

SonicWall[®] Analytics CONSOLE

Administration

SONICWALL[®]

Contents

Console Introduction	4
Contents	5
Related Documents	5
Appliance	6
Switching Between Modes	6
System	7
Status	8
Licenses	9
Time	10
Administration	11
Settings	12
Diagnostics	12
File Manager	15
Backup/Restore	18
Shutdown	20
Network	20
Settings	20
Routes	22
Deployment	23
Roles	23
Settings	24
Services	27
Flow Agent	27
IPM	27
Diagnostics	28
Debug Log Settings	28
Summarizer Status	29
Summarizer Details	30
Syslogs Details	31
3rd Party	32
Key Assignments	32
Generating a New Key	32
Flow Agent	37
Devices	37
Statistics	38
Usage	38
Monitor	39
Process Monitor	40
Log	41
Settings	41

IPM	42
Settings	42
CPU/Processor	43
Memory/RAM	44
Storage/Disk	44
Estimated Capacity	44
Capacity Estimation Settings	44
Monitor	44
History	46
Notifications	47
Global Alert	47
Mail Group	48
Configuring Email	48
Configuring an Email Group	49
Log	52
Configuration	52
View Log	53
Management	56
General	56
Changing your Password	56
Configuring the Miscellaneous Settings	56
Sessions	57
Reports	59
Summarizer	59
Syslog Filter	62
Email/Archive	63
Scheduled Reports	64
Managing the Reports	65
Navigating the Schedules Page	65
Archive	72
Licenses	73
License Summary	73
Managing Licenses	73
Refreshing Licenses	74
Uploading a License	74
SonicWall Support	75
About This Document	76

Console Introduction

This document describes the **CONSOLE** function for on-premises Analytics. This is a management function where you can set the parameters for the on-premises Analytics features. For example, you can manage the license, set the thresholds for IPM, and set your log configurations, and so forth. Both Syslog-based Analytics and IPFIX-based Analytics are included.

When accessing the Analytics **CONSOLE**, the default page is View Log (**CONSOLE > Log > View Log**), which is the same for Syslog-based and IPFIX-based Analytics.

View Log

LocalDomain

SEARCH CRITERIA

Select Time of logs From:

SonicWall Node:

Message contains:

To:

SonicWall Analytics User:

Severity: All (Alert, Warning and Info)

Match case

Exact Phrase

All Words

Any Word

SEARCH RESULTS

Messages per screen (Range: 10-100)

#	DATE	MESSAGE	SEVERITY	FIREWALL NAME	SONICWALL ANALYTICS USER	USER IP
1	Sept 26, 2019 Thur [08:20:43 PM]	Successful login into the system by user: admin	INFO		admin	10.206.23.84
2	Sept 26, 2019 Thur [08:09:30 PM]	Report data summarized: processed in 1.0 minutes.	INFO			10.206.23.84
3	Sept 26, 2019 Thur [08:07:30 PM]	Report data summarization started. All files have been queued for processing.	INFO			10.206.23.84
4	Sept 26, 2019 Thur [08:03:47 PM]	The system logged out the following user because of idle timeout violation: null	INFO			localhost (127.0.0.1)
5	Sept 26, 2019 Thur [07:53:30 PM]	Report data summarized: processed in 1.0 minutes.	INFO			10.206.23.84
6	Sept 26, 2019 Thur [07:53:07 PM]	Successful login into the system by user: admin	INFO		admin	10.206.23.84
7	Sept 26, 2019 Thur [07:52:30 PM]	Report data summarization started. All files have been queued for processing.	INFO			10.206.23.84
8	Sept 26, 2019 Thur [07:38:30 PM]	Report data summarized: processed in 1.0 minutes.	INFO			10.206.23.84
9	Sept 26, 2019 Thur [07:37:30 PM]	Report data summarization started. All files have been queued for processing.	INFO			10.206.23.84
10	Sept 26, 2019 Thur [07:23:30 PM]	Report data summarized: processed in 1.0 minutes.	INFO			10.206.23.84

Displaying 1-10

In addition to the log information in the main window, several icons appear in the top right corner.

Icons

System Status icons



Description



Provide system status. Click on the individual icons for more detail. The color of the icon indicates the status. A color other than green, indicates that features needs attention.

- CPU/Processor
- Memory/RAM
- Storage/Disk
- Estimated Capacity

Alerts and Notifications Center



Available only for IPFIX-based Analytics. Click to open the Alerts and Notifications Center. The number on the icon indicates the number of unacknowledged alerts.

Icons	Description
	Accesses the online help and the Analytics API.
	Indicates the user, the product version, and allows you to log out of the application.

Contents

This document supports both IPFIX-based reporting and Syslog-based reporting. Some of the features are the same in both styles; some features are specific to one style of reporting. The table below describes which chapters apply to which type of Analytics.

Contents for IPFIX-Based Reporting	Contents for Syslog-Based Reporting
Appliance	Appliance
Diagnostics	Diagnostics
3rd Party	
Flow Agent	
IPM	IPM
Notifications	
Log	Log
Management	Management
	Reports
Licenses	Licenses

Related Documents

The following documents provide additional information about Analytics or related firewall management applications:

- *Analytics HOME Administration*
- *Analytics REPORTS Administration*
- *ANALYTICS Administration*
- *Analytics NOTIFICATIONS Administration*

Appliance

This chapter describes the **Appliance** command option for IPFIX-based, on-premises Analytics. With this command, you can switch between **CONSOLE** mode and **Appliance** mode.

Topics:

- [Switching Between Modes](#)
- [System](#)
- [Network](#)
- [Deployment](#)
- [IPM](#)

Switching Between Modes

When you first select the **CONSOLE** view, the **Appliance** option is visible in the command menu. From here you can access the firewalls associated with your implementation.

To switch to the Appliance view:

1. Navigate to **CONSOLE > Appliance**.
2. Click the second **Appliance** link.

The menu options change to reflect the commands you can run against the appliance you selected. The **Appliance** command changes to **Analytics**, and the **System** command appears with several options you can define.

SonicWall Analytics 2.0

Status

Appliance

GENERAL

Name	SonicWall Analytics
Serial Number	[REDACTED]
Version	2.0 (Monday March 25, 2019 08:19:32 AM PDT)
Flow Agent Firmware Version	2.2-1170304
License	Licensed for SonicWall Analytics
Role	SonicWall Analytics

SYSTEM

Host Name	onpremanalytics325
IPv4 Address	[REDACTED]
IPv6 Address	[REDACTED]
Current Time	Apr 08, 2019 10:02:51 AM PDT
Up Time	13 days, 23:24
Operating System	Linux (amd64-4.14.63-soniccore)
CPU	Intel Xeon (2.90 GHz) 4 Cores Cache: 20480 (4 Logical CPUs)
RAM	8192 MB
Available Disk Space on Install Partition	43.51 GB (of Total 61.90 GB)
Available Disk Space on Data Partition	5 GB

GETTING STARTED

SonicWall technical documentation *Getting Started Guides* are available at the [MySonicWall.com Download Center](#) and the [Product Guide Library](#).

To return to the **CONSOLE** view:

- 1 Click on **Analytics**.
- 2 Select **Console**.

The menu options change back to the console management commands.

System

System command on the left navigation panel allows you to access the firewalls in your implementation and get information about them. You can also perform some basic administrative tasks on the firewall. After the System command is expanded, you see its sub-commands, which are listed below:

- [Status](#)
- [Licenses](#)
- [Time](#)
- [Administration](#)

- [Settings](#)
- [Diagnostics](#)
- [File Manager](#)
- [Backup/Restore](#)
- [Shutdown](#)

Status

The **System > Status** page provides general information about the systems you are running. The Status sections are:

- **GENERAL:** Lists the product name, serial number, version, flow agent firmware version, license, and role.

The screenshot shows the 'Status' page for SonicWall Analytics 2.0. The breadcrumb is 'Appliance'. The 'GENERAL' section is active. The following information is displayed:

Name	SonicWall Analytics
Serial Number	[Redacted]
Version	2.0 (Monday March 25, 2019 08:19:32 AM PDT)
Flow Agent Firmware Version	2.2-1170304
License	Licensed for SonicWall Analytics
Role	SonicWall Analytics

- **SYSTEM:** Gives the host name, IPv4/6 addresses, the time, up time, the OS, CPU, RAM, and available disk space on Install and Data partitions.

The screenshot shows the 'SYSTEM' section of the Status page. The following information is displayed:

Host Name	onpreanalytics325
IPv4 Address	[Redacted]
IPv6 Address	[Redacted]
Current Time	Apr 08, 2019 10:52:32 AM PDT
Up Time	14 days, 14 min
Operating System	Linux (amd64-4.14.63-soniccore)
CPU	Intel Xeon (2.90 GHz) 4 Cores Cache: 20480 (4 Logical CPUs)
RAM	8192 MB
Available Disk Space on Install Partition	43.51 GB (of Total 61.90 GB)
Available Disk Space on Data Partition	5 GB

- **GETTING STARTED:** Gives useful information on how access information for your on-premises system.

GETTING STARTED

SonicWall technical documentation *Getting Started Guides* are available at the [MySonicWall.com Download Center](#) and the [Product Guide Library](#).

Licenses

The **System > Licenses** page identifies the status and types of your licenses. You can use this page to manage, refresh or upload licenses. It also includes information about the security service and support service that may be licensed or not. Capacity and expiration are also listed to help manage your licenses more easily.

SonicWall Analytics 2.5

Licenses

Home / Appliance

LICENSE MANAGEMENT

Last SonicWall Registration Site Contact: Sep 26 2019 05:29PM
Serial Number: 004010363B5A

SECURITY SERVICE	STATUS	CAPACITY	EXPIRATION
SonicWall Analytics On-Prem	Licensed	500 GB	

SUPPORT SERVICE	STATUS	EXPIRATION
Analytics E-Class 24X7 Software Support	Not Licensed	

Manage Refresh Upload

Use the three buttons at the bottom of the Licenses table to manage the data.

- 1 Click the **Manage** button to see your license **Serial Number** at the top right of the popup window that displays.

Licenses

Home / Appliance

LICENSE MANAGEMENT

Serial Number: [REDACTED]

MySonicWall username/email

Password

LOGIN

[Forgot your Username or Password?](#)

[Return to License Summary](#)

- Enter your **MySonicWall username/email** in the text field provided.
- Enter your **Password** in the text field provided.

- Click **LOGIN** to see your license details.
 - Click the **Forgot your Username or Password?** link if needed.
 - Click **Return to License Summary** to go back to the **Licenses** page.
- 2 Click **Refresh** to update your Licenses page view.
 - 3 Click the **Upload** button to access the **UPLOAD LICENSES** popup window.

- Find your license **Serial Number** under **UPLOAD LICENSES**.
- Click **Choose File** to browse for your license document to upload.
- Click **Upload** to finish transferring your license.
- Click **Cancel** to call off your selection.

Time

The **System > Time** page shows the time that is used for the system time stamp. You can reset the time here or choose another time zone to operate in. You can also automatically configure the date and time using NTP servers.

- 1 To manually select the time, under **SYSTEM TIME**, select the **Time, Date, and Time Zone**.
- 2 To automatically set the time using an NTP server, select **Set time automatically using Network Time Protocol (NTP)**.
- 3 Enter the NTP Server addresses you want to synchronize in the text fields provided. The maximum is 5.
- 4 Click **Add NTP Server** and enter the IP address or domain name of the NTP server.

i **NOTE:** The system time automatically adjusts the clock for daylight saving time.
- 5 Click **Update** to submit your system time configuration changes.
- 6 Alternatively, click **Reset** to reset the system time to factory defaults.

Administration

The **System > Administration** page helps you ensure the proper management and configuration of your on-premises Analytics system. It has three sections: **HOST SETTINGS**, **ENHANCED SECURITY ACCESS (ESA)**, and **ADMINISTRATOR PASSWORD**.

The screenshot shows the Administration page with the following sections:

- HOST SETTINGS**: Inactivity Timeout is set to 10 minutes (-1 = never times out).
- ENHANCED SECURITY ACCESS (ESA)**:
 - Enforce Password Security
 - Number of failed login attempts before user can be locked out: 6
 - User lockout minutes: 30
 - Number of days to force password change: 90
- ADMINISTRATOR PASSWORD**:
 - Administrator Name: admin
 - Current Password: [text input]
 - New Password: [text input]
 - Confirm Password: [text input]

Buttons for **Update** and **Reset** are located at the bottom right of the form.

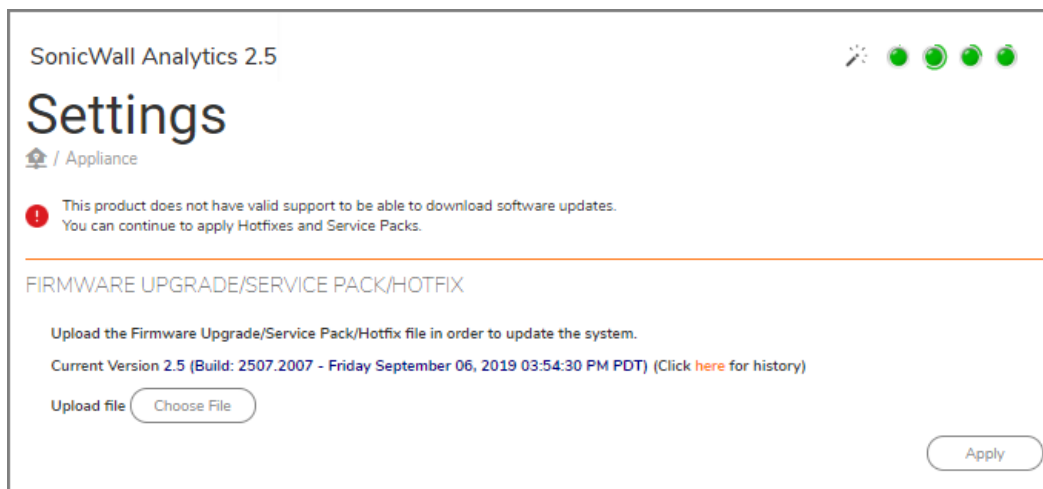
- 1 Under **HOST SETTINGS**, enter the number of minutes of inactivity allowed before the session is logged out. A setting of -1 allows an unlimited amount of inactivity without being logged out.
- 2 Under **ENHANCED SECURITY ACCESS (ESA)**, check the box next to **Enforce Password Security**, if desired, and adjust the settings.
 - The **Number of failed login attempts before user can be locked out** is 6 by default.
 - The number of **User lockout minutes** is 30 by default.
 - The **Number of days to force a password change** is 90 by default.
- 3 Under **ADMINISTRATOR PASSWORD**, check the **Administrator Name**, which is shown next to the entry.

- Enter your **Current Password** in the text field provided.
- Enter your **New Password** in the text field provided.
- **Confirm Password** in the text field provided.
- Click **Update** to make your changes.
- Click **Reset** to revert the fields on the page to their default settings.

Settings

The **System > Settings** page provides the **FIRMWARE UPGRADE/SERVICE PACK/HOTFIX** for your system. To keep your system secure, keep it up to date with the latest SonicWall security patches and service packs.

The page also lists the system **Current Version** with its build information in parenthesis. For example: **(Build: 2507.2007 - Friday September 06, 2019 03:54:30 PM PDT)**.



NOTE: If you do not have the proper support licenses, a warning message with a red exclamation mark informs you that the product does not have valid support to download software updates. You can continue to apply hotfixes and service packs manually. For a major upgrade you need the proper product support license.

To upgrade your firmware, service pack, or hotfix:

- 1 Click the **here** link, next to the **Current Version**, for your system upgrade history of all hotfixes and firmware updates.
- 2 Click **Choose File** to find the file you wish to upload.
- 3 Click **Apply**.

Diagnostics

The **System > Diagnostics** page offers a debug setting that can help you diagnose issues more quickly. This action creates debug log files on all the SonicWall Analytics systems in this deployment, but it could hamper application performance by filling up disk space. You should reset to No Debug for normal operation as soon as the potential issue has been resolved.

IMPORTANT: The debug level should only be set based on guidance from SonicWall Customer Support.

IMPORTANT: When a higher the debug level is selected, more system resources are used to generate debug data and this, in turn, may lower the overall system performance.

A **debug log** records database operations, system processes, and errors that can occur in your system. **Test connectivity** lists the end-to-end connectivity between networked devices. **System log files** record all the events happening in your network.

Debug Log Settings

Setting debug levels allows faster troubleshooting of potential application issues.

Diagnostics
Appliance

DEBUG LOG SETTINGS

Setting debug levels allows for faster troubleshooting of potential application issues. This action creates debug log files on all the SonicWall Analytics 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 will be used up to generate debug data and in turn lower the overall system performance.

System Debug Level: No Debug

Update Reset

To set the debug level when instructed by SonicWall Customer Support:

- 1 Choose the **System Debug Level** from the drop-down choices:
 - No Debug
 - Level 1 (Codepath)
 - Level 2 (Simple)
 - Level 3 (Logic)
 - Level 4 (Detailed)
 - Level 5 (Highly Detailed)
- 2 Click **Update** to make your changes.
- 3 Click **Reset** to start again.

Reporting DB Debug Log Settings

Setting debug levels allows for faster troubleshooting of potential application issues. This action increases the log level of the reporting database in this deployment. This actions can fill up disk space and impact performacne. You should reset to **Min Logs** 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 Customer Support.

