SonicWall® Global Management System Secure Mobile Acess

Administration Guide

Contents

SMA Manage 4

Introduction to SMA Manage 4

Managing SMA General Settings 6

SMA Status 6

SMA Tools 8

SMA Info 10

Settings 11

Saved Settings 11

Store New Settings 12

File Backup Status 12

File Backup Settings 12

Configure Missed Reports Settings 12

Registering/Upgrading 13

Registering SonicWall SSL-VPN Appliances 13

Upgrading SonicWall SMA Firmware 14

Logging in to SMA using SonicWall GMS 14

Configuring Alerts 15

Configuring Alerts in the SMA View 15

Enabling/Disabling/Deleting/Editing Alerts 18

Current Alerts 19

Managing SMA Reports 20

SMA Reporting Overview 20

SMA Reports Tab 20

What is SMA Reporting? 20

Benefits of SMA Reporting 21

How Does SMA Reporting Work? 21

Using and Configuring SMA Reporting 21

Viewing Available SMA Report Types 22

Configuring SMA Scheduled Reports 24

Navigating Through Detailed SMA Reports 25

Viewing SMA Summary Reports 26

Viewing SMA Unit-Level Reports 27

Viewing Unit-Level Data Usage Reports 27

Viewing SMA Top Users Reports 28

Viewing Access Method Reports 29

Viewing SMA Authentication User Login Report 31

Viewing SMA Authentication Failed Login Report 31

Viewing Web Application Firewall (WAF) Reports 32

Viewing Connection Reports 37

Viewing Uptime/Downtime Reports 38

Viewing SMA Log Analyzer 39

Saving System Log Reports 40

Sysog Exclusion Filter 40

Events 42

Current Alerts 43

SonicWall Support 44

About This Document 45

1

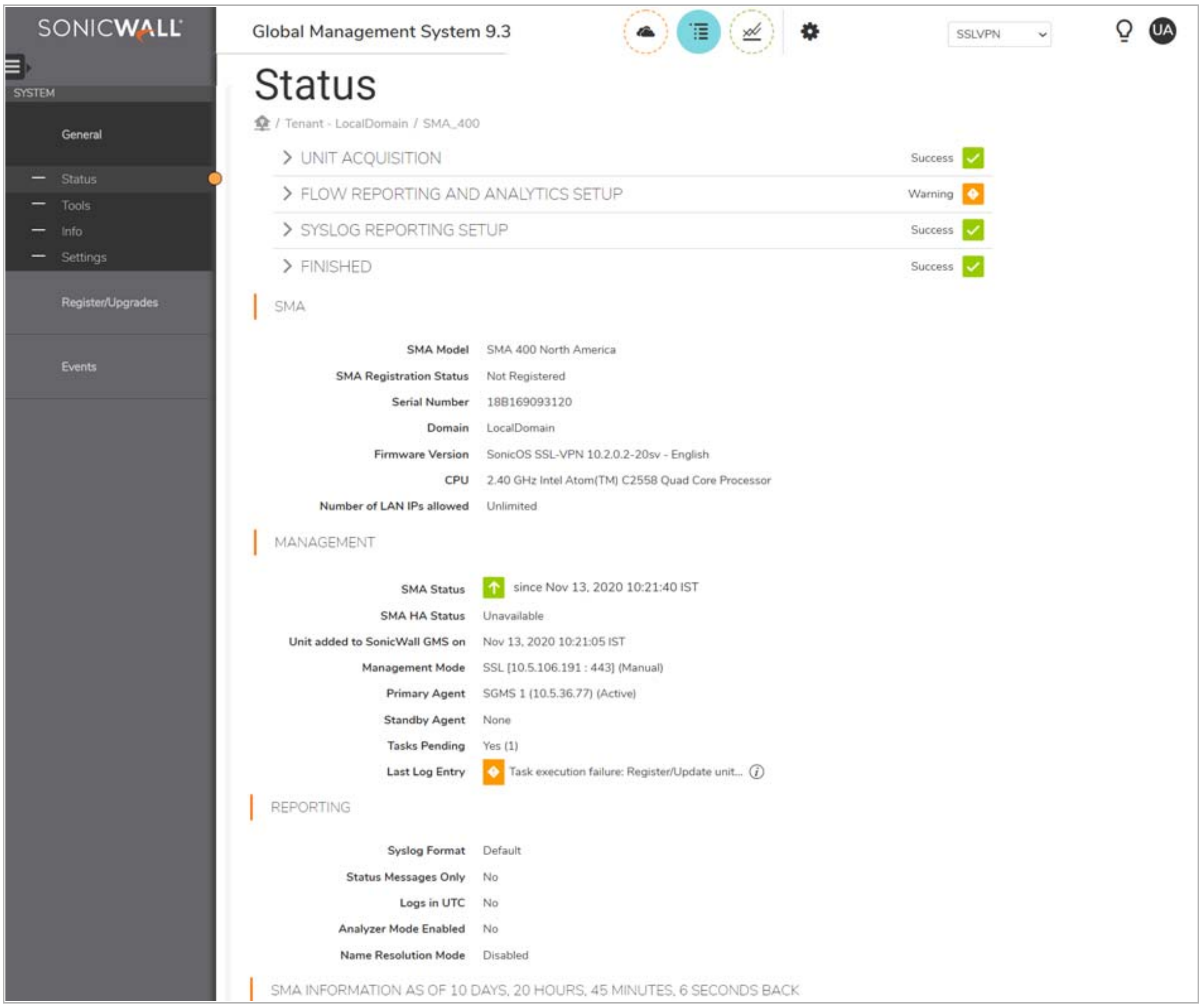
SMA Manage

This chapter provides instructions for configuring or changing polices for SonicWall® Secure Mobile Access (SMA) and contains the following sections:

- Introduction to SMA Manage
- Managing SMA General Settings
- Settings
- Registering/Upgrading
- Logging in to SMA using SonicWall GMS
- Configuring Alerts

Introduction to SMA Manage

This chapter provides instructions for modifying the general status and tools for SonicWall SMA platforms. To modify the general status and tools of a SMA appliance using SonicWall GMS, navigate to **SMA | Management Panel| General**. You will see the options **Status**, **Tools, Info** and **Settings**.



