may allow its services vendors and contractors (each, a "Third **Party User**") to access and use the Products and Documentation provided to Customer hereunder solely for purposes of providing services to Customer, provided that Customer ensures that (i) the Third Party User's access to or use of the Products and Documentation is subject to the restrictions and limitations contained in this Agreement, including, but not limited to those in the Export Section, (ii) the Third Party User cooperates with Provider during any compliance review that may be conducted by Provider or its designated agent, and (iii) the Third Party Users promptly removes any Software installed on its computer equipment upon the completion of the Third Party's need to access or use the Products as permitted by this Section. Customer agrees that it shall be liable to Provider for those acts and omissions of its Third Party Users which, if done or not done by Customer, would be a breach of this Agreement.

3. **Restrictions**. Customer may not reverse engineer, decompile, disassemble, or attempt to discover or modify in any way the underlying source code of the Software, or any part thereof unless and to the extent (a) such restrictions are prohibited by applicable law and (b) Customer has requested interoperability information in writing from Provider and Provider has not provided such information in a timely manner. In addition, Customer may not (i) modify, translate, localize, adapt, rent, lease, loan, create or prepare derivative works of, or create a patent based on the Products, Documentation or any part thereof, (ii) resell, sublicense or distribute the Products or Documentation, (iii) provide, make available to, or permit use of the Products, in whole or in part, by any third party (except as expressly set forth herein), (iv) use the Products or Documentation to create or enhance a competitive offering or for any other purpose which is competitive to Provider, (v) remove Software that was delivered on an Appliance from the Appliance on which it was delivered and load such Software onto a different appliance without Provider's prior written consent, or (vi) perform or fail to perform any other act which would result in a misappropriation or infringement of Provider's intellectual property rights in the Products or Documentation. Each permitted copy of the Software and Documentation made by Customer hereunder must contain all titles, trademarks, copyrights and restricted rights notices as in the original. Customer understands and agrees that the Products may work in conjunction with third party products and Customer agrees to be responsible for ensuring that it is properly licensed to use such third party products. Notwithstanding anything otherwise set forth in this Agreement, the terms and restrictions set forth herein shall not prevent or restrict Customer from exercising additional or different rights to any open source software that may be contained in or provided with the Products in accordance with the applicable open source software licenses which shall be either included with the Products or made available to Customer upon request. Customer may not use any license keys or other license access devices not provided by Provider, including but not limited to "pirate keys", to install or access the Software.

4. **Proprietary Rights.** Customer understands and agrees that (i) the Products are protected by copyright and other intellectual property laws and treaties, (ii) Provider, its Affiliates and/or its licensors own the copyright, and other intellectual property rights in the Products, (iii) the Software is licensed, and not sold, (iv) this Agreement does not grant Customer any rights to Provider's trademarks or service marks, and (v) Provider reserves any and all rights, implied or otherwise, which are not expressly granted to Customer in this Agreement.

5. **Title.** Provider, its Affiliates and/or its licensors own the title to all Software.

6. **Payment.** Customer agrees to pay to Provider (or, if applicable, the Partner) the fees specified in each order, including any applicable shipping fees. Customer will be invoiced promptly following delivery of the Products or prior to the commencement of any Renewal Maintenance Period and Customer shall make all payments due to Provider in full within thirty (30) days from the date of each invoice or such other period (if any) stated in an order. Provider reserves the right to charge Customer a late penalty of 1.5% per month (or the maximum rate permitted by law, whichever is the lesser) for any amounts payable to Provider by Customer that are not subject to a good faith dispute and that remain unpaid after the due date until such amount is paid.

7. **Taxes.** The fees stated in an order from Provider or a Partner may not include taxes. If Provider is required to pay sales, use, property, value-added or other taxes based on the Products or Maintenance Services provided under this Agreement or on Customer's use of Products or Maintenance Services, then such taxes shall be billed to and paid by Customer. This Section does not apply to taxes based on Provider's or a Partner's income.

8. **Termination.**

(a) This Agreement or the Licenses granted hereunder may be terminated (i) by mutual written agreement of Provider and Customer or (ii) by either party for a breach of this Agreement by the other party (or a Third Party User) that the breaching party fails to cure to the non-breaching party's reasonable satisfaction within thirty (30) days following its receipt of notice of the breach. Notwithstanding the foregoing, in the case of MSP Licenses, if Customer or its Client breaches this Agreement two (2) times in any twelve (12) consecutive month period, the breaching party shall not have a cure period for such breach and Provider may terminate this Agreement immediately upon providing written notice to the breaching party.

(b) Upon termination of this Agreement or expiration or termination of a License for any reason, all rights granted to Customer for the applicable Software shall immediately cease and Customer shall immediately: (i) cease using the applicable Software and Documentation, (ii) remove all copies, installations, and instances of the applicable Software from all Appliances, Customer computers and any other devices on which the Software was installed, and ensure that all applicable Third Party Users and Clients do the same, (iii) return the applicable Software to Provider together with all Documentation and other materials associated with the Software and all copies of any of the foregoing, or destroy such items, (iv) cease using the Maintenance Services associated with the applicable Software, (v) pay Provider or the applicable Partner all amounts due and payable up to the date of termination, and (vi) give Provider a written certification, within ten (10) days, that Customer, Third Party Users, and Clients, as applicable, have complied with all of the foregoing obligations.