Reporting DB Debug Log Settings

Setting debug levels allows for faster troubleshooting of potential application issues. This action increases the log level of Reporting DB in this deployment and could hamper application performance and also fill up disk space. You should reset to *Min Logs* 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

Reporting DB Debug Level:

License Manager Connectivity ⓘ
License Manager host lm2.sonicwall.com

SMTP Server Connectivity ⓘ
Currently configured SMTP Server at port

Ping
 ⓘ

Probe Test
 ⓘ

To set the Reporting DB Debug Log Settings:

- 1 Specify whether you want **Min Logs** or **Detail Logs** from the drop-down list next to **Reporting DB Debug Level**:
- 2 Select **License Manager Connectivity** to test against the host name, lm2.sonicwall.com
- 3 Select **SMTP Server Connectivity** to change it in the **Deployment > Settings** screen.
- 4 Select **Ping** and enter the Host Name or IP Address of the server to ping in the text field provided.
- 5 Select **Probe Test** and enter the Host Name or IP Address of the server to probe.
The port to use can be specified after the host name, separated by a colon. Use square brackets to enclose an IPv6 Address when the port number is also specified. For example, [2604:b00:a:2:0:1:df96:c605]:1234
- 6 Click **Test**.

Download System/Log Files

You can download system and log files to monitor your system activity and troubleshoot problems. The system/log files section of the Diagnostics page displays up to 301 archived files. The files are divided into **Application Logs**, **System Logs**, and **Web Server Logs**.

DOWNLOAD SYSTEM/LOG FILES

Technical Support Report (TSR)

Logs

Search Filter:

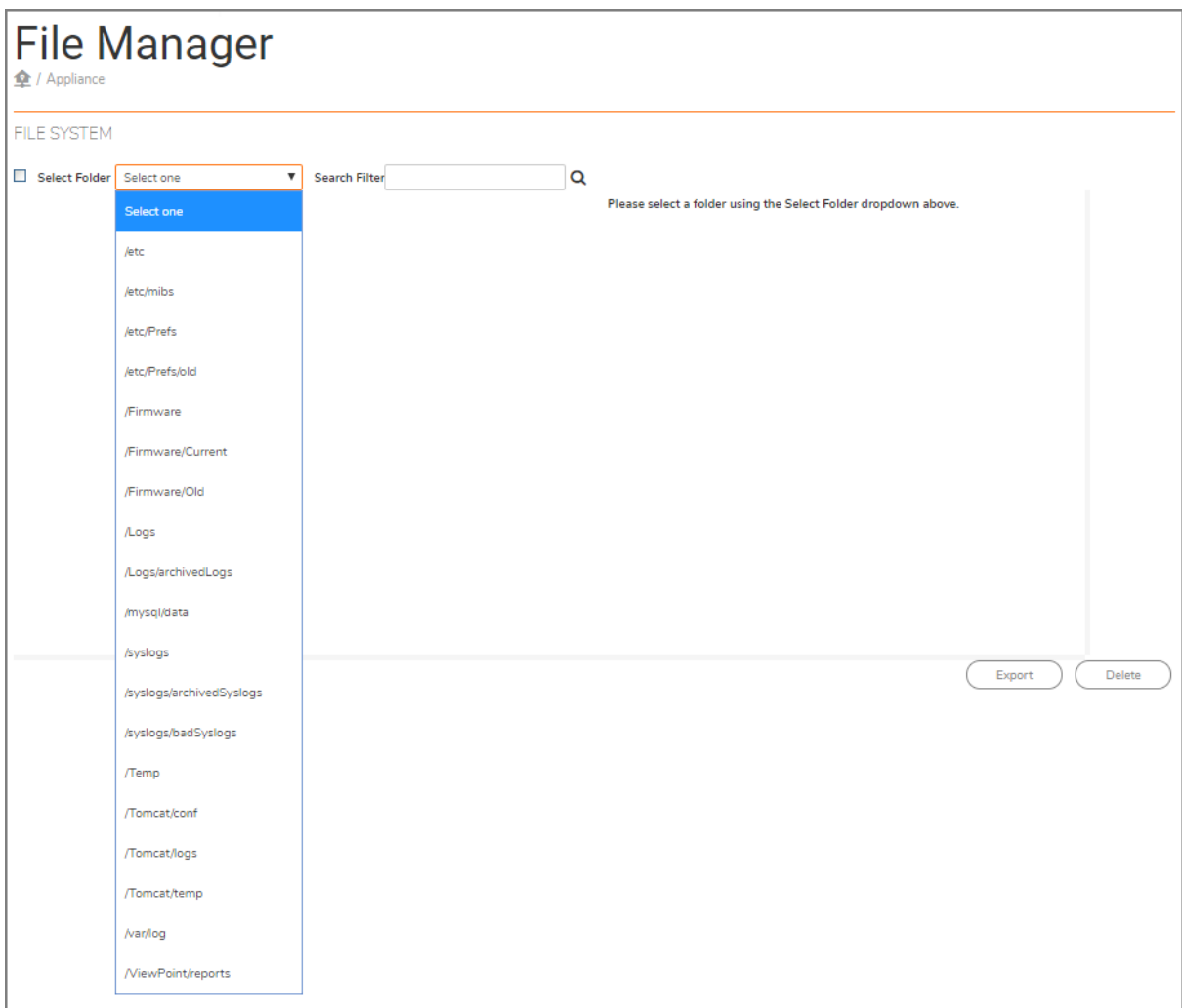
Application Logs

- appflow.log [6,118.98 KB] [04/08/2019 01:46:43]
- appflows.log [46.47 KB] [03/26/2019 11:04:49]
- archive.log [6.35 KB] [03/26/2019 11:04:29]
- DbgAppliance0.log [3,312.92 KB] [04/08/2019 01:54:24]
- DbgAppliance1.log [9,765.63 KB] [04/08/2019 10:35:40]
- DbgAppliance2.log [9,765.66 KB] [04/07/2019 10:55:30]
- DbgSysLogCollector0.log [2.04 KB] [03/25/2019 10:39:34]
- DbgVPScheduler0.log [20.13 KB] [04/08/2019 07:10:37]
- logdump.log [6.35 KB] [03/26/2019 11:04:29]

- 1 Click the check box next to **Technical Support Report (TSR)** to collect diagnostic information for your system.
- 2 Click the check box next to **Logs** to enable the **Search Filter** box.
- 3 In the **Search Filter** text field, specify filters to narrow your search. See the examples below:
 - *.log - for files with extension log
 - *.*? - for files with 3-letter extensions ending in 'g'
- 4 Click **Export** to download your system/log files to your computer.

File Manager

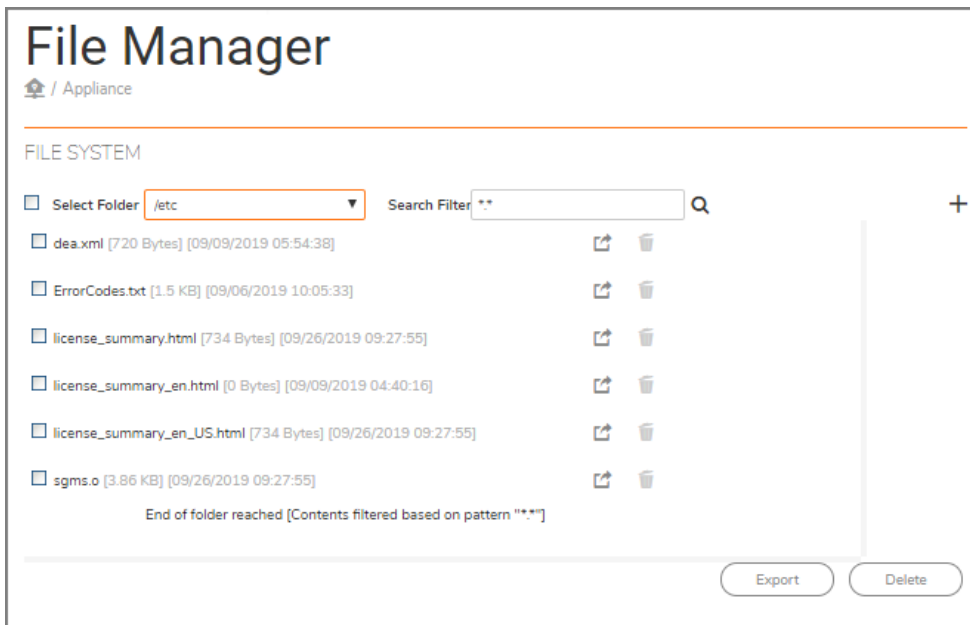
The **System > File Manager** page helps you manage your system files efficiently and easily. Administrators often use this page to export system settings preference files (/etc) to another directory location for backup archiving.



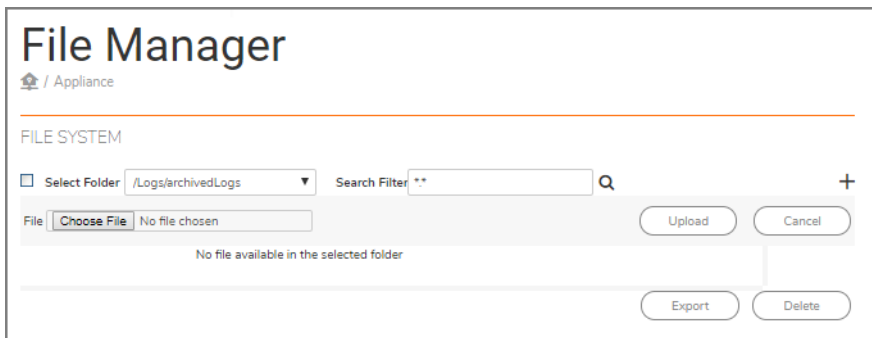
The screenshot displays the File Manager interface. At the top, it says "File Manager" and "Appliance". Below this, there is a "FILE SYSTEM" section. On the left, there is a "Select Folder" checkbox and a dropdown menu currently showing "Select one". A search filter box is also present. A list of folders is displayed in the dropdown menu, including /etc, /etc/mibs, /etc/Prefs, /etc/Prefs/old, /Firmware, /Firmware/Current, /Firmware/Old, /Logs, /Logs/archivedLogs, /mysql/data, /syslogs, /syslogs/archivedSyslogs, /syslogs/badSyslogs, /Temp, /Tomcat/conf, /Tomcat/logs, /Tomcat/temp, /var/log, and /ViewPoint/reports. On the right side, there is a message: "Please select a folder using the Select Folder dropdown above." At the bottom right, there are "Export" and "Delete" buttons.

- 1 Under **FILE SYSTEM**, check the box next to **Select Folder**.
- 2 Choose one of 19 folders from the drop-down menu. The choices are:
 - /etc
 - /etc/mibs
 - /etc/Prefs
 - /etc/Prefs/old
 - /Firmware
 - /Firmware/Current
 - /Firmware/Old
 - /Logs
 - /Logs/archivedLogs
 - /mysql/data
 - /syslogs
 - /syslogs/archivedSyslogs
 - /syslogs/badSyslogs
 - /Temp
 - /Tomcat/conf
 - /Tomcat/logs
 - /Tomcat/temp
 - /var/log
 - /ViewPoint/reports

- 3 Check the box next to the file you want. Each file category displays different content.



- 4 Click the **Export** icon next to your file to download it.
- 5 Click the **Delete** icon next to your file to delete it.
- 6 In the **Search Filter** text field, specify filters to narrow your search.



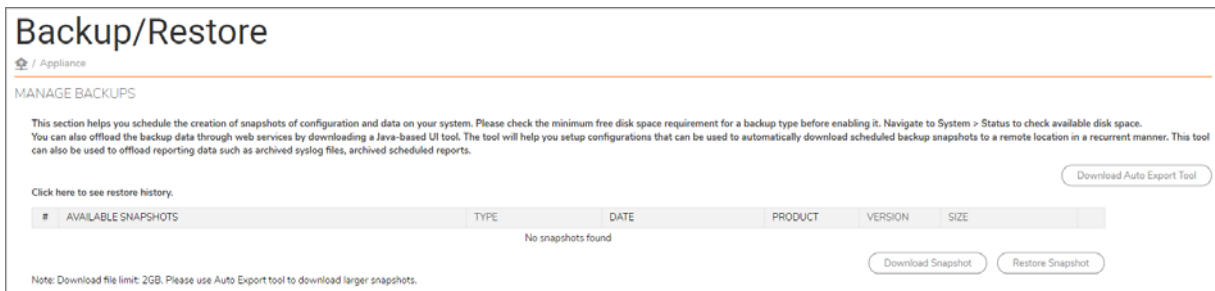
- 7 Click the plus + icon in the top right of the table to **Choose File** to upload to your selected folder. The file management dialog box displays.
- 8 In the file management dialog box, navigate to the file you would like to upload and click **Upload**.
- 9 The selected file is now displayed next to Choose File. Click **Upload** to complete the file manager import.
- 10 For managing a batch of files, select multiple files from the list and click **Export** or **Delete**.

Backup/Restore

The **System > Backup/Restore** page helps you schedule and create immediate snapshots of configuration settings and data on your system. Check the minimum free disk space requirement for a backup/restore operation before enabling it. Navigate to **System > Status** to check your available disk space.

Manage Backups

You can also offload the backup data through web services by downloading a Java-based UI tool. The tool helps you set up configurations that can be used to automatically download scheduled backup snapshots to a remote location in a reoccurring schedule. This tool can also be used to offload reporting data such as archived syslog files and archived scheduled reports.



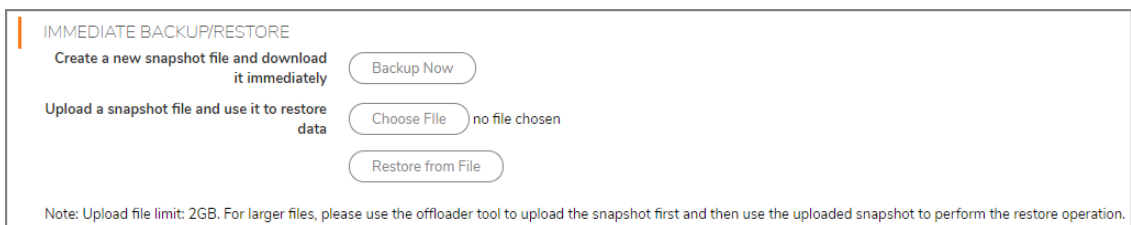
- 1 Click **Download Auto Export Tool**, under the **MANAGE BACKUPS** section, to download your compressed folder tools.
- 2 Click **Download Snapshot**, under **AVAILABLE SNAPSHOTS**, to help you download system backup files.
- 3 Click **Restore Snapshot** to restore a backup snapshot. The snapshot is uploaded to your local storage and then used to restore data.

NOTE: Download file limit: 2GB. Use the Auto Export tool to download larger snapshots.

Immediate Backup/Restore

To perform an immediate backup/restore of your system:

- 1 Under **IMMEDIATE BACKUP/RESTORE**, click **Backup Now** to **Create a new snapshot file and download it immediately**.
- 2 Click **Choose File** to **Upload a snapshot file and use it to restore data**.
- 3 Click **Restore from File**.



NOTE: Upload file limit: 2GB. For larger files, use the offloader tool to upload the snapshot first and then use the uploaded snapshot to perform the restore operation.

Scheduled Backup Settings

To schedule backing up your data:

- 1 Check the box to **Enable Basic Backups**. The files saved for a basic backup include sgmsConfig.xml, applianceConf.txt, and addUnit.xml files.

i **NOTE:** Ensure addUnit.xml files are being saved from the **Console > Management > Settings** screen.

SCHEDULED BACKUP SETTINGS

Enable Basic Backups **i**

Backup schedule Daily at 22 00

Enable Application Backups **i**

Backup schedule Weekly on Friday at 22 30

Backup schedule Monthly on 07 at 23 00

Backup snapshots to directory /opt/GMSVP/backup (This field is disabled on a SonicWall Analytics appliance)

Free disk space required 31 GB (Available: 43.49 GB)

Auto disk space management **i**

Update Settings

Note:

- * Only 1 snapshot per backup type will be saved. Old snapshots will be deleted on successful completion of backup process.
- * On enabling auto disk space management, In case of disk space shortage, the last backup file(s) that was offloaded will be deleted prior to the start of new backup run.
- * Old snapshots will not be deleted if the backup directory is changed, please delete them manually.

- 2 Select the hour and minute for your **Backup schedule** by clicking on the down arrows next to **Daily at**.
- 3 Check the box next to **Enable Application Backups**. Application backups include basic data, database, firmware images, and HM recordings on a monthly or weekly schedule.

i **NOTE:** A database backup only occurs if the deployment has the database configured to run on the system. For more information, check **Deployment > Roles**.

- 4 Select your **Backup schedule** hour and day by clicking on the down arrows next to **on** and **at**.
- 5 Select your **Backup schedule** week or month, day, hour, and minute by clicking on the down arrows next to **on** and **at**.
- 6 If enabled, input a directory name in the **Backup snapshots to directory** field. A note is shown if this option is disabled on a SonicWall Analytics appliance.
- 7 Next to **Free disk space required**, verify that you have enough space for the backup.
- 8 Check the box next to **Auto disk space management** in case of disk space shortage. The last backup file(s) that was offloaded is deleted prior to the start of the new backup run.
- 9 Click **Update Settings**.

NOTE: Only one snapshot per backup type is saved. Old snapshots are deleted on successful completion of the backup process.

On enabling auto disk space management, in case of disk space shortage, the last backup file(s) that was offloaded is deleted prior to the start of the new backup run.

Old snapshots are not deleted if the backup directory is changed. Delete them manually.

Shutdown

This section allows you to shut down or restart your system. You can temporarily disconnect users and stop services. If you made any changes to the settings, be sure to apply them before you restart or shut down. The process of restarting generally takes about three minutes.

SHUTDOWN

Warning! This action will disconnect all users.

This action takes about 3 minutes.
Remember that if you made any changes to the settings, you'll need to apply them before you restart or shutdown.

Restart Shutdown

- 1 To restart your system, click **Restart** and then click **OK** in the confirmation dialog box.
- 2 To shut down your system, click **Shutdown** and then click **OK** in the confirmation dialog box.

Network

Network is the third command on the left navigation panel for on-premises Analytics. After the Network command is expanded, you see its sub-commands, which are listed below. The sub-commands allow the administrator to configure Network-related settings.

- [Settings](#)
- [Routes](#)

Settings

The **Network > Settings** page provides network settings configuration procedures for **HOST**, **NETWORKING**, **IPV4 SETTINGS**, and **SEARCH SUFFIXES**.