Status

/ Tenant - LocalDomain / SMA_400

> UNIT ACQUISITION	Success ✓
> FLOW REPORTING AND ANALYTICS SETUP	Warning ◆
> SYSLOG REPORTING SETUP	Success ✓
> FINISHED	Success ✓

SMA

SMA Model	SMA 400 North America
SMA Registration Status	Not Registered
Serial Number	18B169093120
Domain	LocalDomain
Firmware Version	SonicOS SSL-VPN 10.2.0.2-20sv - English
CPU	2.40 GHz Intel Atom(TM) C2558 Quad Core Processor
Number of LAN IPs allowed	Unlimited

MANAGEMENT

SMA Status	↑ since Nov 13, 2020 10:21:40 IST
SMA HA Status	Unavailable
Unit added to SonicWall GMS on	Nov 13, 2020 10:21:05 IST
Management Mode	SSL [10.5.106.191 : 443] (Manual)
Primary Agent	SGMS 1 (10.5.36.77) (Active)
Standby Agent	None
Tasks Pending	Yes (1)
Last Log Entry	◆ Task execution failure: Register/Update unit... ⓘ

REPORTING

Syslog Format	Default
Status Messages Only	No
Logs in UTC	No
Analyzer Mode Enabled	No
Name Resolution Mode	Disabled

SMA INFORMATION AS OF 10 DAYS, 20 HOURS, 45 MINUTES, 6 SECONDS BACK

General

- The **SMA | Management Panel | General > Status** section provides the current status of the SMA appliance and allows for an instant update of appliance information using **Fetch Information**.
- The **SMA | Management Panel | General > Tools** section provides the following options: **Restart Appliance**, **Synchronize Settings**, and **Synchronize Licenses**.

  ⓘ | **NOTE:** The Restart Appliance option is not available for SonicWall Aventail SMA appliances.

- The **SMA | Management Panel| General > Info** section provides the ability to update the contact information for the SMA appliance. You can update the details including **Appliance Contact Info**, **GEO Location**, **Contact Info**, and **ISP Info**.
- The **SMA | Management Panel | General > Settings** section provides the ability to view the saved settings, save the settings to a local file, restore settings to the unit, and delete the settings. You can also store new settings, enable and set the file backup, and configure missed reports settings.

Register/Upgrades

- The **SMA | Management Panel | Register/Upgrades > Register SSL-VPNs** screen provides the ability to register SMA appliances with your MySonicWall.com account.

  ⓘ | **NOTE:** Registering SonicWall Aventail SMA appliances from GMS is not supported.

- The **SMA | Management Panel | Register/Upgrades > Firmware Upgrade** screen provides the current status of the appliance and offers the option to Upgrade firmware from a local path or from the GMS server.

Events

- The **SMA | Management Panel | Events > Alert Settings** screen allows you to add, edit, or delete a Unit Status alert for managed SMA appliances.
- The **SMA | Management Panel | Events > Current Alerts** screen displays all active alerts for this appliance.

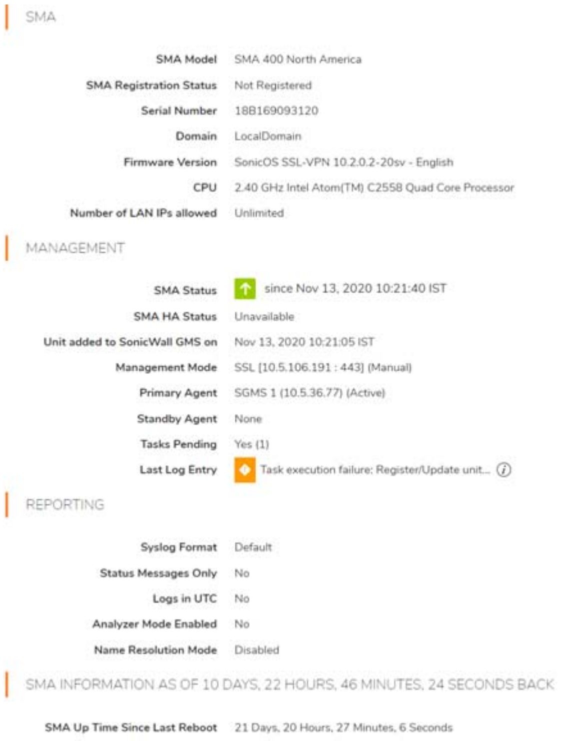
Managing SMA General Settings

To modify the general status and tools of an SMA appliance using ® (GMS), navigate to the **SMA | Management Panel | General page.** You will see the options **Status**, **Tools, Info,** and **Settings**. This section contains the following subsections:

- SMA Status
- SMA Tools
- SMA Info
- Saved Settings

SMA Status

The **SMA | Management Panel | General > Status** section provides the current status of the SMA appliance and allows for an instant update of appliance information using **Fetch Information**.