(c) Any provision of this Agreement that requires or contemplates execution after (i) termination of this Agreement, (ii) a termination or expiration of a License, or (iii) the expiration of a SaaS Term, is enforceable against the other party and their respective successors and assignees notwithstanding such termination or expiration, including, without limitation, the Restrictions, Payment, Taxes, Termination, Survival, Warranty Disclaimer, Infringement Indemnity, Limitation of Liability, Confidential Information, Compliance Verification, and General Sections of this Agreement. Termination of this Agreement or a License shall be without prejudice to any other remedies that the terminating party or a Partner may have under law, subject to the limitations and exclusions set forth in this Agreement.

9. **Export.** Customer acknowledges that the Products and Maintenance Services are subject to the export control laws, rules, regulations, restrictions and national security controls of the United States and other applicable foreign agencies (the "Export Controls") and agrees to abide by the Export Controls. Customer hereby agrees to use the Products and Maintenance Services in accordance with the Export Controls, and shall not export, re-export, sell, lease or otherwise transfer the Products or any copy, portion or direct product of the foregoing in violation of the Export Controls. Customer is solely responsible for obtaining all necessary licenses or authorizations relating to the export, re-export, sale, lease or transfer of the Products and for ensuring compliance with the

requirements of such licenses or authorizations. Customer hereby (i) represents that Customer, and if Customer is providing services under the MSP License herein each of its Clients, is not an entity or person to which shipment of Products, or provision of Maintenance Services, is prohibited by the Export Controls; and (ii) agrees that it shall not export, re-export or otherwise transfer the Products to (a) any country subject to a United States trade embargo, (b) a national or resident of any country subject to a United States trade embargo, (c) any person or entity to which shipment of Products is prohibited by the Export Controls, or (d) anyone who is engaged in activities related to the design, development, production, or use of nuclear materials, nuclear facilities, nuclear weapons, missiles or chemical or biological weapons. Customer shall, at its expense, defend Provider and its Affiliates from any third party claim or action arising out of any inaccurate representation made by Customer regarding the existence of an export license, Customer's failure to provide information to Provider to obtain an export license, or any allegation made against Provider due to Customer's violation or alleged violation of the Export Controls (an "Export Claim") and shall pay any judgments or settlements reached in connection with the Export Claim as well as Provider's costs of responding to the Export Claim.

10. **Maintenance Services.**

(a) **Description.** During any Maintenance Period, Provider shall:

(i) Make available to Customer new versions and releases of the Software, if and when Provider makes them generally available without charge as part of Maintenance Services.

(ii) Respond to communications from Customer that report Software failures not previously reported to Provider by Customer. Nothing in the foregoing shall operate to limit or restrict follow up communication by Customer regarding Software failures.

(iii) Respond to requests from Customer's technical coordinators for assistance with the operational/technical aspects of the Software unrelated to a Software failure. Provider shall have the right to limit such responses if Provider reasonably determines that the volume of such non-error related requests for assistance is excessive or overly repetitive in nature.

(iv) Provide access to Provider's software support web site at https://support.sonicwall.com (the "Support ***Site***").

(v) For Customers that have purchased Maintenance Services continuously since the purchase of such License, provide the repair and return program described on the Support Site for the Appliance on which the Software is delivered.

Maintenance Services are available during regional business support hours ("Business Hours") as indicated on the Support Site, unless Customer has purchased 24x7 Support. The list of Software for which 24x7 Support is available and/or required is listed in the Global Support Guide on the Support Site.

The Maintenance Services for Software that Provider has obtained through an acquisition or merger may, for a period of time following the effective date of the acquisition or merger, be governed by terms other than those in this Section. The applicable different terms, if any, shall be stated on the Support Site.

(b) **Maintenance Period.** The first period for which Customer is entitled to receive Maintenance Services begins on the date of the registration of the Product at Provider's registration portal (the "Registration") and ends twelve (12) months thereafter (the "Initial ***Maintenance Period***"). Following the Initial Maintenance Period, Maintenance Services for the Product(s) may then be renewed for additional terms of twelve (12) or more months (each, a "Renewal ***Maintenance Period"***) For purposes of this Agreement, the Initial Maintenance Period and each Renewal Maintenance Period shall be considered a "Maintenance ***Period."*** For the avoidance of doubt, this Agreement shall apply to each Renewal Maintenance Period. Cancellation of Maintenance Services will not terminate Customer's rights to continue to otherwise use the Products. Maintenance fees shall be due in advance of each Renewal Maintenance Period and shall be subject to the payment requirements set forth in this Agreement. The procedure for reinstating Maintenance Services for the Products after it has lapsed is posted at https://support.sonicwall.com/essentials/support-guide. Maintenance Services are optional and only provided if purchased separately.