Settings
Appliance

HOST

Name: example: hostname
Domain: example: domain.com

NETWORKING

Select IP type: DHCP Static

IPV4 SETTINGS

Host IP Address:
Subnet Mask:
Default Gateway:
DNS Server 1:
DNS Server 2:
DNS Server 3:

SEARCH SUFFIXES

Host Settings

To configure host settings:

- 1 Enter the host **Name** in the text field provided.
- 2 Enter the host **Domain** name in the text field provided.
- 3 Click **Update** to apply the host and networking settings changes.
- 4 Click **Reset** to restore these settings to previous saved values.

Networking Settings

To configure networking settings:

- 1 **Select IP type** by clicking the radio button next to **DHCP** or **Static**.
- 2 Click **Update** to apply the host and networking settings changes.
- 3 Click **Reset** to restore these settings to factory defaults.

IPV4 Settings

To configure IPV4 settings:

- 1 Enter the **Host IP Address**, **Subnet Mask**, **Default Gateway**, and optionally enter **DNS Server 1, 2 and 3 IP** addresses.
- 2 Click **Update** to apply the host and networking settings changes.
- 3 Click **Reset** to restore these settings to factory defaults.

Search Suffixes

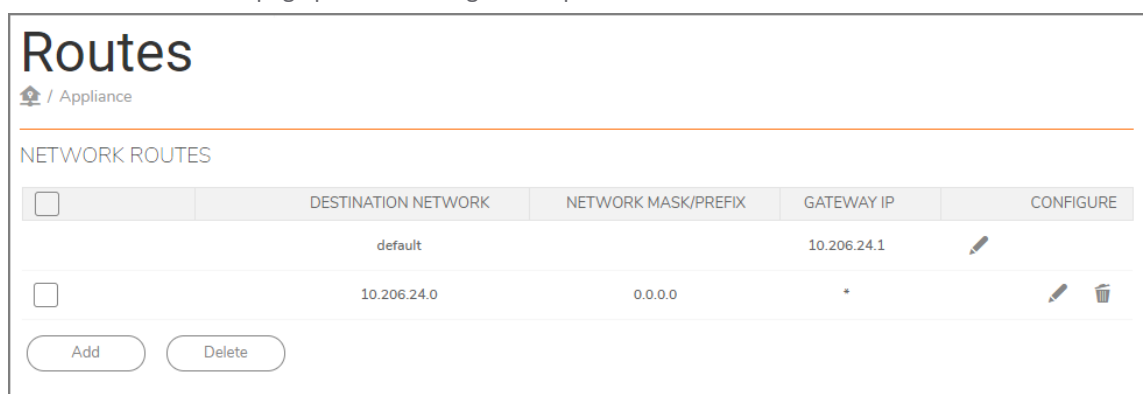
Search Suffixes lets you automatically append a DNS suffix. For example, when you ping “sonicwall” it automatically goes to “sonicwall.engineering.”

To configure Search Suffixes:

- 1 Click **Add** to include multiple search suffixes.
- 2 Check the box next to the **Search Suffixes** list to remove search Suffixes.
- 3 Click **Delete**.

Routes

The **Network > Routes** page provides configuration procedures to add network routes.



The screenshot shows the 'Routes' configuration page. At the top, there is a breadcrumb 'Appliance' and the title 'Routes'. Below this is a section titled 'NETWORK ROUTES' containing a table with the following columns: a checkbox, 'DESTINATION NETWORK', 'NETWORK MASK/PREFIX', 'GATEWAY IP', and 'CONFIGURE'. The table has two rows: the first row has a checked checkbox, 'default', an empty field, '10.206.24.1', and a pencil icon; the second row has an unchecked checkbox, '10.206.24.0', '0.0.0.0', an empty field, and pencil and trash icons. Below the table are 'Add' and 'Delete' buttons.

To add a network route:

- 1 In the **NETWORK ROUTES** table, click **Add**.



The screenshot shows the 'ADD ROUTE' form. It has three input fields: 'Destination Network', 'Network Mask/Prefix length', and 'Gateway Address'. At the bottom, there are 'Add' and 'Cancel' buttons.

- 2 Enter a **DESTINATION NETWORK** IP address,.
- 3 Enter the **NETWORK MASK/PREFIX**.
- 4 Enter the **GATEWAY** address.
- 5 Click **Add**.
- 6 Click **Cancel** to null your choice.

- 7 To edit the default network route, click the **Edit** icon under the **CONFIGURE** column.
- 8 When multiple network routes are added to the list, selecting the check box at the top left of the page selects all the added network routes.
- 9 Click **Delete** to remove a network route from the list.

 **NOTE:** The default network route cannot be deleted.

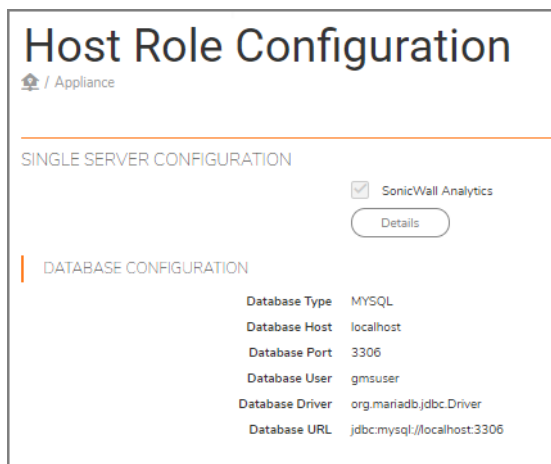
Deployment

Use the **Deployment** command to set various deployment features

- [Roles](#) (for Syslog-based reporting only)
- [Settings](#)
- [Services](#)

Roles

The **Deployment > Roles** page is divided into two sections: **SINGLE SERVER CONFIGURATION** and **DATABASE CONFIGURATION**.



 **NOTE:** The **Roles** option is only available on the Syslog-based Analytics.

Click **Details** to see the **ROLE DETAILS FOR SONICWALL ANALYTICS**, which represents a deployment where all services run on a single server, including the database.

ROLE DETAILS FOR SONICWALL ANALYTICS

The "SonicWall Analytics" represents a deployment where all services run on a single server, including the Database.

Following services run on an "SonicWall Analytics" system:

- SonicWall Universal Management Suite - Database
- SonicWall Universal Management Suite - Reports Database II
- SonicWall Universal Management Suite - Reports Scheduler
- SonicWall Universal Management Suite - Reports Summarizer
- SonicWall Universal Management Suite - Syslog Collector
- SonicWall Universal Management Suite - Web Server

Close

Click **Close** when finished.

The **DATABASE CONFIGURATION** section provides details of the configuration.

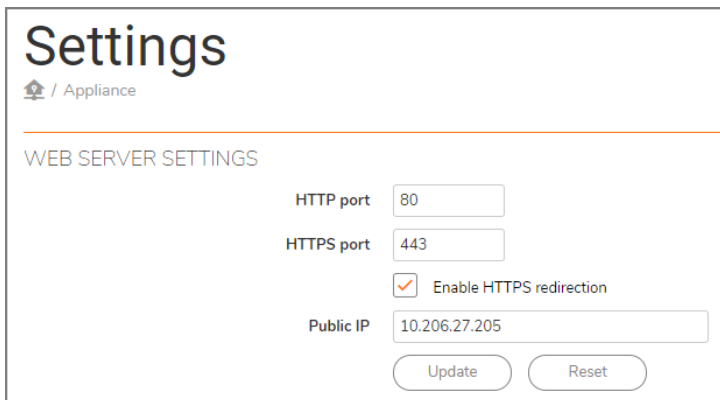
Settings

The **Deployment > Settings** page is divided into three sections: **WEB SERVER SETTINGS**, **SMTP CONFIGURATION**, and **SSL ACCESS CONFIGURATION**.

Configuring Web Server Settings

- 1 Enter the **HTTP port** number in the text field provided. The default port is **80**.
If you enter another port in this field, the port number must be specified when accessing the appliance management interface. For example, if port 8080 is entered, the appliance management interface would be accessed with the URL: `http://<IPAddress>:8080/appliance/`.
- 2 Enter the **HTTPS port** number in the text field provided. 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. For example, if port 4430 is entered, the appliance management interface would be accessed with the URL: `https://<IPAddress>4430/appliance/`.
- 3 Check the box next to **Enable HTTPS redirection** to redirect HTTP to HTTPS when accessing the firewall interface.
- 4 Enter the **Public IP address** in the text field provided.
- 5 Click **Update** when you are finished configuring the web server settings.

- 6 Click **Reset** to refresh your settings.

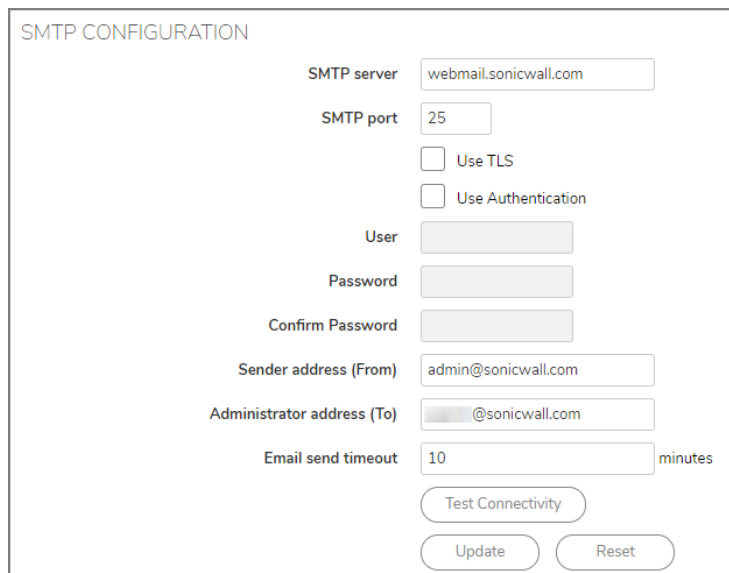


The screenshot shows the 'Settings' page for an appliance. The breadcrumb is 'Home / Appliance'. The section is titled 'WEB SERVER SETTINGS'. It contains the following fields and controls:

- HTTP port: 80
- HTTPS port: 443
- Enable HTTPS redirection:
- Public IP: 10.206.27.205
- Buttons: Update, Reset

Configuring SMTP Settings

The **SMTP CONFIGURATION** section allows you to configure an SMTP server, an SMTP port, a sender email address, and an administrator email address. You can also test connectivity to the configured server.



The screenshot shows the 'SMTP CONFIGURATION' page with the following fields and controls:

- SMTP server: webmail.sonicwall.com
- SMTP port: 25
- Use TLS:
- Use Authentication:
- User: [Empty field]
- Password: [Empty field]
- Confirm Password: [Empty field]
- Sender address (From): admin@sonicwall.com
- Administrator address (To): [Empty field] @sonicwall.com
- Email send timeout: 10 minutes
- Buttons: Test Connectivity, Update, Reset

To configure the SMTP settings:

- 1 Type the FQDN or IP address of the **SMTP server**.
- 2 Type the **SMTP port** in the text field provided. The default is **25**.
- 3 Check the box next to **Use TLS** if you would like to use Transport Layer Security (TLS) for your mail server connectivity.
- 4 If you want the SMTP server in your deployment to require authentication, enable the **Use Authentication** check box. This option is necessary to properly send all outgoing emails to the intended recipients.
- 5 Enter the **User** name for authentication in the text field provided.
- 6 Enter the **Password** for authentication in the text field provided.
- 7 **Confirm Password** in the text field provided.

- 8 Type the email address from which mail is sent into the **Sender address (From)** field.
- 9 Type the email address of the system administrator into the **Administrator address (To)** field.
- 10 Enter the number of minutes in the **Email send timeout** field. The default is 10 minutes.
- 11 To test connectivity to the SMTP server, click **Test Connectivity**.
- 12 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 SonicWall Analytics, or select the default local keystore.

To configure SSL access:

- 1 Select **Default** to keep, or revert to, the default settings.

This selection allows you to keep the default certificate that comes with the application for use by the SonicWall Analytics Web Server for SSL access. Filename for the keystore used is **gmssvpsrver**.

- 2 Select **Custom** to upload a custom keystore certificate for SSL access.

This selection allows you to upload a customer certificate for use by the SonicWall Analytics Web Server for SSL access. The original filename of the certificate imported is replaced with **gmssvpsrvercustom** in the local file system.

NOTE: The upload can be performed on either of the following ways:

- Directly as a certificate: the certificate file (.crt/.cer), its corresponding key file (.key) and the password are required.
- Using a keystore: The keystore and the store password are required, which would be converted and stored as a certificate.

- 3 Under **CERTIFICATE UPLOAD** section,click **Choose File** to select your **Certificate file**.

CERTIFICATE UPLOAD

Certificate file No file chosen

Certificate Key file No file chosen

Certificate password

- 4 Click **Choose File** to select your **Certificate Key file**.
- 5 Type the password for the certificate file into the **Certificate password** field.
- 6 Click **View** to display details about your keystore certificate.
- 7 Click **Update** to submit your changes.

Services

The **Deployment > Services** page provides a list of the services that are running on your system and their current state. It also provides a way to stop or start any of the services.

<input type="checkbox"/>	SERVICE NAME	ADMIN SERVICE STATE
<input type="checkbox"/>	SonicWall Universal Management Suite - Flow TP Client	Started (Enabled)
<input type="checkbox"/>	SonicWall Universal Management Suite - Reports Scheduler	Started (Enabled)
<input type="checkbox"/>	SonicWall Universal Management Suite - Flow API	Started (Enabled)
<input type="checkbox"/>	SonicWall Universal Management Suite - Flow Summarizer	Started (Enabled)
<input type="checkbox"/>	SonicWall Universal Management Suite - Flow Alert Notification	Started (Enabled)

Click **Details** to see the role details for Analytics. To manage a the Host Services, select a service and click **Disable**, **Enable**, or **Restart**.

Flow Agent

The **Flow Agent** option is only visible for IPFIX-based Analytics. The flow agent collects data pertaining to applications and transactions in the network infrastructure. It helps give greater visibility to application traffic utilization and performance.

The **Flow Agent** option at **CONSOLE > Appliance > Appliance > Flow Agent** is the same information displayed at **CONSOLE > Flow Agent**. This allows you to view flow agent information when in either Appliance mode or **CONSOLE** mode. For more details about IPM, refer to [Flow Agent](#).

IPM

Intelligent Platform Management (IPM) monitors the performance of system resources like CPU, RAM, and disk space. The **IPM** option at **CONSOLE > Appliance > Appliance > IPM** is the same information displayed at **CONSOLE > IPM**. This allows you to view IPM information when in either Appliance mode or **CONSOLE** mode. For more details about IPM, refer to [IPM](#)

Diagnostics

This chapter describes the **Debug Log Settings** and **Summarizer Status** that Analytics **CONSOLE** provides for diagnostics.

Topics:

- [Debug Log Settings](#)
- [Summarizer Status](#)

Debug Log Settings

The **Diagnostics > Debug Log Settings** page allows you to set debug levels for faster troubleshooting of potential application issues. This action creates debug log files in a single-server deployment. The system has log rotation so the disk does not fill up. Because of the potential performance degradation, you should only set a debug level based on guidance from SonicWall Customer Support. When done debugging, you should reset the debug log settings back to **No Debug** as soon as the potential issue has been resolved.

NOTE: The higher the debug level, more the system resources are used to generate debug data causing lower the overall system performance.

IMPORTANT: The Debug Log Settings are intended for use only under the direction of SonicWall Customer Support.

To set the debug level when instructed by SonicWall Technical Support:

- 1 Navigate to **CONSOLE | Diagnostics > Debug Log Settings**.

Debug Log Settings
LocalDomain

Debug Log Settings Updated Successfully

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 will be used up to generate debug data and in turn lower the overall system performance.

System Debug Level: No Debug Reset

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

2 Select one of the following from the **System Debug Level** drop-down list:

- **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.

3 Click **Update** to make your changes.

4 Click **Reset** to start again.

Be sure to reset the level to No Debug for normal operation as soon as the potential issue has been resolved.

Summarizer Status

The Summarizer Status option is only available on Syslog-based Analytics.

The **Diagnostics > Summarizer Status** page allows you to see your activity for the past seven days:

The screenshot displays the 'Summarizer Status' page for 'LocalDomain'. It features a 'SUMMARIZER UTILIZATION' section with a gauge chart showing 1% utilization for IP 10.206.23.84. Below this is a table with columns for Summarizer, Reporting Database Size, Raw Data Directory Size, Estimated Cache Size, Backup Directory Size, and Status. The table shows 0 GB of 61.9 GB for the reporting database, 0.02 GB of 61.9 GB for raw data, and 20 GB of 61.9 GB for the estimated cache. The deployment status is 'OK'. A note at the bottom states: 'Please visit the GMS web site for more information on how to manage your deployment. Note: The average load and estimated capacity are specific to the deployment and could vary across systems.' There are also expandable sections for 'Details For Summarizer At 10.206.23.84' and 'Syslogs sent by appliances that are not under Reporting and Management'.

SUMMARIZER	REPORTING DATABASE SIZE	RAW DATA DIRECTORY SIZE	ESTIMATED CACHE SIZE	BACKUP DIRECTORY SIZE	STATUS
10.206.23.84	0 GB of 61.9 GB	0.02 GB of 61.9 GB	20 GB of 61.9 GB	0 GB	OK

NOTE: The average load and estimated capacity are specific to the deployment and could vary across systems.