SMA

SMA Model	SMA 400 North America
SMA Registration Status	Not Registered
Serial Number	18B169093120
Domain	LocalDomain
Firmware Version	SonicOS SSL-VPN 10.2.0.2-20sv - English
CPU	2.40 GHz Intel Atom(TM) C2558 Quad Core Processor
Number of LAN IPs allowed	Unlimited

MANAGEMENT

SMA Status	↑ since Nov 13, 2020 10:21:40 IST
SMA HA Status	Unavailable
Unit added to SonicWall GMS on	Nov 13, 2020 10:21:05 IST
Management Mode	SSL [10.5.106.191 : 443] (Manual)
Primary Agent	SGMS 1 (10.5.36.77) (Active)
Standby Agent	None
Tasks Pending	Yes (1)
Last Log Entry	◆ Task execution failure: Register/Update unit... ⓘ

REPORTING

Syslog Format	Default
Status Messages Only	No
Logs in UTC	No
Analyzer Mode Enabled	No
Name Resolution Mode	Disabled

SMA INFORMATION AS OF 10 DAYS, 22 HOURS, 46 MINUTES, 24 SECONDS BACK

SMA Up Time Since Last Reboot	21 Days, 20 Hours, 27 Minutes, 6 Seconds

The **SMA | Management Panel| General > Status** section provides the following appliance information:

General > Status Information

SMA Status Item	Description
SMA Model	The SMA model number.
SMA Registration Status	The registration status of SMA.
Serial Number	The SMA serial number.
Domain	The SMA appliance domain.
Firmware Version	The SMA firmware version information.
CPU	The SMA CPU information.
Number of LAN IPs allowed	The number of LAN IPs allowed by the SMA.
SMA Status	The current status of the SMA appliance, either **Up**, **Down** or **Unacquired**.
SMA HA Status	The High Availability status of SMA.
Unit added to SonicWall GMS on	The date and time the SMA appliance was added to GMS.
Management Mode	The management mode used to access the SMA.
Primary Agent	The IP address of the primary agent.
Standby Agent	The IP address of the standby agent.
Tasks Pending	The number of tasks pending for the SMA.
Last Log Entry	The last SonicWall GMS system log event message for this device.
Syslog Format	The Syslog format of the SMA.
Status Message Only	The information of the status message.
Logs in UTC	The details of the logs in Coordinated Universal Time (UTC).
Analyzer Mode Enabled	If the analyzer mode is enabled for this appliance or not.
Name Resolution Mode	If the name resolution mode is enabled or disabled.
SMA Information	The up time since last reboot in days, hours, minutes, seconds.

Using Fetch Information

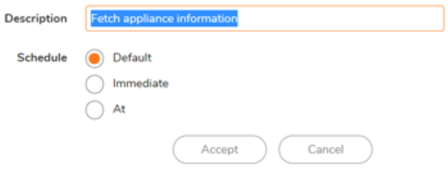
To update the SMA | Management Panel *| General > Status section using Fetch Information:*

1 Navigate to **SMA | Management Panel| General > Status.**

2 Click on the TreeControl Panel ☰ icon. The TreeControl Panel appears.

3 Select the desired SMA appliance from the TreeControl menu to view the status page.

4 Click **Fetch Information**. The update scheduler displays.



Description: Fetch appliance information

Schedule
- ● Default
- ○ Immediate
- ○ At

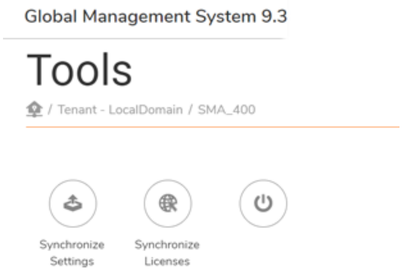
5 Select the required option. The options are **Default**, **Immediate,** or **At**. Alternatively, you can select **At** and specify a date and time for SonicWall GMS to execute the update.

6 Click **Accept**. It might take a few seconds for GMS to fetch the appliance information. The latest status is displayed under **SMA | Management Panel | General > Status**.

SMA Tools

The **SMA | Management Panel | General > Tools** section provides the following options: **Restart Appliance**, **Synchronize Settings**, **Synchronize Licenses**.

NOTE: The Restart Appliance option is not available for SonicWall Aventail SMA appliances.


Global Management System 9.3
Tools
/ Tenant - LocalDomain / SMA_400
Synchronize Settings
Synchronize Licenses

Restarting SMA

To restart the SMA appliance:

1. Navigate to **SMA | Management Panel| General > Tools.**
2. Click on the TreeControl Panel ☰ icon. The TreeControl Panel appears.
3. Select the desired SMA appliance from the TreeControl menu. The tools page appears.
4. Click ⏻. A confirmation pop-up displays.
5. Use the Scheduler to specify a date and time for SonicWall GMS to execute the update.
6. Click **OK** to restart the appliance. It might take a few minutes for the SMA to restart.

Synchronize Settings

If a change is made to a SonicWall appliance through any means other than through SonicWall GMS, GMS is notified of the change through the syslog data stream. After the syslog notification is received, SonicWall GMS schedules a task to synchronize its database with the local change. Auto-synchronization automatically occurs whenever SonicWall GMS receives a local change notification status syslog message from a SonicWall appliance.

You can also force synchronization at any time for a SonicWall appliance or a group of SonicWall appliances.