For SaaS Software, the Maintenance Period is equal to the duration of the applicable SaaS Term. For non-perpetual Licenses or for non-perpetual MSP Licenses, the Maintenance Period is equal to the duration of the License.

11. **Warranties and Remedies.**

(a) **Software Warranties.** Provider warrants that, during the applicable Warranty Period (as defined in subsection (c) below),

(i) the operation of the Software, as provided by Provider, will substantially conform to its Documentation (the "Operational ***Warranty***");

(ii) the Software, as provided by Provider, will not contain any viruses, worms, Trojan Horses, or other malicious or destructive code designed by Provider to allow unauthorized intrusion upon, disabling of, or erasure of the Software, except that the Software may contain a key limiting its use to the scope of the License granted, and license keys issued by Provider for temporary use are time-sensitive (the "Virus ***Warranty"***);

(iii) it will make commercially reasonable efforts to make the SaaS Software available twenty-four hours a day, seven days a week except for scheduled maintenance, the installation of updates, those factors that are beyond the reasonable control of Provider, Customer's failure to meet any minimum system requirements communicated to Customer by Provider, and any breach of this Agreement by Customer that impacts the availability of the SaaS Software (the ***"SaaS Availability Warranty"***).

(b) **Appliance Warranties.** Provider warrants that, during the applicable Warranty Period, the Appliance will operate in a manner which allows the SNWL Software, respectively, to be used in substantial conformance with the Documentation (the "***Appliance Warranty"***,).

(c) **Warranty Periods.** The "Warranty ***Period***" for each of the above warranties (except for E-class appliances which do not include a Software warranty, shall be as follows: (i) for the Operational Warranty as it applies to Software and the Virus Warranty, ninety (90) days following the initial Registration of the Software; (ii) for the Operational Warranty as it applies to SaaS Software and the SaaS Availability Warranty, the duration of the SaaS Term; and (iv) for the Appliance Warranty, one (1) year following the date the Appliance is registered with Provider.

(d) **Remedies.** Any breach of the foregoing warranties must be reported by Customer to Provider during the applicable Warranty Period. Customer's sole and exclusive remedy and Provider's sole obligation for any such breach shall be as follows:

(i) For a breach of the *Operational Warranty* that impacts the use of Software, Provider shall correct or provide a workaround for reproducible errors in the Software that caused the breach within a reasonable time considering the severity of the error and its effect on Customer or, at Provider's option, refund the license fees paid for the nonconforming Software upon return of such Software to Provider and termination of the related License(s) hereunder.

(ii) For a breach of the *Operational Warranty* that impacts the use of SaaS Software, Provider shall correct or provide a workaround for reproducible errors in the Software that caused the breach and provide a credit or refund of the fees allocable to the period during which the Software was not operating in substantial conformance with the applicable Documentation.

(iii) For a breach of the *Virus Warranty*, Provider shall replace the Software with a copy that is in conformance with the Virus Warranty.

(v) For a breach of the *SaaS Availability Warranty*, Provider shall provide a credit or refund of the fees allocable to the period during which the SaaS Software was not available for use.

(e) **Warranty Exclusions.** The warranties set forth in this Section shall not apply to any non-conformance (i) that Provider cannot recreate after exercising commercially reasonable efforts to attempt to do so; (ii) caused by misuse of the applicable Product or by using the Product in a manner that is inconsistent with this Agreement or the Documentation; or (iii) arising from the modification of the Product by anyone other than Provider.

(f) **Third Party Products.** Certain Software may contain features designed to interoperate with third-party products. If the third-party product is no longer made available by the applicable provider, Provider may discontinue the related product feature. Provider shall notify Customer of any such discontinuation, however Customer will not be entitled to any refund, credit or other compensation as a result of the discontinuation.

(g) **Warranty Disclaimer.** THE EXPRESS WARRANTIES AND REMEDIES SET FORTH IN THIS SECTION ARE THE ONLY WARRANTIES AND REMEDIES PROVIDED BY PROVIDER HEREUNDER. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, ALL OTHER WARRANTIES OR REMEDIES ARE EXCLUDED, WHETHER EXPRESS OR IMPLIED, ORAL OR WRITTEN, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE,

NON-INFRINGEMENT, SATISFACTORY QUALITY, AND ANY WARRANTIES ARISING FROM USAGE OF TRADE OR COURSE OF DEALING OR PERFORMANCE. PROVIDER DOES NOT WARRANT UNINTERRUPTED OR ERROR-FREE OPERATION OF THE PRODUCTS.