Sections of the **Summarizer Status** page can be expanded to see more information:

- [Summarizer Details](#)
- [Syslogs Details](#)

Summarizer Details

Click the down arrow next to **Details for Summarizer**. Several other section are also expanded and show related information:

- SUMMARIZER UTILIZATION
- DATA FILE INFORMATION
- SUMMARIZER PROCESS DETAILS
- OPTIMIZATION INFORMATION

▼ Details For Summarizer At 10.206.23.84

▼ SUMMARIZER UTILIZATION

Average Summarizer Utilization	1%
Peak Summarizer Utilization	1%
Average Run Time Per Day:	0h:0m:11s
Average Syslog Summarized (million/day)	0.08
Average Syslog Summarized Per Minute	408,923.62

▼ DATA FILE INFORMATION

DATA FILE TYPE	FILE STATS	OLDEST
Reporting Database	0 MB	
Backup Files	0 MB	
Unprocessed Files	0 Files - 0 MB	
Archived Files	24 Files - 23.47 MB	Tue Sep 10 00:07:28 GMT 2019
Invalid Log Files	0 Files - 0 MB	

▼ SUMMARIZER PROCESS DETAILS

Summarizer is idle.

Last Run Time: 09/27/2019 18:52:34
Next Run Time: 09/27/2019 19:07:34

▼ OPTIMIZATION INFORMATION

Optimization State Queued up

Pending Optimization Sep 26, 2019

Total Un-optimized days 14

Syslogs Details

Click the down arrow next to Syslogs sent by appliances that are under Reporting and Management to see more information. The two subsections are:

- SERIAL # OF APPLIANCES FOR SUMMARIZER AT <IP ADDRESS>
- SERIAL # OF APPLIANCES THAT ARE MISCONFIGURED

i **NOTE:** 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 serial numbers, log in to the appliance and change the GMS settings. The serial numbers are listed in the settings and are updated every 12 hours.

▼ Syslogs sent by appliances that are not under Reporting and Management
▼ SERIAL # OF APPLIANCES FOR SUMMARIZER AT 10.206.23.84
None
▼ SERIAL # OF APPLIANCES THAT ARE MISCONFIGURED
None
Note: * Login to the appliance and disable the syslogs * If you dont have access to the appliance use the rules to the gateway to block the serials * To Fix the misconfigured serials, login to the appliance and change the GMS Settings * The serials listed here refresh every 12 hours

3rd Party

The **3rd Party** command option is available only for IPFIX-based Analytics. The **3rd Party** command provides the means for new API keys and managing the key assignments.

Key Assignments

The default view is the **Key Assignments** tab. All key assignments are listed here along with time of creation, time to live and the actual key. You can select any key or set of key and delete them.

API Keys

/ LocalDomain

Key Assignments Generate New Key

KEY ASSIGNMENTS

	USER NAME	TIME OF CREATION	TIME TO LIVE	KEY
No Entries Found				

Delete Selected

Generating a New Key

To generate a new key:

- 1 Navigate to **CONSOLE > 3rd Party > API Keys**.
- 2 Select the **Generate New Key** tab.

API Keys

/ LocalDomain

Key Assignments Generate New Key

GENERATE NEW KEY

Username

TTL days

Update

- 3 Type **Username** in the field provided.

- 4 In the **TTL** (Time to Live) field, enter the number of days you want the key to be active.
- 5 Click **Update**.

Flow Agent

The **Flow Agent** option is only visible for IPFIX-based Analytics. The flow agent collects data pertaining to applications and transactions in the network infrastructure. It helps give greater visibility to application traffic utilization and performance.

The **Flow Agent** option at **CONSOLE > Flow Agent** is the same information displayed at **CONSOLE > Appliance > Appliance > Flow Agent**. This allows you to view flow agent information when in either Appliance mode or **CONSOLE** mode.

Topics:

- [Devices](#)
- [Statistics](#)
- [Usage](#)
- [Monitor](#)
- [Process Monitor](#)
- [Log](#)
- [Settings](#)

Devices

Navigate to **CONSOLE > Flow Agent > Devices** to see a list of all the devices that are being monitored by IPFIX-based Analytics. The top of the table shows some basic statistics like **AppFlow Server Uptime**, **System Uptime** and **Last Update**.

The Devices table provides many different details about each device listed. The Device table can be searched to find a specific device and it can be refreshed to update the data in the table.

Devices

LocalDomain

DEVICES

Search AppFlow Server Uptime: 0 days 3 hours 41 mins 5 secs System Uptime: 0 days 3 hours 41 mins 51 secs Last Update: 20:38:01 Dec 01

	DEVICE NAME	SERIAL NUMBER	IP ADDRESS	MAX FLOWS/ FILE	FLOW FILE COUNT	TOTAL FLOWS	REPORT FILE COUNT	RTR FILE COUNT	FLOW DB SIZE	FLOW PACKET RATE	FLOW RECORD RATE	STATS	ACTIONS
1	RG	XXXXXXXXXXXX	10.1.1.1	200,000	11	2,200,000	27	2	419.62MB	61	64		
	TOTAL				11	2,200,000	27	2	419.62MB	61	64		

Refresh

Statistics

The **Statistics** page, found at **CONSOLE > Flow Agent > Statistics**, is a list of different kind of statistics collected on various parameters.

Statistics

LocalDomain

System IPFIX Template

NAME	VALUE
Packets Processed	704357
Packets Processed from data	0
Packets Processed from sec	0
Packets Processed from sec1	0
Packets Processed from sec2	0
IPFIX Packets Count	704357
Mirror Packets Count	0
Template Records Processed	0
Data Records Processed	0
Mirror Records Processed	0

Last Updated: 02-Dec-2019 04:44:19

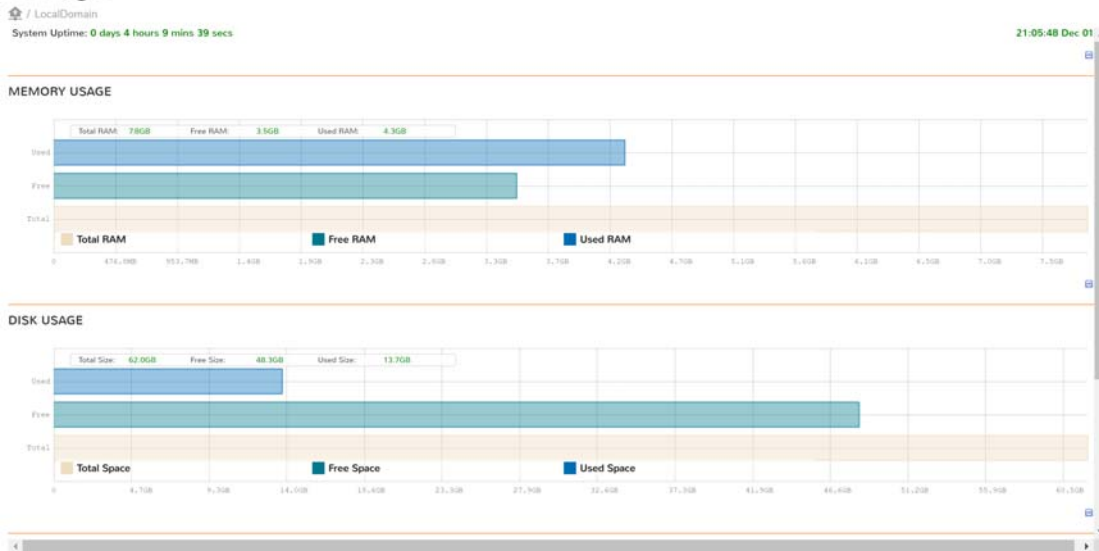
Choose from the tabs across the top to see different types of statistics: **System**, **IPFIX**, or **Template**.

Usage

The **Usage** page shows the statistics for the key system resources: **Memory Usage**, **Disk Usage**, and **DB (Database) Size**. For memory and disk usage, used space, free space and total space are displayed in a bar chart. Current size and maximum are shown for database size.

The charts on this page can be minimized by clicking on the blue minus icon on the upper right corner of each chart. Click the blue plus icon to expand the chart.

Usage



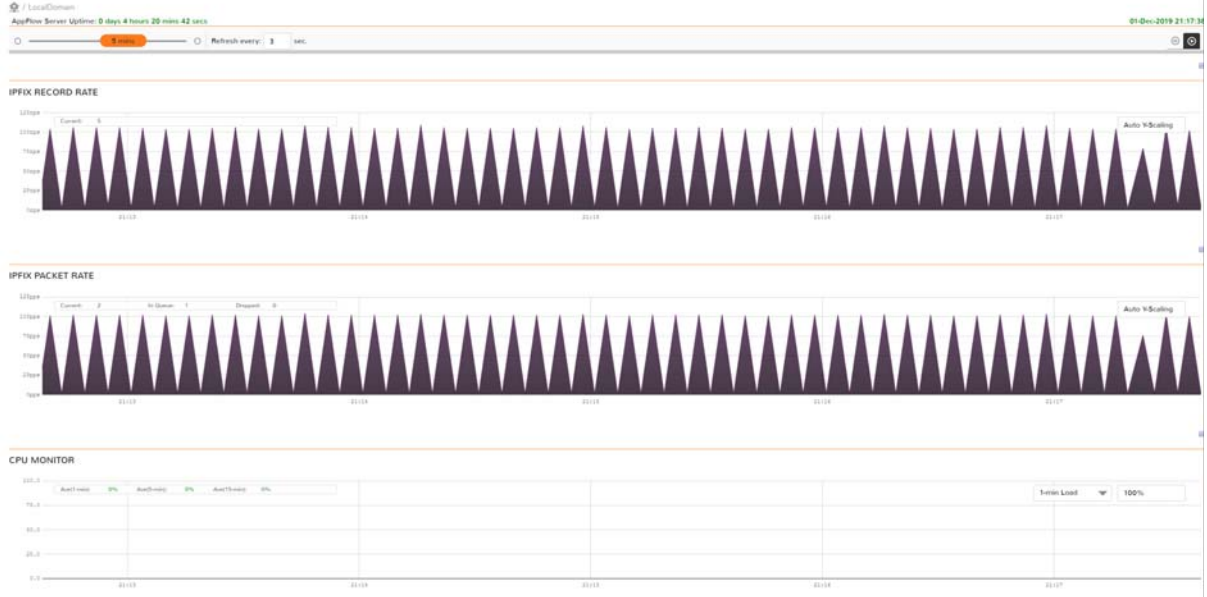
Monitor

The **Monitor** page shows the statistics for IPFIX and the CPU. At the top of the table, you can set the frequency of the monitoring. The preset time periods range from 60 second to 10 minutes. You can also designate how frequently the data refreshes, in seconds. The three data types being monitored include:

- IPFIX RECORD RATE
- IPFIX PACKET RATE
- CPU MONITOR

The charts on this page can be minimized by clicking on the blue minus icon on the upper right corner of each chart. Click the blue plus icon to expand the chart.

Monitor



Process Monitor

Navigate to **CONSOLE > Flow Agent > Process Monitor** to see the page that shows the list of processes being monitored. It also shows the process status. At any time, you can click the **Refresh** button to update the process status.

Process Monitor

LocalDomain

PROCESSES

	PROCESS NAME	PROCESS STATUS
1	MON IPC Thread	Active
2	MON HB TCP Thread	Active
3	User-ip Thread	Active
4	User IPC Thread	Active
5	User TCP Thread	Active
6	Network IPC Thread	Active
7	Network TCP Thread	Active
8	Archive IPC Thread	Active
9	Archive TCP Thread	Active
10	Sysmon IPC Thread	Active
11	Sysmon TCP Thread	Active

Refresh

IPM

Intelligent Platform Management (IPM) monitors the performance of system resources like CPU, RAM, and disk space.

Topics:

- [Settings](#)
- [Monitor](#)
- [History](#)

Settings

The **IPM > Settings** page lets you set the **THRESHOLD SETTINGS** for the following:

- [CPU/Processor](#)
- [Memory/RAM](#)
- [Storage/Disk](#)
- [Estimated Capacity](#)
- [Capacity Estimation Settings](#)

For most settings you can set a medium severity and a high severity for each threshold. (Click **Apply** or **Reset** for each change you make.) For the capacity estimation settings you can **Enforce Disk Capacity Estimation** by checking the box and applying the setting.

Settings

LocalDomain

THRESHOLD SETTINGS

CPU/PROCESSOR

Severity: Medium
 60 80 **70%**

Severity: High
 85 95 **90%**

MEMORY/RAM

Severity: Medium
 60 80 **75%**

Severity: High
 85 95 **90%**

STORAGE/DISK

Severity: Medium
 50 75 **65%**

Severity: High
 80 95 **85%**

ESTIMATED CAPACITY

Severity: Medium
 50 75 **65%**

Severity: High
 80 95 **85%**

CAPACITY ESTIMATION SETTINGS

Enforce Disk Capacity Estimation

CPU/Processor

To set the CPU/Processor setting:

- 1 Move the slider icon between 60 and 80% of severity level to set your **Medium** preference.
- 2 Click **Apply** or **Reset**. Your choice is shown next to the **Reset** button.
- 3 Move the slider icon between 85 and 95% of severity level to set your **High** preference.
- 4 Click **Apply** or **Reset**. Your choice is shown next to the **Reset** button.

Memory/RAM

To set the Memory/RAM setting:

- 1 Move the slider icon between 60 and 80% of severity level to set your **Medium** preference.
- 2 Click **Apply** or **Reset**. Your choice is shown next to the **Reset** button.
- 3 Move the slider icon between 85 and 95% of severity level to set your **High** preference.
- 4 Click **Apply** or **Reset**. Your choice is shown next to the **Reset** button.

Storage/Disk

To set the Storage/Disk setting:

- 1 Move the slider icon between 50 and 75% of severity level to set your **Medium** preference.
- 2 Click **Apply** or **Reset**. Your choice is shown next to the **Reset** button.
- 3 Move the slider icon between 80 and 95% of severity level to set your **High** preference.
- 4 Click **Apply** or **Reset**. Your choice is shown next to the **Reset** button.

Estimated Capacity

To set the Estimated Capacity setting:

- 1 Move the slider icon between 50 and 75% of severity level to set your **Medium** preference.
- 2 Click **Apply** or **Reset**. Your choice is shown next to the **Reset** button.
- 3 Move the slider icon between 80 and 95% of severity level to set your **High** preference.
- 4 Click **Apply** or **Reset**. Your choice is shown next to the **Reset** button.

Capacity Estimation Settings

- 1 Click the box next to Enforce Disk Capacity Estimation for your configuration.
- 2 Click **Apply** when done.

Monitor

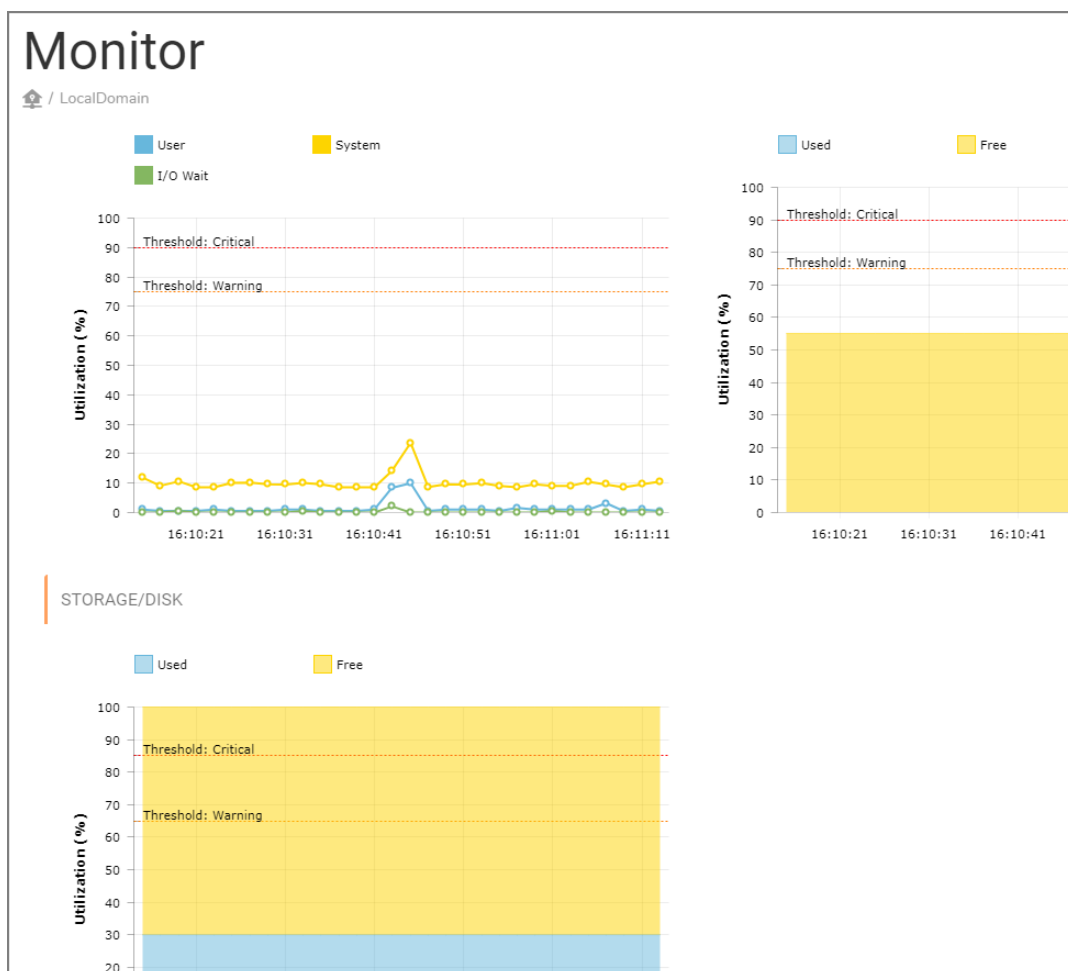
The **IPM > Monitor** page gives you the **SYSTEM RESOURCE REAL-TIME MONITOR** table which features real-time interactive line charts for **CPU/PROCESSOR**, **MEMORY/RAM**, and **STORAGE/DISK**. Use the charts to get important data for each system component being monitored. All three charts have two upper-control level lines starting at 75% of utilization for **Warning** and 90% of utilization for **Critical** thresholds.