To synchronize the SMA appliance:

1. Navigate to **SMA | Management Panel| General > Tools.**
2. Click on the TreeControl Panel ☰ icon. The TreeControl Panel appears.
3. Select the desired SMA appliance from the TreeControl menu. The tools page appears.
4. Click **Synchronize Settings**. A confirmation pop-up displays.
5. Click **OK**.
6. Use the Scheduler to specify a date and time for SonicWall GMS to execute the update. It might take a few seconds for SMA to synchronize.

Synchronize Licenses

SonicWall appliances check their licenses and subscriptions with mysonicwall.com once every 24 hours. Using **Synchronize Licenses**, you can force the SonicWall SMA appliance to synchronize this information with mysonicwall.com immediately.

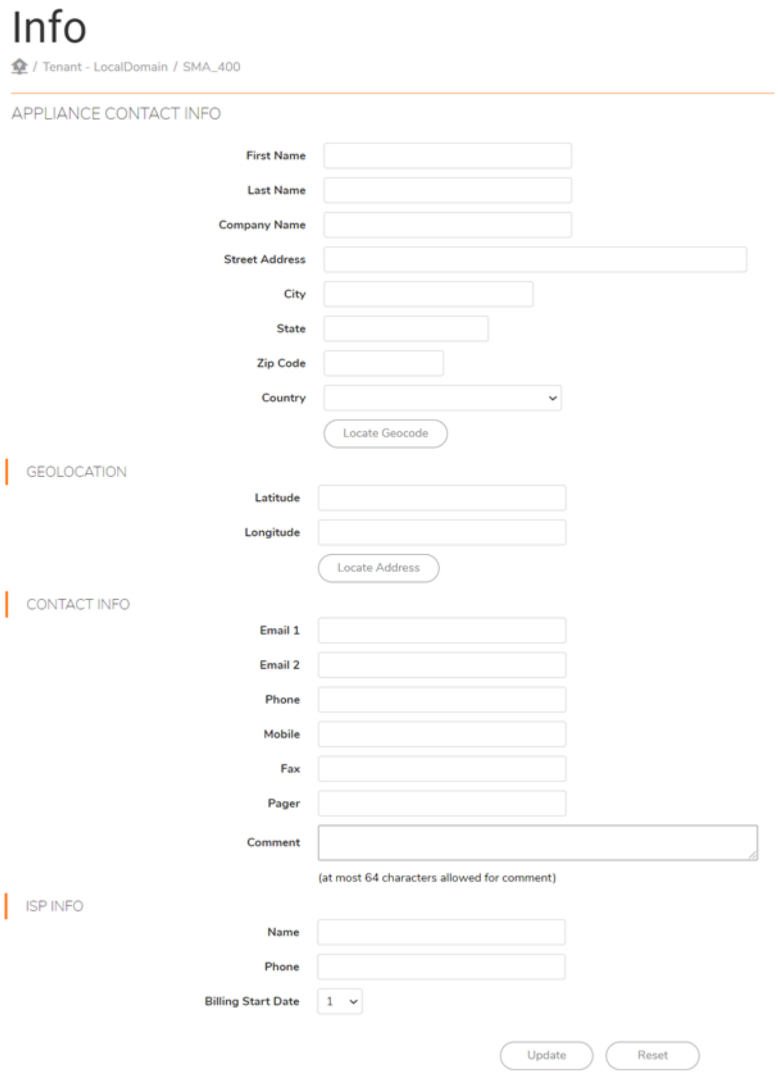
To synchronize the SMA appliance licenses with mysonicwall.com:

1. Navigate to **SMA | Management Panel| General > Tools.**
2. Click on the TreeControl Panel ☰ icon. The TreeControl Panel appears.
3. Select the desired SMA appliance from the TreeControl menu. The tools page appears.
4. Click **Synchronize Licenses**. A confirmation pop-up displays.
5. Click **OK**. The update scheduler displays.

6 Use the Scheduler to specify a date and time for SonicWall GMS to execute the update. It might take a few seconds for the SMA to synchronize with MySonicWall.com.

SMA Info

The SMA | Management Panel | General > Info section provides the ability to update the contact information for the SMA appliance.



Info

/ Tenant - LocalDomain / SMA_400

APPLIANCE CONTACT INFO

First Name
Last Name
Company Name
Street Address
City
State
Zip Code
Country

GEOLOCATION

Latitude
Longitude

CONTACT INFO

Email 1
Email 2
Phone
Mobile
Fax
Pager
Comment
(at most 64 characters allowed for comment)

ISP INFO

Name
Phone
Billing Start Date 1

Updating SMA Appliance Information

To update the SMA appliance information:

1 Navigate to **SMA | Management Panel | General > Info.**

2 Click on the TreeControl Panel ☰ icon. The TreeControl Panel appears.

3 Select the desired SMA appliance from the TreeControl menu. The info page appears.

4 Enter the appropriate information for each field.

5 Click **Update** to update the information, or **Reset** to clear the form and start over.

Settings

The **SMA | Management Panel| General > Settings** section provides the ability to view saved settings, store new settings, enable/disable settings file backup, and configure missed report settings. This section contains the following topics:

- Saved Settings
- Store New Settings
- File Backup Status
- File Backup Settings
- Configure Missed Reports Settings

Saved Settings

To configure saved settings:

1 Navigate to **SMA | Management Panel| General > Settings.**

2 Click on the TreeControl Panel ☰ icon. The TreeControl Panel appears.

3 Select the desired SMA appliance from the TreeControl menu. The settings page appears.

4 The **Saved Settings** section shows a list of currently saved settings and has the following options:

  - **Details of Saved Settings**
  - **Save the settings to a local file**
  - **Restore the settings to the unit**
  - **Delete the settings**

Store New Settings

To store new settings:

1. Navigate to **SMA | Management Panel| General > Settings.**
2. Click on the TreeControl Panel ☰ icon. The TreeControl Panel appears.
3. Select the desired SMA appliance from the TreeControl menu. The settings page appears.
4. Scroll to the **Store New Settings** section and enter a name for your saved settings in the **Name** field.
5. Click the radio button to select **Store settings read from unit** or **Store Settings from local file** and enter a file name in the local file field.
6. Click **Update** to save settings.