(h) **High-Risk Disclaimer.** CUSTOMER UNDERSTANDS AND AGREES THAT THE PRODUCTS ARE NOT FAULT-TOLERANT AND ARE NOT DESIGNED OR INTENDED FOR USE IN ANY HIGH-RISK OR HAZARDOUS ENVIRONMENT, INCLUDING WITHOUT LIMITATION, THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION, AIR TRAFFIC CONTROL, LIFE SUPPORT MACHINES, WEAPONS SYSTEMS, OR ANY OTHER APPLICATION WHERE THE FAILURE OR MALFUNCTION OF ANY PRODUCT CAN REASONABLY BE EXPECTED TO RESULT IN DEATH, PERSONAL INJURY, SEVERE PROPERTY DAMAGE OR SEVERE ENVIRONMENTAL HARM (A "***HIGH RISK ENVIRONMENT***"). ACCORDINGLY, (I) CUSTOMER SHOULD NOT USE THE PRODUCTS IN A HIGH RISK ENVIRONMENT, (II) ANY USE OF THE PRODUCTS BY CUSTOMER IN A HIGH RISK ENVIRONMENT IS AT CUSTOMER'S OWN RISK, (III) PROVIDER, ITS AFFILIATES AND SUPPLIERS SHALL NOT BE LIABLE TO CUSTOMER IN ANY WAY FOR USE OF THE PRODUCTS IN A HIGH RISK ENVIRONMENT, AND (IV) PROVIDER MAKES NO WARRANTIES OR ASSURANCES, EXPRESS OR IMPLIED, REGARDING USE OF THE PRODUCTS IN A HIGH RISK ENVIRONMENT.

12. **Infringement Indemnity.** Provider shall indemnify Customer from and against any claim, suit, action, or proceeding brought against Customer by a third party to the extent it is based on an allegation that the Software directly infringes any patent, copyright, trademark, or other proprietary right enforceable in the country in which Provider has authorized Customer to use the Software, including, but not limited to the country to which the Software is delivered to Customer, or misappropriates a trade secret in such country (a "Claim"). Indemnification for a Claim shall consist of the following: Provider shall (a) defend or settle the Claim at its own expense, (b) pay any judgments finally awarded against Customer under a Claim or any amounts assessed against Customer in any settlements of a Claim, and (c) reimburse Customer for the reasonable administrative costs or expenses, including without limitation reasonable attorneys' fees, it necessarily incurs in responding to the Claim. Provider's obligations under this *Infringement Indemnity* Section are conditioned upon Customer (i) giving prompt written notice of the Claim to Provider, (ii) permitting Provider to retain sole control of the investigation, defense or settlement of the Claim, and (iii) providing Provider with cooperation and assistance as Provider may reasonably request in connection with the Claim. Provider shall have no obligation hereunder to defend Customer against any Claim (a) resulting from use of the Software other than as authorized by this Agreement, (b) resulting from a modification of the Software other than by Provider, (c) based on Customer's use of any release of the Software after Provider recommends discontinuation because of possible or actual infringement and has provided a non-infringing version at no charge, or (d) to the extent the Claim arises from or is based on the use of the Software with other products, services, or data not supplied by Provider if the infringement would not have occurred but for such use. If, as a result of a Claim or an injunction, Customer must stop using any Software ("Infringing ***Software***"), Provider shall at its expense and option either (1) obtain for Customer the right to continue using the Infringing Software, (2) replace the Infringing Software with a functionally equivalent non-infringing product, (3) modify the Infringing Software so that it is non-infringing, or (4) terminate the License for the Infringing Software and (A) for non-SaaS Software, accept the return of the Infringing Software and refund the license fee paid for the Infringing Software, pro-rated over a sixty (60) month period from the date of initial delivery of such Software, or (B) for SaaS Software, discontinue Customer's right to access and use the Infringing Software and refund the unused pro-rated portion of any license fees pre-paid by Customer for such Software. This Section states Provider's entire liability and its sole and exclusive indemnification obligations with respect to a Claim and Infringing Software.

13. **Limitation of Liability**. EXCEPT FOR (A) ANY BREACH OF THE *RESTRICTIONS* OR *CONFIDENTIAL INFORMATION* SECTIONS OF THIS AGREEMENT, (B) AMOUNTS CONTAINED IN JUDGMENTS OR SETTLEMENTS WHICH PROVIDER OR CUSTOMER IS LIABLE TO PAY TO A THIRD PARTY UNDER THE *INFRINGEMENT INDEMNITY* SECTION OF THIS AGREEMENT AND CUSTOMER IS LIABLE TO PAY ON BEHALF OF OR TO PROVIDER UNDER THE *CONDUCT*, *EXPORT*, *MSP LICENSE*, AND *USE BY THIRD PARTIES SECTIONS* OF THIS AGREEMENT, OR (C) ANY LIABILITY TO THE EXTENT LIABILITY MAY NOT BE EXCLUDED OR LIMITED AS A MATTER OF APPLICABLE LAW, IN NO EVENT SHALL CUSTOMER OR ITS AFFILIATES, OR PROVIDER, ITS AFFILIATES OR SUPPLIERS BE LIABLE FOR (X) ANY INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL LOSS OR DAMAGE OF ANY KIND OR (Y) LOSS OF REVENUE, LOSS OF ACTUAL OR ANTICIPATED PROFITS, LOSS OF BUSINESS, LOSS OF CONTRACTS, LOSS OF GOODWILL OR REPUTATION, LOSS OF ANTICIPATED SAVINGS, LOSS OF, DAMAGE TO OR CORRUPTION OF DATA, HOWSOEVER ARISING, WHETHER SUCH LOSS OR DAMAGE WAS FORESEEABLE OR IN THE CONTEMPLATION OF THE PARTIES AND WHETHER ARISING IN OR FOR BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF STATUTORY DUTY, OR OTHERWISE.