To use the CPU/Processor chart:

- 1 Hover over the chart to select the data you want to plot.
- 2 The chart distributes the category data (a 10-second time interval) along a horizontal axis and the numerical percentage **Utilization (%)** value data along a vertical axis.
- 3 Select the blue line on the chart to see the **User** data.
- 4 Select the green line on the chart to see the **I/O Wait** data.
- 5 Select the yellow line on the chart to see the **System** data.

To use the Memory/RAM and Storage Disk charts:

- 1 Hover over the charts to select the data you want to plot.
- 2 The chart distributes the category data (a 10-second time interval) along a horizontal axis and the numerical percentage **Utilization (%)** value data along a vertical axis.
- 3 Select the blue horizontal bars on the chart to see the **Used** data.
- 4 Select the yellow horizontal bars on the chart to see the **Free** data.



History

The **IPM > History** page gives you the **HISTORICAL DATA VIEW** of your **CPU/PROCESSOR** and **MEMORY/RAM**. You can see the data time period by choosing the **PAST 24 HRS**, **PAST 3 DAYS**, and **PAST 5 DAYS** from the drop-down menu.

The CPU/Processor and Memory/RAM data is displayed in two real-time interactive line and bar charts, respectively. Use the charts to get important data for each system component being monitored. Both charts have two upper-control level lines starting at 75% of utilization for **Warning** and 90% of utilization for **Critical** thresholds.

To use the CPU/Processor chart:

- 1 Hover over the chart to select the data you want to plot.
- 2 The chart distributes the category data (a three-hour time interval) along a horizontal axis and the numerical percentage **Utilization (%)** value data along a vertical axis.
- 3 Select the blue line on the chart to see the **User** data.
- 4 Select the green line on the chart to see the **I/O Wait** data.
- 5 Select the yellow line on the chart to see the **System** data.

To use the Memory/RAM chart:

- 1 Hover over the charts to select the data you want to plot.
- 2 The chart distributes the category data (a three-hour time interval) along a horizontal axis and the numerical percentage **Utilization (%)** value data along a vertical axis.
- 3 Select the blue horizontal bars on the chart to see the **Used** data.
- 4 Select the yellow horizontal bars on the chart to see the **Free** data.



Notifications

The **Notifications** option is only visible for IPFIX-based Analytics. These settings define the parameters for the alerts and notifications. Navigate to **CONSOLE > Notifications > Settings** to see the options.

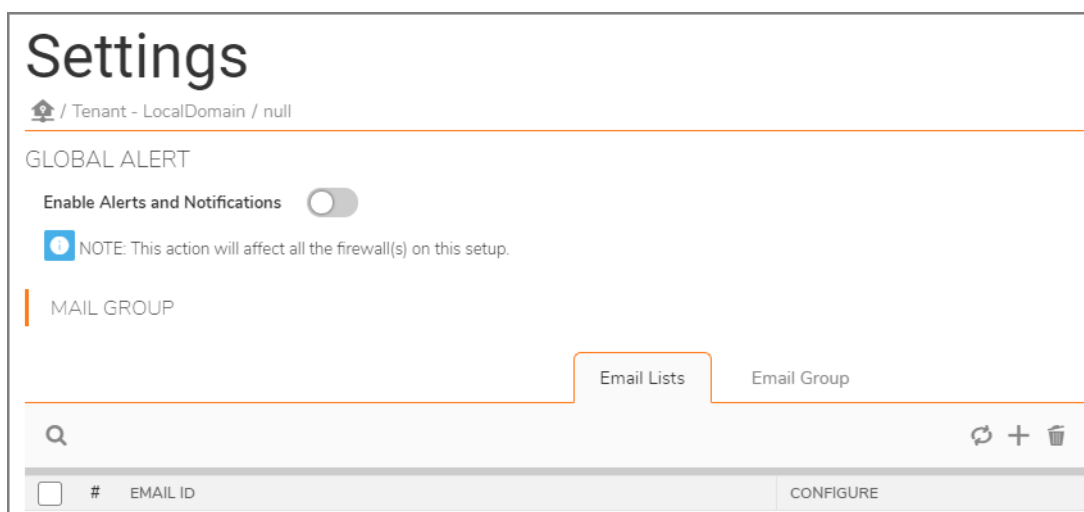
The **Settings** view is broken into the following sections:

- [Global Alert](#)
- [Mail Group](#)

Global Alert

To enable or disable Alerts and Notifications:

- 1 Go to **Notifications > Settings**.

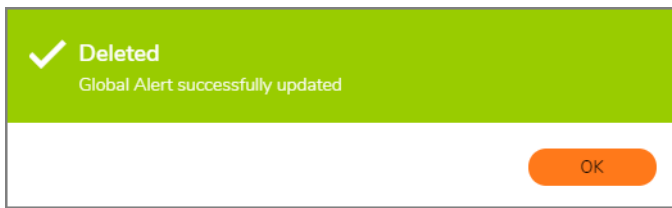


- 2 Toggle **Enable Alerts and Notifications**. A green switch indicates that the option is enabled. The gray switch indicates that the option is disabled.

NOTE: By default, the **Enable Alerts and Notifications** switch is enabled.

NOTE: This action affects all the firewalls on this setup.

- 3 Click **OK** to acknowledge the message that the Global Alert has been changed.

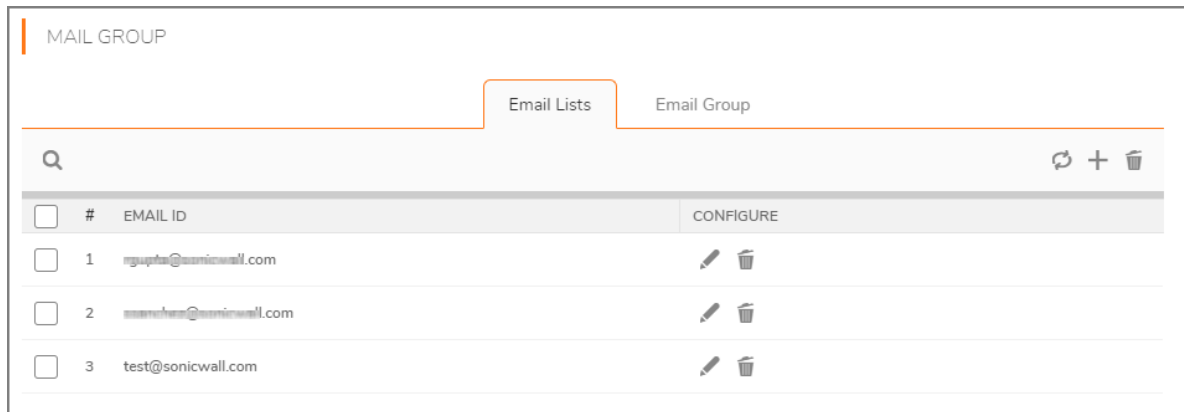


Mail Group

MAIL GROUP settings are configured by administrators to set the email parameters so your network infrastructure can send email reports, alarm notifications, and so on.

There are two tabs to work with in the **MAIL GROUP** table:

- **Email Lists**
- **Email Group.**



Configuring Email

You can configure your **Email Lists** settings by working with the **EMAIL ID** and **CONFIGURE** columns in the **Email Lists** tab. You can use the **Edit** and **Delete** icons for your email addresses.

Email Lists Options

Option	Description
Search Emails	Allows you to look for specific email addresses you have added to create your alerts.
Refresh Emails	Allows you to update your email address list.
Add Email	Allows you to add an email address using email ID settings.
Delete Email	Allows you to delete one or many email addresses listed in the Email ID column.

Editing Email Lists

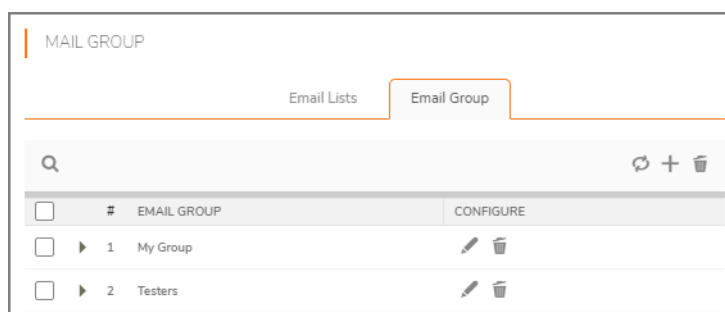
- 1 Click the check boxes next the **EMAIL ID** you want to edit.
- 2 Click the **Edit** icon to access the **EMAIL ID SETTINGS** dialog box.
- 3 Modify the **Previous Email Id** by entering a new email address in the **Changed Email Id** text field.
- 4 Click **Next**.
- 5 Check that the correct email address is displayed under the **SUMMARY** text field next to **Email Group Name** and then click **Create**.
- 6 Click **Close** after you have successfully changed the email address.

Deleting Email Lists

- 1 Click one or more of the check boxes under the **EMAIL ID** column to indicate the email addresses you want to delete.
- 2 Click the **Delete** icon.
- 3 Click **OK** in the dialog box to confirm your deletion.
- 4 Click **OK** in the confirmation message to finish deleting the email address.

Configuring an Email Group

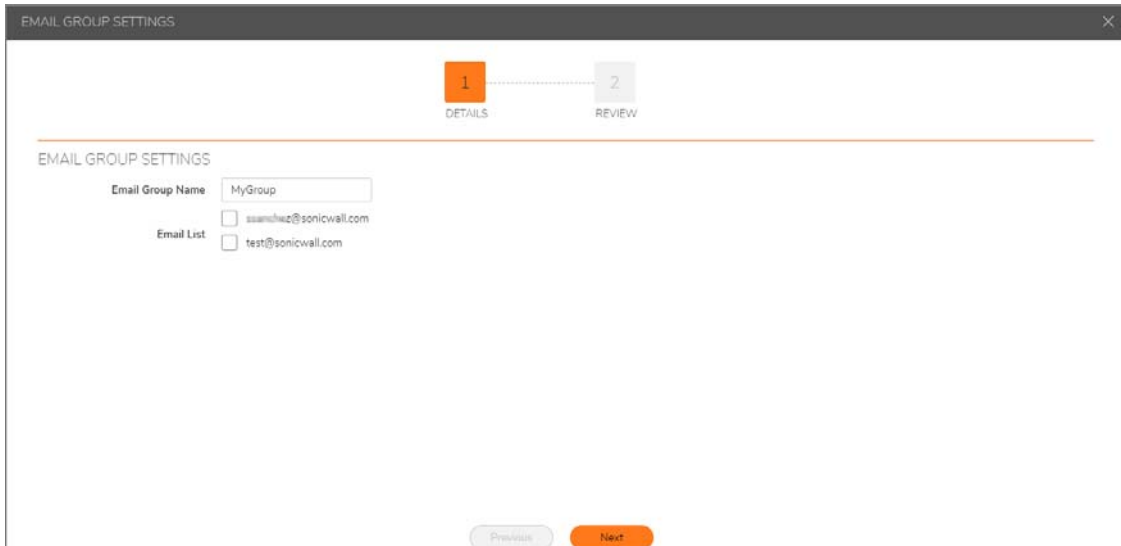
The view under the **Email Group** tab is different than the view under the **Email Lists** tab. You can configure your **Email Group** settings by working with the **EMAIL GROUP** and **CONFIGURE** columns in the **Email Group** tab. You can use the **Edit** and **Delete** icons to configure your email addresses.



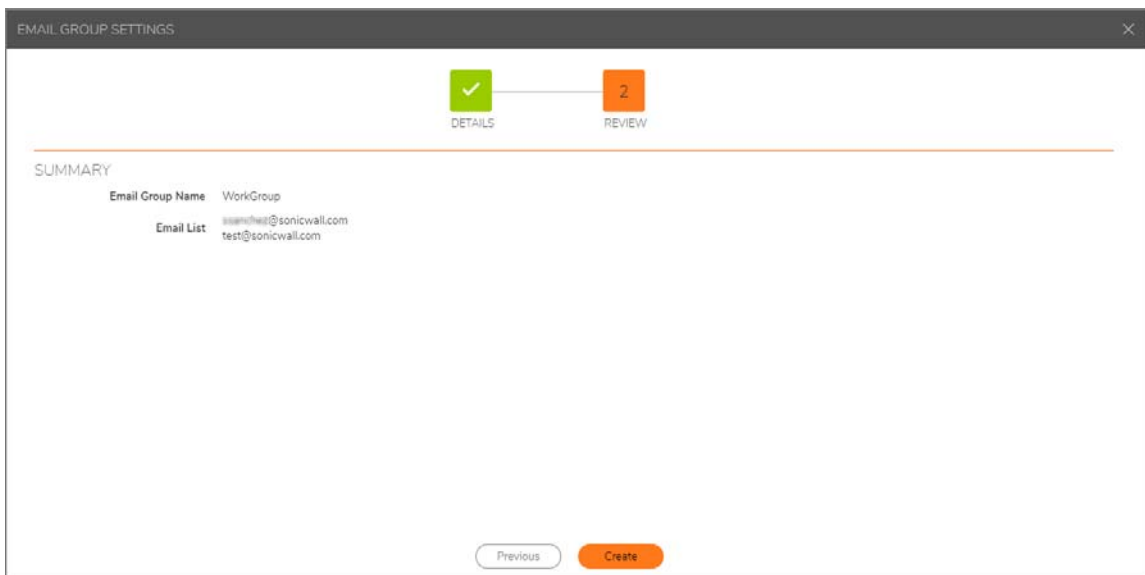
Adding an Email Group

To add an Email Group:

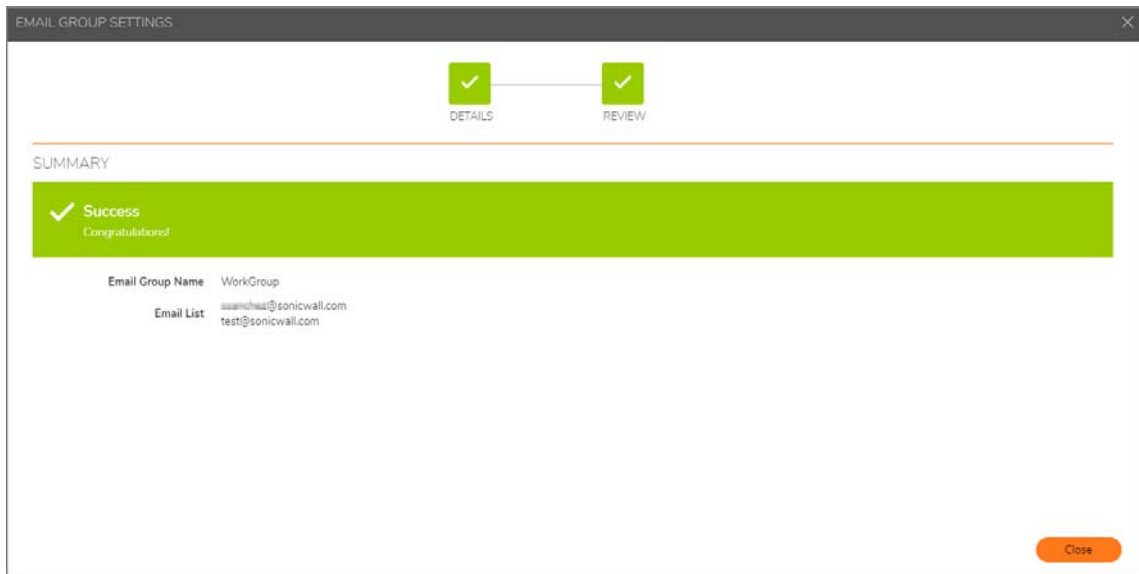
- 1 Click the **Email Group** tab.
- 2 Click the **+** icon at the top right of the **Mail Group** table.



- 3 In the **EMAIL GROUP SETTINGS** dialog screen, type the **Email Group Name** for your email group.
- 4 Check the boxes next to the email addresses that you want included in your email group.
- 5 Click **Next**.



- 6 Review your settings in the **SUMMARY** section.
- 7 Click **Create** to proceed or **Previous** to adjust your settings.



- 8 Click **Close** after you have successfully created your email group.

Editing an Email Group

- 1 Click the **Email Group** tab.
- 2 Click the check box next the email group, under the **EMAIL GROUP** column, to indicate the email address of the group you want to edit.
- 3 Click the **Edit** icon to access the **EMAIL GROUP SETTINGS** dialog box. The **EMAIL GROUP SETTINGS** dialog displays.
- 4 Edit or enter a new **Email Group Name** for your group of email addresses.
- 5 Optionally, check the boxes of the email addresses you want to include or exclude in the group.
- 6 Click **Next**.
- 7 Check that the correct name for the group of email addresses is displayed under the **SUMMARY** text field next to **Email Group Name**.
- 8 Click **Create**.
- 9 Click **Close** after you have successfully changed the name of the group for your email addresses.

Deleting an Email Group

- 1 Click the **Email Group** tab.
- 2 Click one or more of the check boxes, under the **EMAIL GROUP** column, to indicate the groups of email addresses you want to delete.
- 3 Click the **Delete** icon.
- 4 Click **OK** in the dialog box that displays to confirm your deletion.
- 5 Click **OK** in the dialog box that displays to finish deleting the name for your group of email addresses.

Log

Logs help track activities in the system. These activities are associated, either directly or indirectly, with user-initiated actions or based on system-initiated actions. These logs are important support for audit trails and compliance purposes, as well as for troubleshooting system operation.

Topics:

- [Configuration](#)
- [View Log](#)

Configuration

The **Log > Configuration** page lets you manually delete logs that no longer need to be stored in the system. This is a one-time action and is executed based on the date selected for deletion.

DELETE SONICWALL ANALYTICS LOG MESSAGES

Logs help track activities in this system. These activities are associated either directly or indirectly to user initiated actions, or based on system initiated actions. These logs are important for audit trailing and compliance purposes, as well as for troubleshooting system operation.

Logs, that no longer require to be stored in the system can be deleted manually. This is a one-time action and will be executed based on the date selected for deletion.