File Backup Status

To enable automatic file backup status:

1. Navigate to **SMA | Management Panel | General > Settings.**
2. Click on the TreeControl Panel ☰ icon. The TreeControl Panel appears.
3. Select the desired SMA appliance from the TreeControl menu. The settings page appears.
4. Scroll down to the **File Backup Status** section and click the checkbox next to **Enable Settings File Backup.**
5. Click **Update** to save settings.

File Backup Settings

To enable file backup settings:

1. Navigate to **SMA | Management Panel | General > Settings.**
2. Click on the TreeControl Panel ☰ icon. The TreeControl Panel appears.
3. Select the desired SMA appliance from the TreeControl menu. The settings page appears.
4. Scroll down to the **File Backup Settings** section and enter the number of newest setting files to be preserved.
5. Click **Update** to save settings.

ⓘ **NOTE:** The frequency of automatic settings backup is configured on the **CONSOLE | Management > Settings** page.

Configure Missed Reports Settings

To configure missed reports settings:

1. Navigate to **SMA | Management Panel | General > Settings.**

2 Click on the TreeControl Panel ☰ icon. The TreeControl Panel appears.

3 Select the desired SMA appliance from the TreeControl menu. The settings page appears.

4 Scroll down to the **Configure Missed Reports Settings** section and enter a number in the **Missed Reports Threshold** field.

> **NOTE:** Entering “0” will cause the unit to never be reported as down/red in GMS.

5 Click **Update** to save settings.

Registering/Upgrading

This chapter describes how to register SonicWall SMA appliances using GMS. **Register SSL-VPNs** is an option in the SMA view that registers your SMA using the account information you provided when you registered your GMS.

This chapter contains the following subsections:

- Registering SonicWall SSL-VPN Appliances
- Upgrading SonicWall SMA Firmware

Registering SonicWall SSL-VPN Appliances

> **NOTE:** Registering SonicWall Aventail SMA appliances from GMS is not supported.

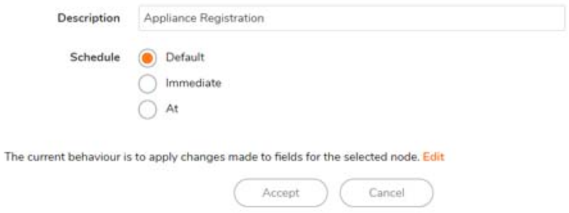
To register a SonicWall SSL-VPN using GMS:

1 Navigate to **SMA | Management Panel | Register/Upgrades > Register SSL-VPNs.**

2 Click on the TreeControl Panel ☰ icon. The TreeControl Panel appears.

3 Select the desired SMA appliance from the TreeControl menu. The current status page appears.

4 Click **Register** to open the appliance management interface. The update scheduler displays.



Description: Appliance Registration

Schedule: ● Default ○ Immediate ○ At

The current behaviour is to apply changes made to fields for the selected node. Edit

5 Select the options to schedule the registration. The options are **Default**, **Immediate** and **At**. Alternatively, you can select **At** and specify a date and time for SonicWall GMS to execute the update.

6 Click **Accept**. You will receive a notification that a task has been created/spooled for execution.

7 Click on the task to complete registration.

> **NOTE:** If you receive an error message, navigate to the **CONSOLE | Log > View Log**. A detailed error message is displayed.

Upgrading SonicWall SMA Firmware

The SonicWall SMA appliance must be registered before the firmware can be upgraded. For information about registering your SMA appliance, refer to Registering SonicWall SSL-VPN Appliances.

NOTE: Upgrading SonicWall Aventail SMA appliances from GMS is not supported.

To upgrade the firmware of a SonicWall SMA appliance using GMS:

1. Navigate to **SMA | Management Panel | Register/Upgrades > Firmware Upgrade.**
2. Click on the TreeControl Panel ☰ icon. The TreeControl Panel appears.
3. Select the desired SMA appliance from the TreeControl menu. The current SMA appliance firmware is displayed under **Current Status**.
4. To upgrade the SMA appliance firmware using a file on the GMS server, click **Upgrade from GMS Server**.
5. To upgrade the SMA appliance firmware using a local file, enter the path and file name of the firmware file in the field under the **Firmware Upgrade from Local File:** section, or click **Browse** to locate the firmware file.
6. Click **Upgrade firmware from local file**.
7. A message displays indicating that an appliance restart is necessary to complete the firmware upgrade. Click **OK** to continue. The license agreement message displays.
8. Read the message and click **OK** to agree and download the firmware, or click **Cancel** to disagree and cancel the firmware upgrade.

Logging in to SMA using SonicWall GMS

Before logging in to the SonicWall SMA using SonicWall GMS, make sure that pop-ups are enabled on your Web browser and use the procedure in this section.