EXCEPT FOR (A) ANY BREACH OF THE *SOFTWARE LICENSE*, *RESTRICTIONS*, OR CONFIDENTIAL INFORMATION SECTIONS OF THIS AGREEMENT, OR ANY OTHER VIOLATION OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS; (B) PROVIDER'S EXPRESS OBLIGATIONS UNDER THE *INFRINGEMENT INDEMNITY* SECTION OF THIS AGREEMENT AND CUSTOMER'S EXPRESS OBLIGATIONS UNDER THE *CONDUCT*, *EXPORT*, *MSP LICENSE*, AND *USE BY THIRD PARTIES* SECTIONS OF THIS AGREEMENT, (C) PROVIDER'S COSTS OF COLLECTING DELINQUENT AMOUNTS WHICH ARE NOT THE SUBJECT OF A GOOD FAITH DISPUTE; (D) A PREVAILING PARTY'S LEGAL FEES PURSUANT TO THE *LEGAL FEES* SECTION OF THIS AGREEMENT; OR (E) ANY LIABILITY TO THE EXTENT LIABILITY MAY NOT BE EXCLUDED OR LIMITED AS A MATTER OF APPLICABLE LAW, THE MAXIMUM AGGREGATE AND CUMULATIVE LIABILITY OF CUSTOMER AND ITS AFFILIATES, AND PROVIDER, ITS AFFILIATES AND SUPPLIERS, FOR DAMAGES UNDER THIS AGREEMENT, WHETHER ARISING IN OR FOR BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF STATUTORY DUTY, OR OTHERWISE, SHALL BE AN AMOUNT EQUAL TO (Y) THE GREATER OF THE FEES PAID AND/OR OWED (AS APPLICABLE) BY CUSTOMER OR ITS AFFILIATES FOR THE PRODUCTS THAT ARE THE SUBJECT OF THE BREACH OR FIVE HUNDRED DOLLARS ($500.00),EXCEPT FOR (Z) MAINTENANCE SERVICES OR A PRODUCT SUBJECT TO RECURRING FEES, FOR WHICH THE MAXIMUM AGGREGATE AND CUMULATIVE LIABILITY SHALL BE THE GREATER OF THE AMOUNT PAID AND/OR OWED (AS APPLICABLE) FOR SUCH MAINTENANCE SERVICE OR PRODUCT DURING THE TWELVE (12) MONTHS PRECEDING THE BREACH OR FIVE HUNDRED DOLLARS ($500.00). THE PARTIES AGREE THAT THESE LIMITATIONS OF LIABILITY ARE AGREED ALLOCATIONS OF RISK CONSTITUTING IN PART THE CONSIDERATION FOR PROVIDER PROVIDING PRODUCTS AND SERVICES TO CUSTOMER, AND SUCH LIMITATIONS WILL APPLY NOTWITHSTANDING THE FAILURE OF THE ESSENTIAL PURPOSE OF ANY LIMITED REMEDY AND EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LIABILITIES OR FAILURES.

Provider's Affiliates and suppliers and Customer's Affiliates shall be beneficiaries of this Limitation of Liability Section and Customer's Clients and Third Party Users are entitled to the rights granted under the MSP License and Use by Third Parties Sections of this Agreement; otherwise, no third party beneficiaries exist under this Agreement. Provider expressly excludes any and all liability to Third Party Users, Clients and to any other third party.

14. **Confidential Information.**

(a) **Definition.** "Confidential ***Information"*** means information or materials disclosed by one party (the "Disclosing ***Party"***) to the other party (the "***Receiving Party"***) that are not generally available to the public and which, due to their character and nature, a reasonable person under like circumstances would treat as confidential, including, without limitation, financial, marketing, and pricing information, trade secrets, know-how, proprietary tools, knowledge and methodologies, the Software (in source code and/or object code form), information or benchmark test results regarding the functionality and performance of the Software, any Software license keys provided to Customer, and the terms and conditions of this Agreement.

Confidential Information shall not include information or materials that (i) are generally known to the public, other than as a result of an unpermitted disclosure by the Receiving Party after the date that Customer accepts the Agreement (the "Effective ***Date***"); (ii) were known to the Receiving Party without an obligation of confidentiality prior to receipt from the Disclosing Party; (iii) the Receiving Party lawfully received from a third party without that third party's breach of agreement or obligation of trust; (iv) are protected by Provider in accordance with its obligations under the Protected Data Section below, or (v) are or were independently developed by the Receiving Party without access to or use of the Disclosing Party's Confidential Information.