Delete Logs Older Than / / for

ARCHIVE SONICWALL ANALYTICS LOG MESSAGES

Logs that no longer require to be stored in the system can be exported in CSV/HTML format and be offloaded from the database. The archive process will first archive the data to *archivedLogs* directory as per "Archive Log Schedule" and the data will then be deleted from the database.

Note: For non-window deployments: To offload the archived log files to the local drive, navigate to the Appliance > Systems > File Manager screen.

Enable Archive

Archive SonicWall Analytics Log Messages for months (?)

Maximum Log Message Files (?)

Delete Data Every at :

Archive Format CSV HTML

To delete Analytics log messages:

- 1 Under the heading **DELETE SONICWALL ANALYTICS LOG MESSAGES**, select the deletion date from the drop-down menu for month, day, and year next to **Delete Logs Older Than**.
- 2 Select the location for the logs in the drop-down menu next to **for**. You have two choices: **All Domains** and **LocalDomain**.
- 3 Click **Update** when done.

To archive Analytics log messages:

Logs that no longer require to be stored in the system can be exported in CSV or HTML format and be offloaded from the database. The archive process first archives the data to **archivedLogs** directory as per **Archive Log Schedule** and the data is then deleted from the database.

i | **NOTE:** For non-window deployments: to offload the archived log files to the local drive, navigate to the **Appliance > Systems > File Manager** screen.

- 1 Under the **ARCHIVE SONICWALL ANALYTICS LOG MESSAGES**, click the check box next to **Enable Archive** to store your logs.
- 2 Choose the number of months you want to **Archive SonicWall Analytics Log Messages for** from the drop-down list. You can archive your log messages for up to 12 months.
- 3 Choose the **Maximum Log Message Files** to be archived in the archivedLogs folder from the drop-down list. You can store a maximum of 99 files.
- 4 Delete your data by setting the day and time of your deletion using the drop-down menu next to **Delete Data Every**.
- 5 Choose your file **Archive Format** by clicking on the radio buttons for **CSV** or **HTML**.
- 6 Click **Update** when done.

View Log

The **Log > View Log** page tracks changes made from the user 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 log:

- 1 Scroll down to the **SEARCH RESULTS** section. Each log entry contains the following fields:
 - **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 Info).
 - **FIREWALL NAME**—specifies the name of the SonicWall appliance that generated the event (if applicable).
 - **SONICWALL ANALYTICS USER**—identifies the user role.
 - **USER IP**—specifies the user name and IP address.

You can also sort the **SEARCH RESULTS**. Click on any one of the column headings to sort the table descending or ascending based on the column heading.

- 2 Enter any number between 10 and 100 in the **Messages Per Screen** field to set number results shown per page.
- 3 Click **Apply**.
- 4 Click **Next** to view more.

SEARCH RESULTS

10 Messages per screen (Range: 10-100)

#	DATE	MESSAGE	SEVERITY	FIREWALL NAME	SONICWALL ANALYTICS USER	USER IP
1	Apr 11, 2019 Thur [00:18:30 AM]	Successful login into the system by user: admin	INFO		admin	10.21.120.202
2	Apr 11, 2019 Thur [00:03:16 AM]	The system logged out the following user because of idle timeout violation: admin	INFO		admin	10.21.120.202
3	Apr 10, 2019 Wed [10:44:01 PM]	Successful login into the system by user: admin	INFO		admin	10.21.120.202
4	Apr 10, 2019 Wed [09:37:19 PM]	Successful login into the system by user: admin	INFO		admin	10.21.120.202
5	Apr 10, 2019 Wed [07:10:32 AM]	Archived reports have exceeded the limitation. The oldest archived PDF report will be deleted.	WARNING		System	
6	Apr 10, 2019 Wed [07:10:32 AM]	Email/Archive Schedule ID 1 [Daily applications]: Schedule failed. Reason: Email action failed - Email Failed. Senders Email id is empty Archive result - Reports archived successfully to the specified folder.	WARNING		System	
7	Apr 9, 2019 Tue [07:10:31 AM]	Archived reports have exceeded the limitation. The oldest archived PDF report will be deleted.	WARNING		System	
8	Apr 9, 2019 Tue [07:10:31 AM]	Email/Archive Schedule ID 1 [Daily applications]: Schedule failed. Reason: Email action failed - Email Failed. Senders Email id is empty Archive result - Reports archived successfully to the specified folder.	WARNING		System	
9	Apr 8, 2019 Mon [07:10:30 AM]	Archived reports have exceeded the limitation. The oldest archived PDF report will be deleted.	WARNING		System	
10	Apr 8, 2019 Mon [07:10:30 AM]	Email/Archive Schedule ID 1 [Daily applications]: Schedule failed. Reason: Email action failed - Email Failed. Senders Email id is empty Archive result - Reports archived successfully to the specified folder.	WARNING		System	

Displaying 1-10


To search the results:

i **TIP:** You can press **Enter** to navigate from one element to the next in this section.

- In the **SEARCH CRITERIA** section, use the following fields, as needed, to refine your search:
 - Select Time of logs (From and To)**—Select from and to date to find the log entries created during the time.
 - SonicWall Node**—displays all log entries associated with the specified SonicWall appliance that you list.
 - Message contains**—enter any text find the events relevant to the text.
 - Severity**—select the severity level of the log. Your options are:
 - All (Alert, Warning, and Info)**
 - Alert and Warning**
 - Alert**
 - Select **Match case** to make the **SonicWall Node** and **Message contains** search fields case sensitive.
 - Select one of **Exact Phrase**, **All Words**, or **Any Word** to customize your search.
- Click **Start Search**.
- To clear all values from the input fields and start over, click **Clear Search**.


- 4 To download the results as an HTML file on your system, click **Export Logs** and download the file to your computer.

SEARCH CRITERIA

Select Time of logs: From 
(mm/dd/yyyy)

SonicWall Node

Message contains

To 
(mm/dd/yyyy)

SonicWall Analytics User

Severity ▾

Match case

Exact Phrase

All Words

Any Word

Management

This chapter describes the settings available in the **CONSOLE | Management** section.

Topics:

- [General](#)
- [Sessions](#)

General

On the **Management > General** page, you can change your password and configure your on-premises Analytics miscellaneous settings.

Changing your Password

To change your password:

- 1 Enter your **Current Password** in the text field provided.
- 2 Enter your **New Password** in the text field provided.
- 3 **Confirm New Password** in the text field provided.

Configuring the Miscellaneous Settings

To configure the miscellaneous settings:

- 1 Under **MISCELLANEOUS SETTINGS**, set the **Inactivity Timeout** in the field provided. The time should be stated in minutes. An entry of **-1** means the system never times out.
- 2 Set the number of rows that appear in non-reporting related paginated screens in **Max Rows Per Screen**. The value can range from 10 to 100.
- 3 Define the **Auto Save Dashboard Settings**. The value can range from 1 to 60. An entry of **-1** means the auto save is not enabled.
- 4 To configure what you want to see on the **Appliance Selection Panel**, **Show** enable or disable the following:
 - Select **Icons, Text**, or **Icons and Text (default)**
 - Check one of the following:
 - **Enable Audio Alarm when a Managed Unit goes Up**
 - **Enable Audio Alarm when a Managed Unit goes Down**

- 5 To configure the **Message of the Day**:
 - a Click on **View Message of the Day**.
 - b Disable the **Message of the Day** by checking the box **Don't display message when logging in**.
 - c Click **Close**.
- 6 Click **Update** to save the new settings.

General

🏠 / LocalDomain

CHANGE PASSWORD

Current Password

New Password

Confirm New Password

MISCELLANEOUS SETTINGS

Inactivity Timeout Minutes (-1 = never times out)

Max Rows Per Screen Range: [10..100] (Applicable to non-report)

Auto Save Dashboard Settings Minutes (-1:Auto Save not enabled or Ran)

Appliance Selection Panel, Show

- Icons
- Text
- Icons and Text (default)
-

Sessions

The **Management > Sessions** page allows you to view session statistics for currently logged in users and to end selected sessions. The **CURRENT SESSIONS** table has the **Delete**, **USER NAME**, **IP ADDRESS**, **LOGIN TIME**, **LAST ACCESS TIME**, and **DOMAIN NAME** columns.


To end a session:

- 1 Check the box next to any active session to end it. You can delete more than one session.
- 2 Click **End selected sessions** at the bottom right of the table.

Sessions

LocalDomain

CURRENT SESSIONS

	USER NAME	IP ADDRESS	LOGIN TIME	LAST ACCESS TIME	DOMAIN NAME
<input type="checkbox"/>	admin	10.21.112.222	Wed Jan 30 01:01:19 GMT 2019	Wed Jan 30 01:49:37 GMT 2019	LocalDomain
<input type="checkbox"/>	admin	10.21.112.222	Wed Jan 30 23:32:42 GMT 2019	Thu Jan 31 00:02:00 GMT 2019	LocalDomain
<input type="checkbox"/>	admin	10.21.112.222	Thu Jan 31 16:00:19 GMT 2019	Thu Jan 31 16:00:42 GMT 2019	LocalDomain
<input type="checkbox"/>	admin	10.21.112.222	Thu Jan 31 18:21:16 GMT 2019	Thu Jan 31 19:11:54 GMT 2019	LocalDomain
<input type="checkbox"/>	admin	10.21.112.222	Thu Jan 31 20:18:47 GMT 2019	Thu Jan 31 21:48:01 GMT 2019	LocalDomain
<input type="checkbox"/>	admin	10.50.193.54	Fri Feb 01 18:44:22 GMT 2019	Fri Feb 01 18:48:26 GMT 2019	LocalDomain
<input type="checkbox"/>	admin	10.21.112.222	Fri Feb 01 22:17:26 GMT 2019	Fri Feb 01 23:29:16 GMT 2019	LocalDomain
<input type="checkbox"/>	admin	10.21.112.222	Sat Feb 02 00:00:08 GMT 2019	Sat Feb 02 00:03:09 GMT 2019	LocalDomain
<input type="checkbox"/>	admin	10.21.112.222	Mon Feb 04 23:07:35 GMT 2019	Tue Feb 05 00:05:32 GMT 2019	LocalDomain
<input type="checkbox"/>	admin	10.50.193.54	Tue Feb 05 21:43:25 GMT 2019	Wed Feb 06 00:00:33 GMT 2019	LocalDomain

Reports

The **Reports** option is only visible for Syslog-based Analytics. These settings define the parameters for the various reports provided. Navigate to **CONSOLE > Reports** to see the options.

Topics:

- [Summarizer](#)
- [Syslog Filter](#)
- [Email/Archive](#)
- [Scheduled Reports](#)
- [Archive](#)

Summarizer

The **Reports > Summarizer** page provides several sections to help manage your reports.

The sections are:

- **DATA DELETION SCHEDULE**
- **DATA STORAGE CONFIGURATION**
- **PRIVATE IP HOSTNAME RESOLUTION CONFIGURATION**
- **PUBLIC IP HOSTYNAME RESOLUTION CONFIGURATION**
- **SYSLOGS SENT BY APPLIANCES THAT ARE NOT UNDER REPORTING AND MANAGEMENT**
- **SYSLOG DATA FILE SIZE CONFIGURATION**
- **MINIMUM DISK SPACE CONFIGURATION**
- **PACKET DATA VIEWER CONFIGURATION**

Summarizer

LocalDomain

DATA DELETION SCHEDULE

Delete Data Every: Saturday at 19 : 00

Update

DATA STORAGE CONFIGURATION

Summarizer at: 10.206.23.84

Keep Reporting Data for: 01 months

Keep Raw Syslog Data Files for: 01 months

Update

PRIVATE IP HOSTNAME RESOLUTION CONFIGURATION

Enable Reverse Hostname Resolution:

Refresh Resolved Hostname Cache every: 60 minutes

Scan every: 2 minutes

Lookup thread count: 10

Update

PUBLIC IP HOSTNAME RESOLUTION CONFIGURATION

Enable Public IP Host-name Resolution:

Time out value for Resolution: 100 milliseconds

Update

SYSLOGS SENT BY APPLIANCES THAT ARE NOT UNDER REPORTING AND MANAGEMENT

Store Syslogs:

Update

SYSLOG DATA FILE SIZE CONFIGURATION

Number of syslog messages per file: 100000

Update

MINIMUM DISK SPACE CONFIGURATION

Minimum % of disk space that should be free for Syslog Collector to consume syslogs: 10

Update

PACKET DATA VIEWER CONFIGURATION

Enable Packet Data Viewer:

Update

To set your data deletion schedule:

- 1 Choose the day and the time when you want your data deleted from the drop-down menu next to **Delete Data Every**.
- 2 Click **Update** when done.

To set your data storage configuration schedule:

- 1 Choose the IP address from the drop-down menu next to Summarizer at.
- 2 Select how long you want your data stored for from the drop-down menu next to **Keep Reporting Data for**. The choices are between one and 36 months.
- 3 Select how long you want your raw syslog data files stored for from the drop-down menu next to **Keep Raw Syslog Data Files for**. The choices are between one and 36 months.
- 4 Click **Update** when done.

To set your private hostname resolution configuration:

- 1 Check the box next to **Enable Reverse Hostname Resolution**.
- 2 Choose to **Refresh Resolved Hostname Cache every XX minutes**. This is the time duration for which the hostname is cached to a particular IP address.
- 3 Choose to **Scan every xx minutes**. This is the time intervals at which the lookup is triggered.
- 4 Choose to **Lookup the thread count**. This is the number of threads that will be processing the resolution.
- 5 Click **Update** when done.

To set your public hostname resolution configuration:

- 1 Check the box next to **Enable Public IP Hostname Resolution**.
- 2 Choose the **Time out value for Resolution in XX milliseconds**.
- 3 Click **Update** when done.

To store your syslog reports:

- 1 Check the box next to **Store Syslogs**.
- 2 Click **Update** when done.

To store your syslog messages per file:

- 1 Enter the **Number of syslog messages per file** you want to keep. The default number is 10,000.
- 2 Click **Update** when done.

To set your minimum disk space configuration:

- 1 Choose the **Minimum % of disk space that should be free for Syslog Collector to consume syslogs:**. The disk space choices in the drop-down menu range from default to 10, 15, 20, and 25 percentage. **Default** sets it at 5GB minimum disk space required.
- 2 Click **Update** when done.

To set your packet data viewer configuration:

- 1 Check the box next to **Enable Packet Data Viewer**.
- 2 Click **Update** when done.

- i** **NOTE:** Changes to **Data Deletion Schedule** and **Data Storage Configuration** take effect after the current run.
- Report data older than current month + **Number of month to keep** are deleted.
- It is recommended that the **Data Deletion Schedule** be configured to run after the data has been backed up. Navigate to **Appliance > System > Backup/Restore** to review the current backup schedule.
- Enabling **Private IP 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 the summarizer, increase memory and consume more CPU cycle. Also, the memory and CPU are impacted further by changing the default configurations of **Lookup thread count**, **Scan every**, and **Refresh Resolved Hostname Cache every**.
- Any changes to Hostname Resolution Configuration take effect during the next summarizer run.
- Syslog Collector needs to be restarted for the changes to **Minimum Disk Space Configuration** to take effect. If the free disk space falls below this value, Syslog Collector stops listening for syslogs.
- Changes to **Syslog Data File Size Configuration** reflects the number of syslog messages per .src file in the syslogs directory.
- Setting the **Minimum Disk Space** percentage to **Default** sets it to 5GB minimum disk space required.

Syslog Filter

The **Reports > Syslog Filter** page gives you access to the Syslog Exclusion Filters, which you can apply to the syslogs uploaded to the reporting database. All syslogs continue to be stored in the file system without any filtering.

Exclusion filter settings are picked up the summarizer every: 00 hour(s):15 min(s).

To add/modify a Syslog Exclusion Filter at the unit level, navigate to **Firewall/SRA > Unit Level > Reports > Filter Settings**.

The Syslog Filter table features the **STATUS**, **SYSLOG FIELD NAME**, **OPERATOR**, **SYSLOG FILTER VALUE**, **LEVEL**, **COMMENT**, **GMS USER**, and **CONFIGURE** columns.

- i** **NOTE:** Only a super administrator, also known as a Super Admin, can edit, add, and delete a filter.

To add, delete, or enable/disable a syslog filter:

- 1 Check the box next to the filter you want to manage.
- 2 Click the **Add**, **Delete**, or **Enable/Disable** buttons at the bottom of the table.

To access the **Scheduled Reports** page in **Syslog Reports**, click the **CONSOLE** button, next to **REPORTS**, in the top navigation menu. The view changes immediately to the **Log > View Log** default page.

Click **Reports > Scheduled Reports** to set up or change the reports you want generated on a regular basis.