To log in to a SonicWall SMA appliance using GMS:

1. Right-click on the unit from the GMS SMA TreeControl menu and select **Login to Unit.**
2. Enter the appliance credentials then navigate to the **SMA | Management Panel** view**.**
3. Click on the TreeControl Panel ☰ icon. The TreeControl Panel appears.
4. Select the desired SMA appliance from the TreeControl menu. Click **Yes** to the security certificate warning to continue.
5. The SMA management interface opens in a new browser window. This might take a few seconds. You can now manage the SonicWall SMA directly from the management interface.

NOTE: For detailed instructions about configuration tasks using the SonicWall SMA management interface, refer to the *SonicWall SMA Administration Guide*, available at https://support.sonicwall.com/sonicwall-secure-mobile-access/sma%206200/technical-documents.

Configuring Alerts

This chapter provides configuration procedures for adding, enabling / disabling, deleting, and editing the **SMA | Management Panel| Events > Alert Settings** page, at a unit or group level.

Topics:

- Configuring Alerts in the SMA View
- Enabling/Disabling/Deleting/Editing Alerts
- Deleting Alerts
- Editing Alerts
- Current Alerts

Configuring Alerts in the SMA View

This section details the configuration procedures for adding an alert, selecting an alert type, and configuring a Destination/Schedule.

Add Alert

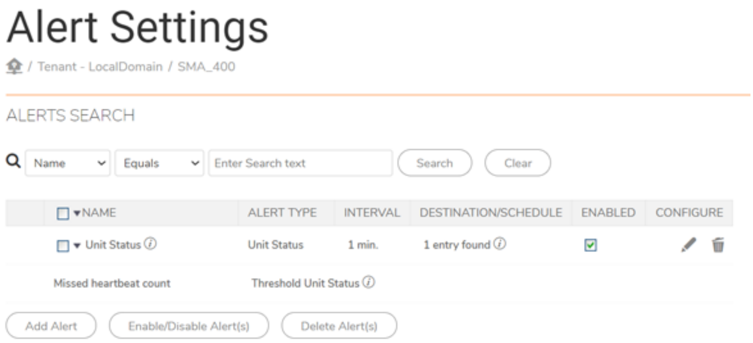
In the **Add Alert** panel you can enter an alert name and description, select the options for visible to non-administrators and disable, and enter the polling interval.

To add an alert:

1 Navigate to **SMA | Management Panel | Events > Alert Settings.**

2 Click on the TreeControl Panel ☰ icon. The TreeControl Panel appears.

3 Select the desired SMA appliance from the TreeControl menu. The **Alert Settings** page appears.



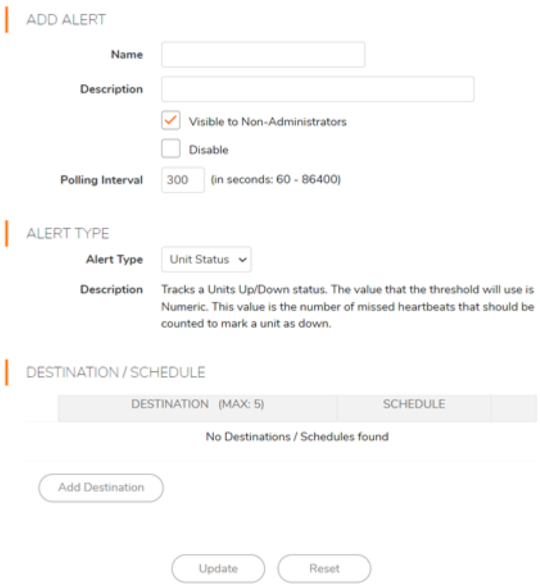
Alert Settings

/ Tenant - LocalDomain / SMA_400

ALERTS SEARCH

	☐ ▾NAME	ALERT TYPE	INTERVAL	DESTINATION/SCHEDULE	ENABLED	CONFIGURE
	☐ ▾ Unit Status ⓘ	Unit Status	1 min.	1 entry found ⓘ	☑	
	Missed heartbeat count	Threshold Unit Status ⓘ				

4 Click **Add Alert**. The Add Alert screen displays.



ADD ALERT

Name

Description

☑ Visible to Non-Administrators

□ Disable

Polling Interval 300 (in seconds: 60 - 86400)

ALERT TYPE

Alert Type: Unit Status

Description: Tracks a Units Up/Down status. The value that the threshold will use is Numeric. This value is the number of missed heartbeats that should be counted to mark a unit as down.

DESTINATION / SCHEDULE

DESTINATION (MAX: 5)	SCHEDULE
No Destinations / Schedules found	

5 Enter a name and description for your alert.

6 Select **Visible to Non-Administrators** if you want your alert to be visible to non-administrators.

7 Select the **Disable** check-box to disable this alert.

8 Enter a **Polling Interval** value (in seconds: 60-86400).

Alert Type

In the Alert Type panel you can select an alert type from the provided list and view the definitions of each alert type.

To configure an Alert Type:

1 Click the **Alert Type** pull-down list and select an alert type. The table that follows displays all the SMA Alert Types and definitions of each alert.

SMA Alert Types and Definitions

Name	Description
Unit Status	Tracks a Units Up/Down status. The value that the threshold uses is Numeric. This value is the number of missed heartbeats that should be counted to mark a unit as down. Optionally, the **Edit Content** option is available.