(b) **Obligations.** The Receiving Party shall (i) not disclose the Disclosing Party's Confidential Information to any third party, except as permitted in subsection (c) below and (ii) protect the Disclosing Party's Confidential Information from unauthorized use or disclosure by exercising at least the same degree of care it uses to protect its own similar information, but in no event less than a reasonable degree of care. The Receiving Party shall promptly notify the Disclosing Party of any known unauthorized use or disclosure of the Disclosing Party's Confidential Information and will cooperate with the Disclosing Party in any litigation brought by the Disclosing Party against third parties to protect its proprietary rights. For the avoidance of doubt, this Section shall apply to all disclosures of the parties' Confidential Information as of the Effective Date, whether or not specifically arising from a party's performance under this Agreement.

(c) **Permitted Disclosures.** Notwithstanding the foregoing, the Receiving Party may disclose the Disclosing Party's Confidential Information without the Disclosing Party's prior written consent to any of its Affiliates, directors, officers, employees, consultants, contractors or representatives (collectively, the "Representatives"), but only to those Representatives that (i) have a "need to know" in order to carry out the purposes of this Agreement or to provide professional advice in connection with this Agreement, (ii) are legally bound to the Receiving Party to protect information such as the Confidential Information under terms at least as restrictive as those provided herein, and (iii) have been informed by the Receiving Party of the confidential nature of the Confidential

Information and the requirements regarding restrictions on disclosure and use as set forth in this Section. The Receiving Party shall be liable to the Disclosing Party for the acts or omissions of any Representatives to which it discloses Confidential Information which, if done by the Receiving Party, would be a breach of this Agreement.

Additionally, it shall not be a breach of this Section for the Receiving Party to disclose the Disclosing Party's Confidential Information as may be required by operation of law or legal process, provided that the Receiving Party provides prior notice of such disclosure to the Disclosing Party unless expressly prohibited from doing so by a court, arbitration panel or other legal authority of competent jurisdiction.

15. **Protected Data.** For purposes of this Section, "Protected ***Data***" means any information or data that is provided by Customer to Provider during this Agreement that alone or together with any other information relates to an identified or identifiable natural person or data considered to be personal data as defined under Privacy Laws, and "Privacy ***Laws***" means any applicable law, statute, directive or regulation regarding privacy, data protection, information security obligations and/or the processing of Protected Data.

Except as permitted herein or to the extent required by Privacy Laws or legal process, Provider shall implement reasonable technical and organizational measures to prevent unauthorized disclosure of or access to Protected Data by third parties, and shall only store and process Protected Data as may be required to fulfill its obligations under this Agreement. If Provider complies with Customer's written instructions with respect to the Protected Data, Provider shall have no liability to Customer for any breach of this Section resulting from such compliance. Provider shall promptly notify Customer of any disclosure of or access to the Protected Data by a third party in breach of this Section and shall cooperate with Customer to reasonably remediate the effects of such disclosure or access. Provider further affirms to Customer that it has adequate agreements in place incorporating the EU standard contractual clauses for the transfer of Protected Data from the European Union ("EU") to a country outside the EU.

Customer hereby (i) represents that it has the right to send the Protected Data to Provider, (ii) consents for Provider to store and use the Protected Data worldwide for the sole purpose of performing its obligations under this Agreement, (iii) agrees that the Protected Data may be accessed and used by Provider and its Representatives worldwide as may be needed to support Provider's standard business operations, and (iv) agrees that Protected Data consisting of Customer contact information (e.g., email addresses, names) provided as part of Maintenance Services may be sent to Provider's third party service providers as part of Provider's services improvement processes.

16**. Compliance Verification.** Customer agrees to maintain and use systems and procedures to accurately track, document, and report its installations, acquisitions and usage of the Software. Such systems and procedures shall be sufficient to determine if Customer's deployment of the Software or, if applicable, use of the SaaS Software is within the quantities, terms, and maintenance releases to which it is entitled. Provider or its designated auditing agent shall have the right to audit Customer's deployment of the Software or, if applicable, use of the SaaS Software for compliance with the terms and conditions of this Agreement. Any such audits shall be scheduled at least ten (10) days in advance and shall be conducted during normal business hours at Customer's facilities. Customer shall provide its full cooperation and assistance with such audit and provide access to the applicable records and computers. Without limiting the generality of the foregoing, as part of the audit, Provider may request, and Customer agrees to provide, a written report, signed by an authorized representative, listing Customer's then current deployment of the Software and/or the number of individuals that have accessed and used SaaS Software. If Customer's deployment of the Software or, if applicable, use of the SaaS Software is found to be greater than its purchased entitlement to such Software, Customer will be invoiced for the over-deployed quantities at Provider's then current list price plus the applicable Maintenance Services and applicable over-deployment fees. All such amounts shall be payable in accordance with this Agreement. Additionally, if the unpaid fees exceed five percent (5%) of the fees paid for the applicable Software, then Customer shall also pay Provider's reasonable costs of conducting the audit. The requirements of this Section shall survive for two (2) years following the termination of the last License governed by this Agreement.