Syslog Filter

LocalDomain

SYSDLOG EXCLUSION FILTER

<input type="checkbox"/>	STATUS	SYSDLOG FIELD NAME	OPERATOR	SYSDLOG FILTER VALUE	LEVEL	COMMENT	OMS USER	CONFIGURE
<input type="checkbox"/>	●	m	=	98	Appliance	Connection Opened. Source for the system filters is taken from Log Event Reference Guides	System@LocalDomain	
<input type="checkbox"/>	●	m	=	805	Appliance	Interface Statistics Report. Source for the system filters is taken from Log Event Reference Guides	System@LocalDomain	
<input type="checkbox"/>	●	m	=	37	Appliance	UDP packet dropped. Source for the system filters is taken from Log Event Reference Guides	System@LocalDomain	
<input type="checkbox"/>	●	m	=	602	Appliance	DNS packet allowed. Source for the system filters is taken from Log Event Reference Guides	System@LocalDomain	
<input type="checkbox"/>	●	m	=	700	Appliance	Deleting from Multicast policy list. VPN SPT. Source for the system filters is taken from Log Event Reference Guides	System@LocalDomain	
<input type="checkbox"/>	●	proto	=	udp/dns	Appliance	UDP DNS traffic. Source for the system filters is taken from Log Event Reference Guides	System@LocalDomain	
<input type="checkbox"/>	●	proto	=	vdshetbios-rs	Appliance	UDP traffic. Source for the system filters is taken from Log Event Reference Guides	System@LocalDomain	
<input type="checkbox"/>	●	m	=	1197	Appliance	NAT Mapping. Source for the system filters is taken from Log Event Reference Guides	System@LocalDomain	
<input type="checkbox"/>	●	m	=	897	Appliance	ICMP packet allowed. Source for the system filters is taken from Log Event Reference Guides	System@LocalDomain	
<input type="checkbox"/>	●	pri	=	7	Appliance	Message priority. 7-debug. Source for the system filters is taken from Log Event Reference Guides	System@LocalDomain	
<input type="checkbox"/>	●	m	=	36	Appliance	TCP connection dropped. Source for the system filters is taken from Log Event Reference Guides	System@LocalDomain	
<input type="checkbox"/>	●	m	=	520	Appliance	Web management request allowed. Source for the system filters is taken from Log Event Reference Guides	System@LocalDomain	
<input type="checkbox"/>	●	m	=	30	Appliance	ICMP packet dropped due to policy. Source for the system filters is taken from Log Event Reference Guides	System@LocalDomain	
<input type="checkbox"/>	●	m	=	346	Appliance	IKE Initiator: Start Quick Mode. Source for the system filters is taken from Log Event Reference Guides	System@LocalDomain	
<input type="checkbox"/>	●	m	=	483	Appliance	Received notify. INVALID_ID_INFO. Source for the system filters is taken from Log Event Reference Guides	System@LocalDomain	
<input type="checkbox"/>	●	m	=	524	Appliance	Web access request dropped. Source for the system filters is taken from Log Event Reference Guides	System@LocalDomain	
<input type="checkbox"/>	●	m	=	352	Appliance	IKE Responder: Received Quick Mode Request. Source for the system filters is taken from Log Event Reference Guides	System@LocalDomain	
<input type="checkbox"/>	●	m	=	88	Appliance	IKE Responder: Psec proposal does not match. Source for the system filters is taken from Log Event Reference Guides	System@LocalDomain	
<input type="checkbox"/>	●	m	=	934	Appliance	IKE Responder: Peer local network does not match VPN policy's Destination Network. Source for the system filters is taken from Log Event Reference Guides	System@LocalDomain	
<input type="checkbox"/>	●	m	=	830	Appliance	IKE Initiator: Remote saary timeout - Retransmitting IKE request. Source for the system filters is taken from Log Event Reference Guides	System@LocalDomain	
<input type="checkbox"/>	●	m	=	401	Appliance	Received notify. NO_PROPOSAL_CHOSEN. Source for the system filters is taken from Log Event Reference Guides	System@LocalDomain	
<input type="checkbox"/>	●	m	=	402	Appliance	IKE Responder: IKE proposal does not match. Source for the system filters is taken from Log Event Reference Guides	System@LocalDomain	
<input type="checkbox"/>	●	m	=	1391	Deployment	Packet Data. Source for the system filters is taken from Log Event Reference Guides	System@LocalDomain	

Add Delete Enable/Disable

Email/Archive

The **Reports > Email/Archive** page has three sections to allow you to manage your reports. The sections are:

- EMAIL/ARCHIVE TIME SETTINGS
- LOGO SETTINGS
- USER TIMEOUT CONFIGURATION
- SORT BY SETTINGS IN PDF REPORTS

Email/Archive

LocalDomain

EMAIL/ARCHIVE TIME SETTINGS

Next Scheduled Email/Archive Time (mm/dd/yyyy hh:min) 09/28/2019 07 : 10

Send Weekly Reports Every Monday

Send Monthly Reports Every 7 of the Month

Note:
* Weekly reports are generated for Monday-Sunday of the week, and Monthly Reports are generated for the 1-30/31 of the month.

LOGO SETTINGS

Logo currently in use: cover_logo.gif
Logo File: No file chosen

USR TIMEOUT CONFIGURATION

Time out Value: 120 minutes

SORT BY SETTINGS IN PDF REPORTS

MBytes
Hits/Connections/Events

To set your email and archive settings:

- 1 Choose your **Next Scheduled Email/Archive Time (mm/dd/yyyy hh:min)** by specifying the date in the text field provided and the hour of the day and minutes from the drop-down menus.
- 2 Choose the day of the week you want to **Send Weekly Reports Every** from the drop-down menu.
- 3 Choose the day of the month you want to **Send Monthly Reports Every** from the drop-down menu. You can choose to send your email/reports between the first and the last day (31) of the month.
- 4 Click the **Update** buttons next to each of the choices above.

i **NOTE:** Weekly reports are generated for Monday-Sunday of the week and Monthly Reports are generated for the 1-30/31 of the month.

To set your logo settings:

- 1 Click **Choose File** next to **Logo File**.
- 2 Click **Update** when done.

To set your timeout configuration:

- 1 Choose your Time out Value up to 120 minutes, which is the default.
- 2 Click **Update** when done.

To sort by settings in the PDF reports:

- 1 Check the radius button for either MBytes or Hits/Connections/Events.
- 2 Click **Update** when done.

Scheduled Reports

SonicWall Analytics

REPORTS | CONSOLE

Scheduled Reports

Schedules in the system: 2
Weekly Schedules Last Attempted: 2019-09-23T07:10
Monthly Schedules Last Attempted: Not Available

Next Scheduled Email/Archive Time: 2019-09-27T07:10
Next Weekly Reports Time: 2019-09-30T07:10
Next Monthly Reports Time: 2019-10-07T07:10

SCHEDULE NAME	ID	SCHEDULE TYPE	ARCHIVE / EMAIL	EMAIL SUBJECT	OWNER	LAST RUN TIME	STATUS	ACTIONS
myreport	2	Daily		Scheduled Reports	admin@LocalDomain	2019-09-26T07:10:29-07:00	Failed	
test	1	Daily		Scheduled Reports	admin@LocalDomain	2019-09-26T07:10:22-07:00	Failed	


Total 2 Schedule(s)

Topics:






- [Managing the Reports](#)
- [Navigating the Schedules Page](#)
 - [Setting Up the Reports in Analytics Syslog](#)
 - [Checking the Reports](#)
 - [Setting the Report Date Range](#)

Managing the Reports

Several icons at the top right corner of the **Scheduled Reports** table help you manage your reports. Some restrictions and limits are enforced, and a few additional steps are involved while creating a group-level Scheduled Report. Refer to the image and table below to learn more about them.

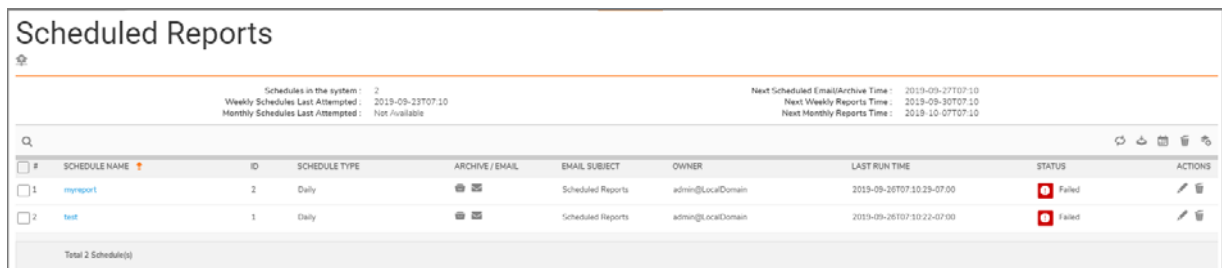
 **NOTE:** A maximum of 10 schedules are allowed to be created for a single group.











Scheduled Reports icons

Icon	Description
	Allows you to refresh the data.
	Allows you to archive your report when you click on the icon.
	Allows you to archive your report for the specific date range you define.
	Allows you to delete scheduled reports.
	Allows you to create a scheduled report.

Navigating the Schedules Page

Go to **Reports > Scheduled Reports** to view a list of all the scheduled reports that have been defined. The details of each report are shown in the table.



#	SCHEDULE NAME	ID	SCHEDULE TYPE	ARCHIVE / EMAIL	EMAIL SUBJECT	OWNER	LAST RUN TIME	STATUS	ACTIONS
1	myreport	2	Daily	 	Scheduled Reports	admin@LocalDomain	2019-09-26T07:10:29-07:00	 Failed	 
2	test	1	Daily	 	Scheduled Reports	admin@LocalDomain	2019-09-26T07:10:22-07:00	 Failed	 


Click the search icon at the top left of the table to search for a specific report. As you type characters in the field, the table filters accordingly. To clear the filter, delete the characters.

- Click **SCHEDULE NAME** to see details about the report schedule.
- Click **ID** to see the number associated with a report.
- Click **SCHEDULE TYPE** to sort the schedules.
- The icons in the **ARCHIVE/EMAIL** column indicate whether the report is set up for archiving or emailing, or both. This parameter can be changed by clicking the **Edit** icon.
- Click **EMAIL SUBJECT** to sort by email subject.
- Click **OWNER** to sort by owner.
- Click **LAST RUN TIME** to sort by the time the schedule was last executed.
- Click **STATUS** to see whether the report was successfully run or not.
- Click **ACTIONS** to **Edit** or **Delete** a report.

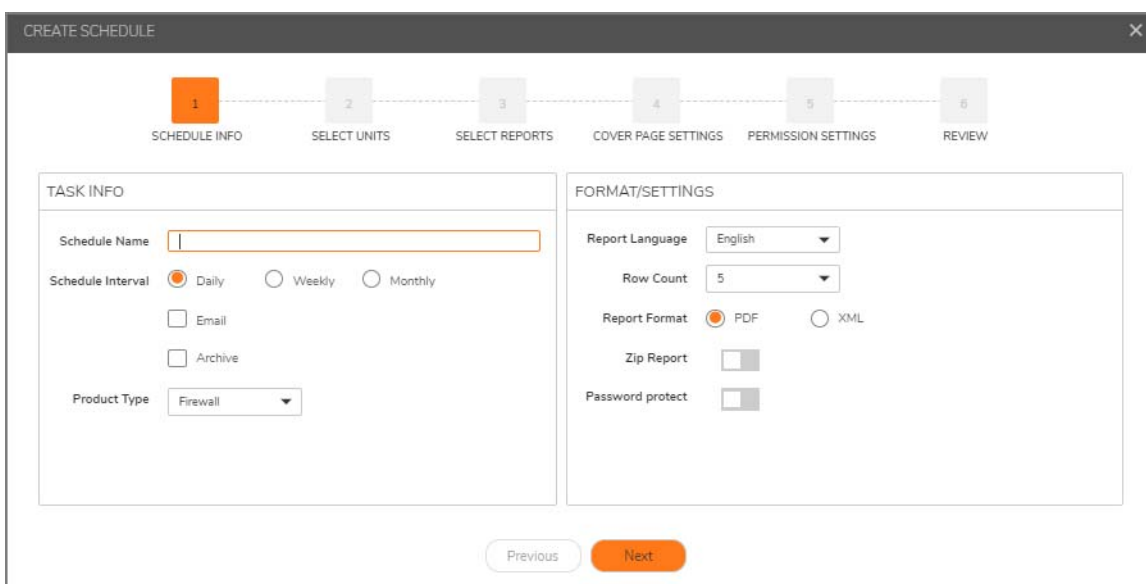
Setting Up the Reports in Analytics Syslog

To set up a scheduled report in an Analytics 2.5 syslog system:

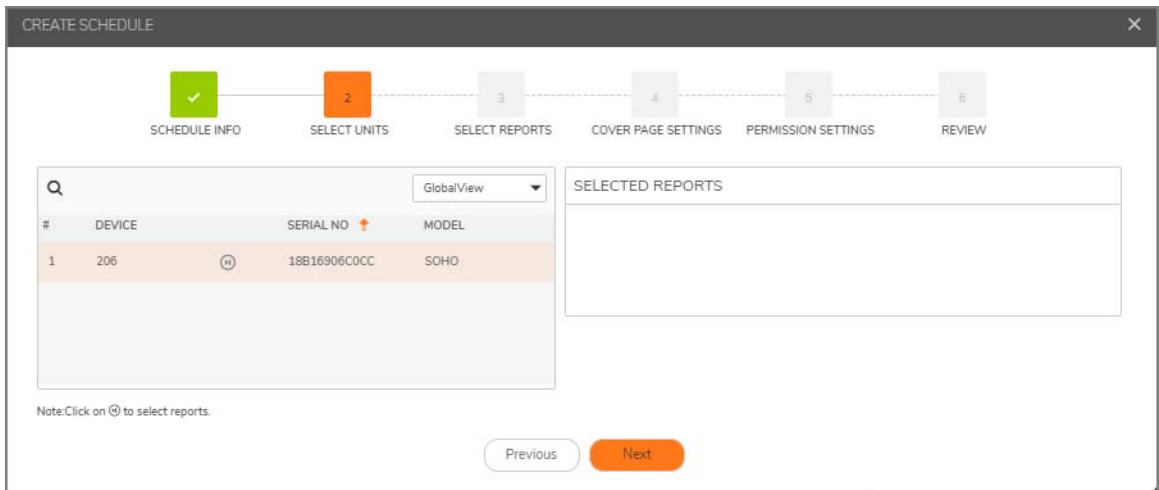
- 1 At the top right of the **Scheduled Reports** table, click on the icon to **Create a Schedule Report**.
- 2 Under **TASK INFO**, type the **Schedule Name**.
- 3 Select the **Schedule Interval**. You can choose **Daily**, **Weekly**, and **Monthly**. The default time interval is **Daily**.
- 4 Check **Email** if you want the report emailed directly to someone and provide the email address in the field that appears.
- 5 Check **Archive** if you want the report stored locally.

 **NOTE:** You can select both the **Email** and the **Archive** options.

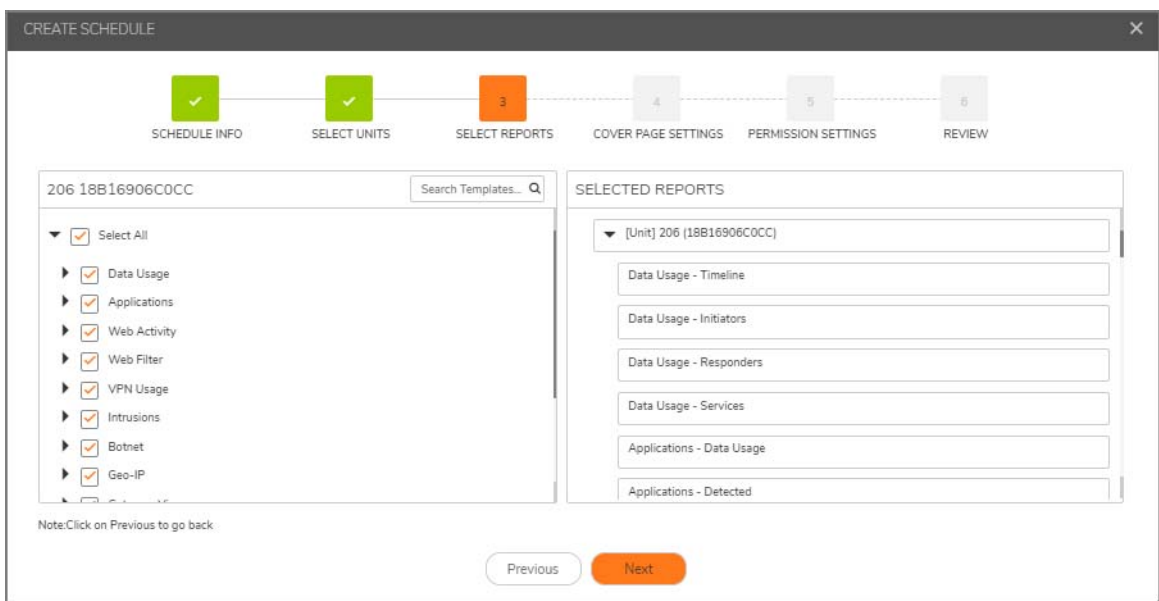
- 6 Under **FORMAT/SETTINGS**, select the **Report Language**.
- 7 Select the **Row Count** from the drop-down list. You can choose between 5, 10, 20, and 50.
- 8 Select the **Report Format** in either **PDF** or **XML** files.
- 9 Check the box for a **Zip Report** and/or **Password protect it**.



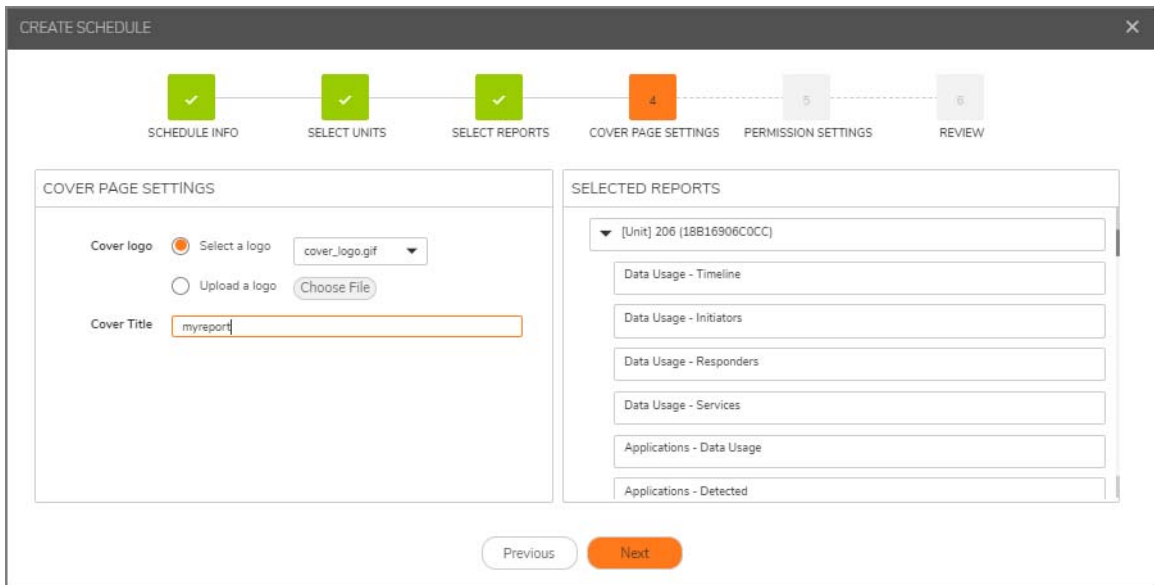
- 10 Click **Next**.
- 11 Select one of the views from the drop-down list. You can choose from **GlobalView**, **FirmwareView**, **ModelView**, or **InstanceView**.
- 12 Click the **DEVICE** you want.
- 13 Click **Next**.