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

If the Alert Type requires you to Edit Content, an icon displays in the Alert Type panel. Editing Contents allows the user to pick additional information, in a granular fashion, on which the alerting has to be completed.

2 Click the **Edit Content** Link. The **Edit Contents for Alert Type Unit Status** pop-up window displays.

3 Click the **Threshold** pull-down list and select a threshold.

> ⓘ **NOTE:** You can create a new threshold on-the-fly by clicking the icon. Only one new threshold can be created in this feature.

4 To save the alert, click **Update.** To reset the settings, click **Reset**.

Destination/Schedule

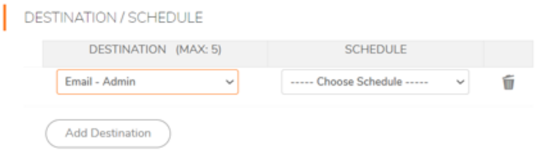
In the Destination/Schedule panel of the Add Alert pop-up, you can add up to five destinations and set a schedule for each.

To add a destination and set a schedule:

> ⓘ **NOTE:** Every selected destination is required to have a schedule set.

1 Click the **Add Destination** link under the Destination/Schedule section.

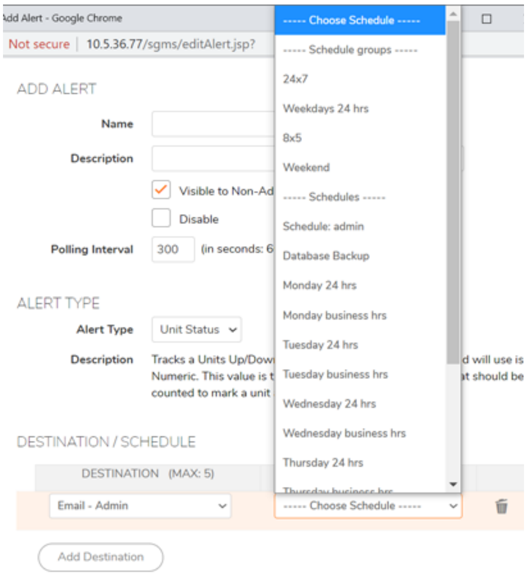
2 Click the **Destination** pull-down list, then select an alert destination. The Destination field designates where you want alerts to be sent. You have a maximum number of five destinations.



DESTINATION / SCHEDULE

DESTINATION (MAX: 5)	SCHEDULE
Email - Admin	----- Choose Schedule -----

3 Click the **Schedule** pull-down list, then select a schedule type. The Schedule field designates the frequency of when you want alerts to be sent to the destination.



Add Alert - Google Chrome

Not secure | 10.5.36.77/sgms/editAlert.jsp?

ADD ALERT

Name

Description

☑ Visible to Non-Ad

□ Disable

Polling Interval 300 (in seconds: 6

ALERT TYPE

Alert Type Unit Status

Description Tracks a Units Up/Dow... Numeric. This value is t... counted to mark a unit ... d will use is ... t should be

DESTINATION / SCHEDULE

DESTINATION (MAX: 5)	
Email - Admin	----- Choose Schedule -----

4 Click **Update** to finish adding an alert.

Enabling/Disabling/Deleting/Editing Alerts

In the Enabling/Disabling panel of the Add Alert pop-up, you can enable, disable, delete, or edit an alert.

Enabling an Alert

To enable an alert:

1. Navigate to **SMA | Management Panel | Events > Alert Settings.** The **Alert Settings** page appears.
2. Click on the TreeControl Panel ☰ icon. The TreeControl Panel appears.
3. Select the desired SMA appliance from the TreeControl menu.
4. Select the **Enabled** checkbox next to the alerts you wish to enable.
5. Click the **Enable/Disable Alert(s)** button. A confirmation window displays.
6. Click **OK**.

Disabling an Alert

To disable an alert:

1. Navigate to **SMA | Management Panel | Events > Alert Settings.**
2. Click on the TreeControl Panel ☰ icon. The TreeControl Panel appears.
3. Select the desired SMA appliance from the TreeControl menu. The Alert Settings page appears.
4. Deselect **Enabled** for the alert(s) you wish to disable.
5. Click the **Enable/Disable Alert(s)** link. A confirmation window displays.
6. Click **OK**.

Deleting Alerts

To delete an alert:

1. Navigate to **SMA | Management Panel | Events > Alert Settings.** The Alert Settings page appears.
2. Click on the TreeControl Panel ☰ icon. The TreeControl Panel appears.
3. Select the desired SMA appliance from the TreeControl menu.
4. Select the check box of the Alerts you wish to delete.
5. Click the **Delete Alert(s)** button. A confirmation window displays.
6. Click **OK**.

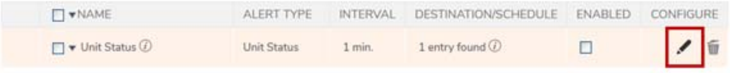
> ⓘ **NOTE:** You can also delete an alert by clicking the Delete icon under the Configure section of the alert you wish the delete.