17. **SaaS Provisions.**

(a) **Data.** Customer may store data on the systems to which it is provided access in connection with its use of the SaaS Software (the "SaaS ***Environment***"). Provider may periodically make back-up copies of Customer data, however, such back-ups are not intended to replace Customer's obligation to maintain regular data backups or redundant data archives. Customer is solely responsible for collecting, inputting and updating all Customer data stored in the SaaS Environment, and for ensuring that it does not (i) knowingly create and store data that actually or potentially infringes or misappropriates the copyright, trade secret, trademark or other intellectual property right of any third party, or (ii) use the SaaS Environment for purposes that would reasonably be seen as obscene, defamatory, harassing, offensive or malicious. Provider shall have the right to delete all Customer data stored in connection with the use of the SaaS Software thirty (30) days following any termination of this Agreement or any License to SaaS Software granted hereunder.

Customer represents and warrants that it has obtained all rights, permissions and consents necessary to use and transfer all Customer and/or third party data within and outside of the country in which Customer or the applicable Customer Affiliate is located (including providing adequate disclosures and obtaining legally sufficient consents from Customer's employees, customers, agents, and contractors). If Customer transmits data to a third-party website or other provider that is linked to or made accessible by the SaaS Software, Customer will be deemed to have given its consent to Provider enabling such transmission and Provider shall have no liability to Customer in connection with any claims by a third party in connection with such transmission.

(b) **Conduct.** In connection with the use of SaaS Software, Customer may not (i) attempt to use or gain unauthorized access to Provider's or to any third-party's networks or equipment; (ii) permit other individuals or entities to copy the SaaS Software; (iii) provide unauthorized access to or use of any SaaS Software or the associated access credentials; (iv) attempt to probe, scan or test the vulnerability of the SaaS Software, the SaaS Environment, or a system, account or network of Provider or any of Provider's customers or suppliers; (v) interfere or attempt to interfere with service to any user, host or network; (vi) engage in fraudulent, offensive or illegal activity of any nature or intentionally engage in any activity that infringes the intellectual property rights or privacy rights of any individual or third party; (vii) transmit unsolicited bulk or commercial messages; (viii) intentionally distribute worms, Trojan horses, viruses, corrupted files or any similar items; (ix) restrict, inhibit, or otherwise interfere with the ability of any other person, regardless of intent, purpose or knowledge, to use or enjoy the SaaS Software (except for tools with safety and security functions); or (x) restrict, inhibit, interfere with or otherwise disrupt or cause a performance degradation to any Provider (or Provider supplier) facilities used to provide the SaaS Environment. Customer shall cooperate with Provider's reasonable investigation of SaaS Environment outages, security issues, and any suspected breach of this Section, and shall, at its expense, defend Provider and its Affiliates from any claim, suit, or action by a third party (a "Third ***Party Claim"***) alleging harm to such third party caused by Customer's breach of any of the provisions of this Section. Additionally, Customer shall pay any judgments or settlements reached in connection with the Third Party Claim as well as Provider's costs of responding to the Third Party Claim.

(c) **Suspension.** Provider may suspend Customer's use of SaaS Software (a) if so required by law enforcement or legal process, (b) in the event of an imminent security risk to Provider or its customers, or (c) if continued use would subject Provider to material liability. Provider shall make commercially reasonable efforts under the circumstances to provide prior notice to Customer of any such suspension.

18. **General.**

(a) **Governing Law and Venue.** This Agreement shall be governed by and construed in accordance with the laws of the State of California, without giving effect to any conflict of laws principles that would require the application of laws of a different state. Any action seeking enforcement of this Agreement or any provision hereof shall be brought exclusively in the state or federal courts located in the Santa Clara County, California. Each party hereby agrees to submit to the jurisdiction of such courts. The parties agree that neither the United Nations Convention on Contracts for the International Sale of Goods, nor the Uniform Computer Information Transaction Act (UCITA) shall apply to this Agreement, regardless of the states in which the parties do business or are incorporated.

(b) **Assignment.** Except as otherwise set forth herein, Customer shall not, in whole or part, assign or transfer any part of this Agreement, the Licenses granted under this Agreement or any other rights, interest or obligations hereunder, whether voluntarily, by contract, by operation of law or by merger (whether that party is the surviving or disappearing entity), stock or asset sale, consolidation, dissolution, through government action or order, or otherwise without the prior written consent of Provider. Any attempted transfer or assignment by Customer that is not permitted by this Agreement shall be null and void.