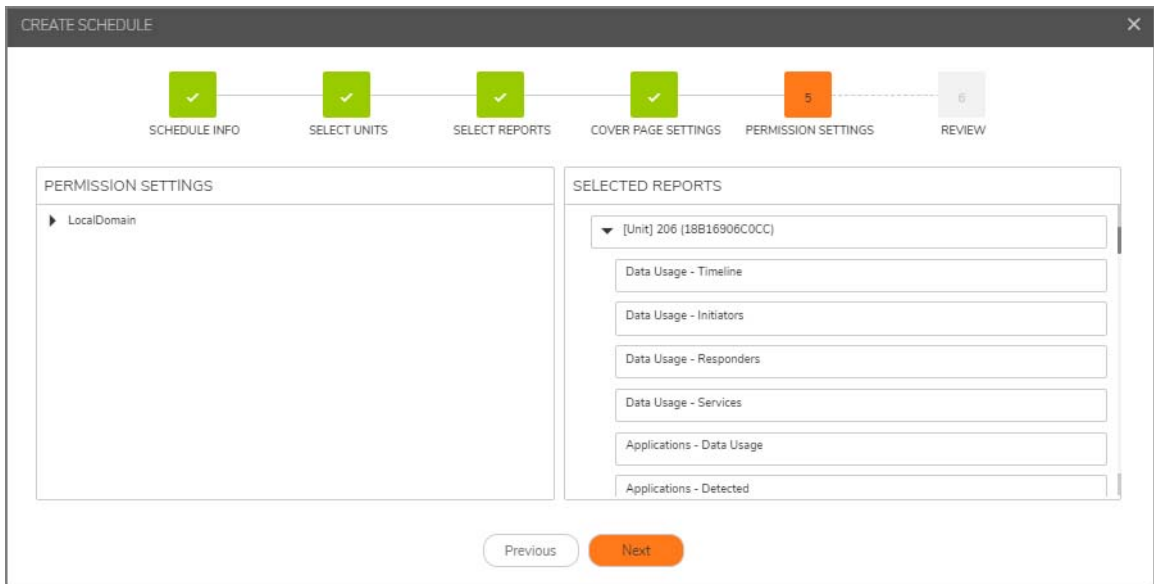
- 14 Search Templates next to the small search icon.
- 15 Check the box for the report you want. You can **Select All** or select individual reports.
- 16 Your choices appear under the **SELECTED REPORTS** section.
- 17 Click **Next**.



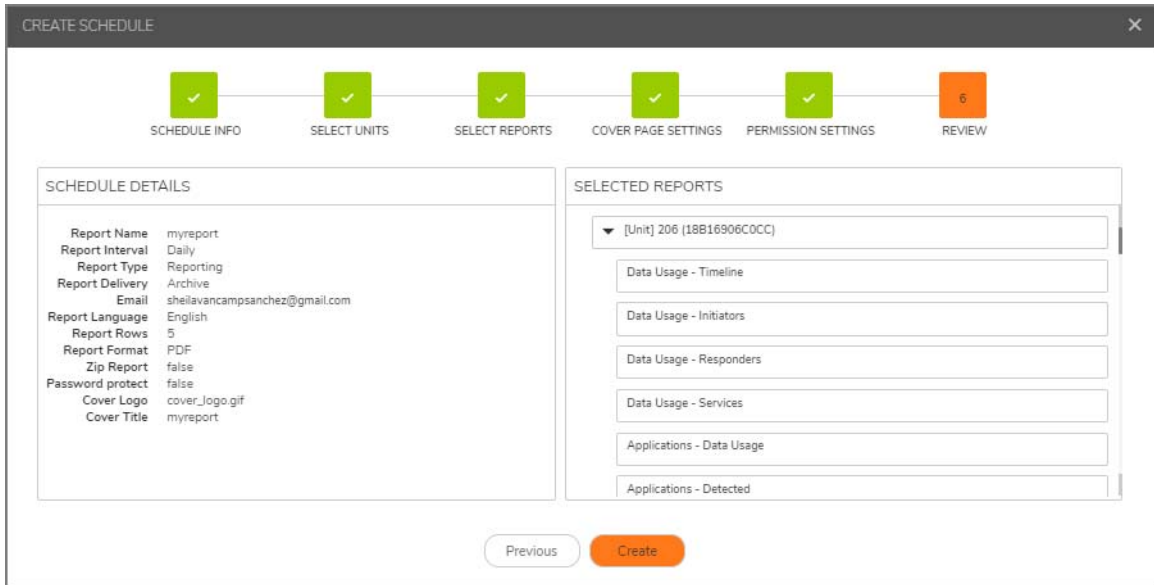
- 18 Under **COVER PAGE SETTINGS**, select your **Cover logo** from the drop-down list or **Upload a logo** by clicking **Choose File**.
- 19 Enter your **Cover Title** in the text field provided.
- 20 Click **Next**.



21 Check your **PERMISSION SETTINGS**, your **SELECTED REPORTS**, and click Next.

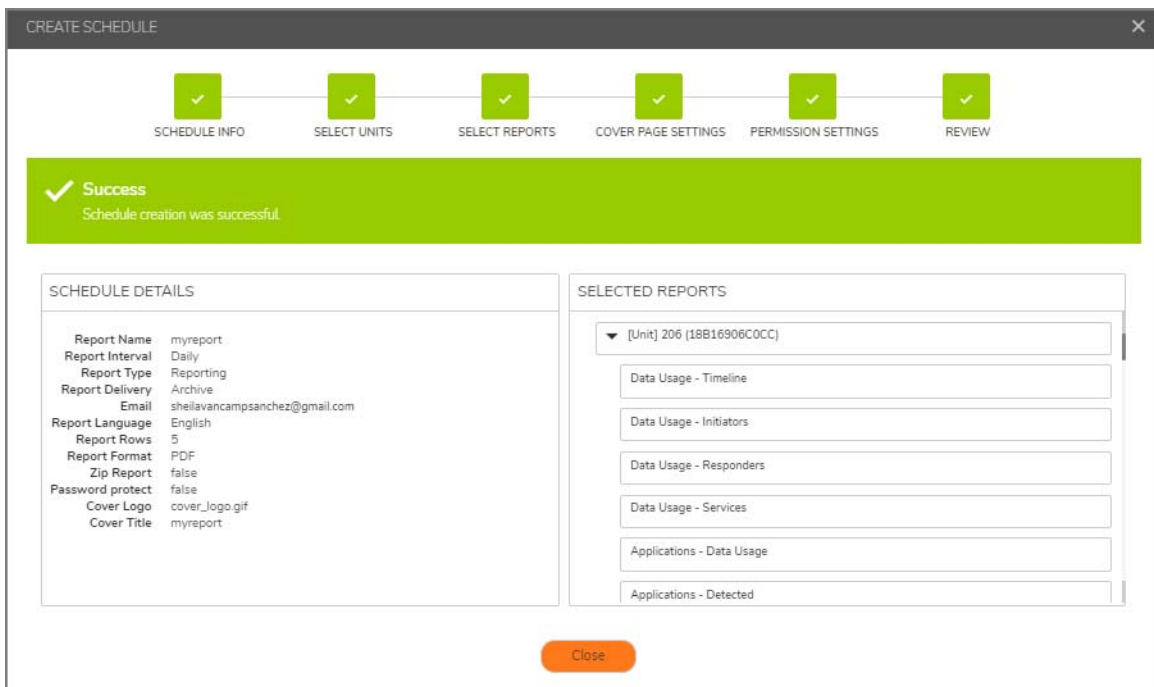


22 Review your **SCHEDULE DETAILS**, your **SELECTED REPORTS**, and click Create.



23 After your Schedule creation has been successful a screen appears with your **SCHEDULE DETAILS** and **SELECTED REPORTS**.

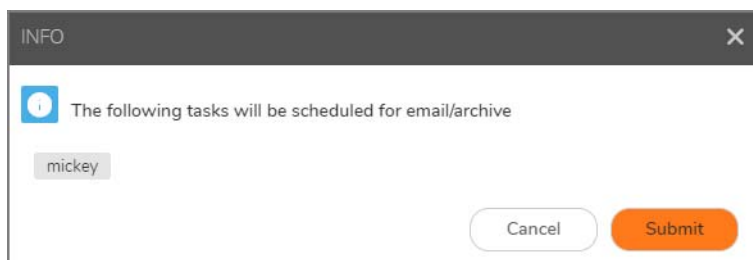
24 Click **Close** when done.



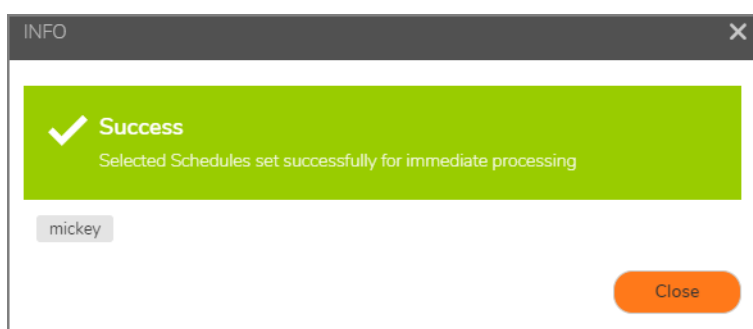
Checking the Reports

After you have created your reports, you can check on them by clicking the check boxes next to them. You can also check if your configurations have been saved and are scheduled as you have planned.

- 1 Navigate to **CONSOLE | Scheduled Reports | SCHEDULE NAME** column.
- 2 Check the box next to the name of your report.
- 3 Click the **Archive Now** icon at the top right of the table.



- 4 Click **Submit**.



- 5 Click **Close**.


Setting the Report Date Range

- 1 Check the box next to your report **SCHEDULE NAME**.
- 2 Then, click the **Archive for date range** icon at the top right of the table to select your date range.
- 3 Click in the **Start Date** and **End Date** fields to select your preferred dates.
- 4 Click **Submit**.

SELECT DATE RANGE ✕

Start Date

End Date

 The following tasks will be scheduled for email/archive

My Report

Archive

The **Reports > Archive** page gives you access to the Archived reports, which you can search for in the reporting database. All archived reports continue to be stored in the file system until you delete them.

The Archive table features the **SCHEDULE NAME**, **FORMAT**, **SOURCE**, **TRIGGER**, **GENERATION TIME**, **START TIME**, **END TIME**, and **ACTION** columns.

To download or delete your archived reports:

- 1 Check the box next to the archived report you want to **download** or **delete**.
- 2 Click the **Download** or **Delete** icons under the **ACTIONS** column for the row you selected.

Archive									
🏠 / LocalDomain / null									
🔍 📄 🗑️ 🔄									
<input type="checkbox"/>	#	SCHEDULE NAME	FORMAT	SOURCE	TRIGGER	GENERATION TIME ↓	START TIME	END TIME	ACTIONS
<input checked="" type="checkbox"/>	1	myreport	PDF	SYSLOG	Scheduled	2019-09-27T00:10:29-07:00	2019-09-25T17:00:00-07:00	2019-09-26T16:59:59-07:00	📄 🗑️
<input type="checkbox"/>	2	test	PDF	SYSLOG	Scheduled	2019-09-27T00:10:22-07:00	2019-09-25T17:00:00-07:00	2019-09-26T16:59:59-07:00	📄 🗑️
<input type="checkbox"/>	3	myreport	PDF	SYSLOG	Scheduled	2019-09-26T00:10:29-07:00	2019-09-24T17:00:00-07:00	2019-09-25T16:59:59-07:00	📄 🗑️
<input type="checkbox"/>	4	test	PDF	SYSLOG	Scheduled	2019-09-26T00:10:22-07:00	2019-09-24T17:00:00-07:00	2019-09-25T16:59:59-07:00	📄 🗑️
<input type="checkbox"/>	5	myreport	PDF	SYSLOG	Scheduled	2019-09-25T00:10:30-07:00	2019-09-23T17:00:00-07:00	2019-09-24T16:59:59-07:00	📄 🗑️
<input type="checkbox"/>	6	test	PDF	SYSLOG	Scheduled	2019-09-25T00:10:22-07:00	2019-09-23T17:00:00-07:00	2019-09-24T16:59:59-07:00	📄 🗑️
<input type="checkbox"/>	7	myreport	PDF	SYSLOG	Scheduled	2019-09-24T00:10:28-07:00	2019-09-22T17:00:00-07:00	2019-09-23T16:59:59-07:00	📄 🗑️
<input type="checkbox"/>	8	test	PDF	SYSLOG	Scheduled	2019-09-24T00:10:22-07:00	2019-09-22T17:00:00-07:00	2019-09-23T16:59:59-07:00	📄 🗑️
<input type="checkbox"/>	9	myreport	PDF	SYSLOG	Scheduled	2019-09-23T00:10:29-07:00	2019-09-21T17:00:00-07:00	2019-09-22T16:59:59-07:00	📄 🗑️
<input type="checkbox"/>	10	test	PDF	SYSLOG	Scheduled	2019-09-23T00:10:22-07:00	2019-09-21T17:00:00-07:00	2019-09-22T16:59:59-07:00	📄 🗑️
<input type="checkbox"/>	11	myreport	PDF	SYSLOG	Scheduled	2019-09-22T00:10:29-07:00	2019-09-20T17:00:00-07:00	2019-09-21T16:59:59-07:00	📄 🗑️
<input type="checkbox"/>	12	test	PDF	SYSLOG	Scheduled	2019-09-22T00:10:22-07:00	2019-09-20T17:00:00-07:00	2019-09-21T16:59:59-07:00	📄 🗑️
<input type="checkbox"/>	13	myreport	PDF	SYSLOG	Scheduled	2019-09-21T00:10:29-07:00	2019-09-19T17:00:00-07:00	2019-09-20T16:59:59-07:00	📄 🗑️
<input type="checkbox"/>	14	test	PDF	SYSLOG	Scheduled	2019-09-21T00:10:22-07:00	2019-09-19T17:00:00-07:00	2019-09-20T16:59:59-07:00	📄 🗑️
<input type="checkbox"/>	15	myreport	PDF	SYSLOG	Scheduled	2019-09-20T00:10:33-07:00	2019-09-18T17:00:00-07:00	2019-09-19T16:59:59-07:00	📄 🗑️
<input type="checkbox"/>	16	test	PDF	SYSLOG	Scheduled	2019-09-20T00:10:25-07:00	2019-09-18T17:00:00-07:00	2019-09-19T16:59:59-07:00	📄 🗑️

Total 16 File(s)

Licenses

The **Licenses > Product Licenses** page allows the user to view, upload, and manage licenses and subscriptions for this implementation.

Topics:

- [License Summary](#)
- [Managing Licenses](#)
- [Refreshing Licenses](#)
- [Uploading a License](#)

License Summary

View license details on the **CONSOLE | Licenses > Product Licenses** page, under the **LICENSE SUMMARY** section. You can view the following information:

- Last date and time THE SonicWall license registration was contacted
- The serial number for the firewall being monitored.
- Security Service information: if licensed, the license capacity and the expiration date
- Support Service information:
 - Analytics E-Class 24x7 Software Support

Managing Licenses

Your MySonicWall account is a one-stop resource for registering all your SonicWall security appliances and managing all your SonicWall security service upgrades and changes. MySonicWall provides you with an easy to use interface to manage services and upgrades for multiple SonicWall appliances.

To manage licenses:

- 1 Click **Manage**.
- 2 Enter your **MySonicWall username/email address**.
- 3 Enter your **Password**.
- 4 Click **Login**.
- 5 If you forgot your username and password, click **Return to License Summary**.

Refreshing Licenses

This feature allows you to synchronize Management services with the MySonicWall license server. Synchronization is useful if you have recently purchased new licenses, and these licenses are not yet appearing in the summary page.

Click **Refresh**. The License Summary page notes that the refresh completed successfully, and the date of the last contact changes to reflect the new date and time.

Uploading a License

Normally, MySonicWall communicates with your Management service to synchronize licenses automatically. The manual upload feature is useful if for some reason your unit is without Internet connectivity.

To manually upload a license:

- 1 Click **Upload**.
- 2 Click **Choose File** to search for your locally stored license file.

i **NOTE:** License files for manual updates are available for download through your MySonicWall account.

- 3 Click **Upload** to complete the license transfer.

Product Licenses

LocalDomain

LICENSE SUMMARY

i License refresh completed successfully.

Last SonicWall Registration Site Contact Sep 27 2019 10:02PM

Serial Number 004010363B5A

SECURITY SERVICE	STATUS	CAPACITY	EXPIRATION
SonicWall Analytics On-Prem	Licensed	500 GB	

SUPPORT SERVICE

Analytics E-Class 24x7 Software Support Not Licensed

Manage Refresh Upload

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://www.sonicwall.com/support>.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View video tutorials
- Access MySonicWall
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit <https://www.sonicwall.com/support/contact-support>.

About This Document

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.

SonicWall Firewall Management **CONSOLE** Administration Guide
Updated - December 2019
232-005146-00 Rev A

Copyright © 2019 SonicWall Inc. All rights reserved.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit <https://www.sonicwall.com/legal>.

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/en-us/legal/license-agreements>.

Open Source Code

SonicWall is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request
SonicWall Inc. Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035