(c) **Severability.** If any provision of this Agreement shall be held by a court of competent jurisdiction to be contrary to law, such provision will be enforced to the maximum extent permissible by law to effect the intent of the parties and the remaining provisions of this Agreement will remain in full force and effect. Notwithstanding the foregoing, the terms of this Agreement that limit, disclaim, or exclude warranties, remedies or damages are intended by the parties to be

independent and remain in effect despite the failure or unenforceability of an agreed remedy. The parties have relied on the limitations and exclusions set forth in this Agreement in determining whether to enter into it.

(d) **Use by U.S. Government.** The Software is a "commercial item" under FAR 12.201. Consistent with FAR section 12.212 and DFARS section 227.7202, any use, modification, reproduction, release, performance, display, disclosure or distribution of the Software or Documentation by the U.S. government is prohibited except as expressly permitted by the terms of this Agreement. In addition, when Customer is a U.S. government entity, the language in Subsection (ii) of the *Infringement Indemnity* Section of this Agreement and the *Injunctive Relief* Section of this Agreement shall not be applicable.

(e) **Notices.** All notices provided hereunder shall be in writing and may be delivered by email, in the case of Provider to *legal@sonicwall.com* and in the case of Customer to the email address Provider has on file for Customer. All notices, requests, demands or communications shall be deemed effective upon delivery in accordance with this paragraph.

(f) **Disclosure of Customer Status.** Provider may include Customer in its listing of customers and, upon written consent by Customer, announce Customer's selection of Provider in its marketing communications.

(g) **Waiver.** Performance of any obligation required by a party hereunder may be waived only by a written waiver signed by an authorized representative of the other party, which waiver shall be effective only with respect to the specific obligation described therein. Any waiver or failure to enforce any provision of this Agreement on one occasion will not be deemed a waiver of any other provision or of such provision on any other occasion.

(h) **Injunctive Relief.** Each party acknowledges and agrees that in the event of a material breach of this Agreement, including but not limited to a breach of the *Software License*, *Restrictions* or *Confidential Information* Sections of this Agreement, the non-breaching party shall be entitled to seek immediate injunctive relief, without limiting its other rights and remedies.

(i**) Force Majeure.** Each party will be excused from performance for any period during which, and to the extent that, it is prevented from performing any obligation or service as a result of causes beyond its reasonable control, and without its fault or negligence, including without limitation, acts of God, strikes, lockouts, riots, acts of war, epidemics, communication line failures, and power failures. For added certainty, this Section shall not operate to change, delete, or modify any of the parties' obligations under this Agreement (e.g., payment), but rather only to excuse a delay in the performance of such obligations.

(j) **Equal Opportunity.** Provider is a federal contractor and Affirmative Action employer (M/F/D/V) as required by the Equal Opportunity clause C.F.R. § 60-741.5(a).

(k) **Headings**. Headings in this Agreement are for convenience only and do not affect the meaning or interpretation of this Agreement. This Agreement will not be construed either in favor of or against one party or the other, but rather in accordance with its fair meaning. When the term "including" is used in this Agreement it will be construed in each case to mean "including, but not limited to."

(l) **Legal Fees.** If any legal action is brought to enforce any rights or obligations under this Agreement, the prevailing party shall be entitled to recover its reasonable attorneys' fees, court costs and other collection expenses, in addition to any other relief it may be awarded.

(m) **Entire Agreement.** This Agreement is intended by the parties as a final expression of their agreement with respect to the subject matter thereof and may not be contradicted by evidence of any prior or contemporaneous agreement unless such agreement is signed by both parties. In the absence of such an agreement, this Agreement shall constitute the complete and exclusive statement of the terms and conditions and no extrinsic evidence whatsoever may be introduced in any proceeding that may involve the Agreement. Each party acknowledges that in entering into the Agreement it has not relied on, and shall have no right or remedy in respect of, any statement, representation, assurance or warranty (whether made negligently or innocently) other than as expressly set out in the Agreement. In those jurisdictions where an original (non-faxed, non-electronic, or non-scanned) copy of an agreement or an original (non-electronic) signature on agreements such as this Agreement is required by law or regulation, the parties hereby agree that, notwithstanding any such law or regulation, a faxed, electronic, or scanned copy of and a certified electronic signature on this Agreement shall be sufficient to create an enforceable and valid agreement. This Agreement, may only be modified or amended t by a writing executed by a duly authorized representative of each party. No other act, document, usage or custom shall be deemed to amend or modify this Agreement.

C

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract and to customers who have trial versions.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://support.sonicwall.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. In addition, the Support Portal provides direct access to product support engineers through an online Service Request system.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- Download software
- View video tutorials
- Collaborate with peers and experts in user forums
- Get licensing assistance
- Access MySonicWall
- Learn about SonicWall professional services
- Register for training and certification

To contact SonicWall Support, refer to https://support.sonicwall.com/contact-support.

To view the SonicWall End User Product Agreement (EUPA), see https://www.sonicwall.com/legal/eupa.aspx. Select the language based on your geographic location to see the EUPA that applies to your region.