Editing Alerts

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

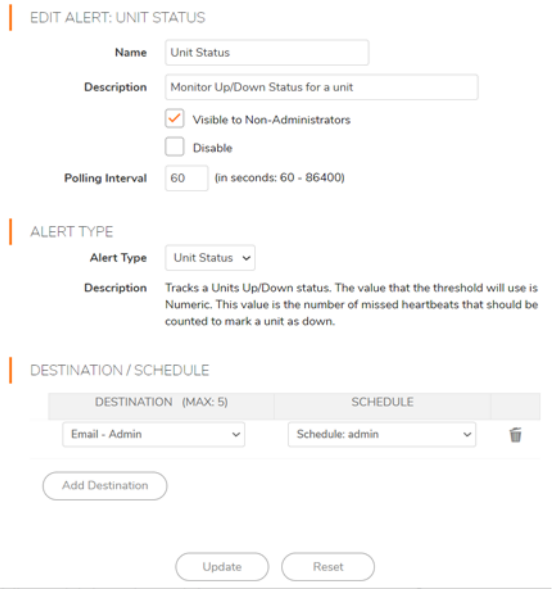
To edit an alert:

1. Navigate to **SMA | Management Panel | Events > Alert Settings.** The Alert Settings page appears.
2. Click on the TreeControl Panel ☰ icon. The TreeControl Panel appears.
3. Select the desired SMA appliance from the TreeControl menu.
4. Click the **Configure** icon of the alert you wish to edit.



□ ▾NAME	ALERT TYPE	INTERVAL	DESTINATION/SCHEDULE	ENABLED	CONFIGURE
□ ▾ Unit Status ⓘ	Unit Status	1 min.	1 entry found ⓘ	□	✎ 🗑

The **Edit Alert** page displays.



EDIT ALERT: UNIT STATUS

Name: Unit Status

Description: Monitor Up/Down Status for a unit

☑ Visible to Non-Administrators

□ Disable

Polling Interval: 60 (in seconds: 60 - 86400)

ALERT TYPE

Alert Type: Unit Status

Description: Tracks a Units Up/Down status. The value that the threshold will use is Numeric. This value is the number of missed heartbeats that should be counted to mark a unit as down.

DESTINATION / SCHEDULE

DESTINATION (MAX: 5)	SCHEDULE	
Email - Admin	Schedule: admin	🗑

5. Refer to Configuring Alerts in the SMA View and follow the configuration procedures to edit an existing Alert.

Current Alerts

To check the status of current alerts for your SonicWall SMA appliance or group of appliances:

1. Navigate to **SMA | Management Panel| Events > Current Alerts.**
2. Click on the TreeControl Panel ☰ icon. The TreeControl Panel appears.
3. Select the desired SMA appliance from the TreeControl menu. The Current Alerts page appears. All active alerts for this appliance are listed under Alert Listing.

2

Managing SMA Reports

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

This chapter contains the following sections:

- SMA Reporting Overview
- Using and Configuring SMA Reporting
- Viewing SMA Summary Reports
- Viewing SMA Unit-Level Reports
- Viewing SMA Log Analyzer
- Events
- Current Alerts

SMA Reporting Overview

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

- SMA Reports Tab
- What is SMA Reporting?
- Benefits of SMA Reporting
- How Does SMA Reporting Work?

The GMS SMA Reporting Overview section helps you to understand the main steps to be taken in order to create and customize reports successfully.

SMA Reports Tab

The SMA tab gives you access to the Secure Mobile Access (SMA) Reports section of the GMS management interface. Reporting supports both graph and non-graph reports, and allows you to filter data according to your business requirements.

What is SMA Reporting?

Secure Mobile Access (SMA) reporting allows you to configure and design your reports according to your business requirements. This feature offers various types of static and dynamic reporting that you can customize.

SonicWall GMS SMA reporting provides a visual presentation of User connectivity activity, Up-Down status, and other reports related to remote access. With SMA reporting, you can view your reports in enhanced graphs, create granular and custom reports and scheduled reports, and search for reports using the search bar tool.

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

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

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

Benefits of SMA Reporting

SMA reports provide visibility into the resource use by the users, leading to policies that enhance the user experience and the productivity of employees.

The following capabilities contribute to the benefits of the SMA reporting feature:

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

How Does SMA Reporting Work?

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

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

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

Using and Configuring SMA Reporting

This section describes how to use and configure SMA reporting:

- Viewing Available SMA Report Types
- Configuring SMA Scheduled Reports

Viewing Available SMA Report Types

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

1. Log into your GMS management console.
2. Navigate to the **SMA | Reports** tab. The following types of reports are available:

For E-Class SMA series appliances

Group Level Reports:

- Data Usage
  - Summary: connections per SMA appliance
- WAF
  - Summary: connections listed by appliance for one day (default)
- Connections
  - Summary: offloaded connections listed by appliance for one day (default)
- Events
  - Alert Settings: list of alerts, interval, destination, and configuration details
  - Current Alerts: list of alerts with their severity, names, descriptions, and connectwise ticket

Unit Level Reports:

Click on the hyperlinks in the Unit Level Reports to view the Analyzer Log with more information.

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

    - Users Prevented: Number of blocked users prevented per day
- Connections
    - Timeline: connections, peak connections, average connections, and peak throughputs in Mbps
    - Applications: the application IP, URI, and connection details
    - Users: user details with agent and connections
- Up/Down Status
    - Timeline: uptime and downtime by hour for one day
- Custom Reports
    - Manage Reports: manage custom reports
- Analyzers
    - Log Analyzer: logs of all activity
- Configuration: allow setting Report display options
    - Syslog Filter: applies filters to the system logs uploaded to the reporting database
- Events: allow setting options
    - Alert Settings: provides search functions, adding or removing Alerts
    - Current Alerts: displays current applicable Alerts

For SMA series appliances:

Group Level Reports:

- Data Usage
    - Summary: connections per SMA appliance
- WAF
    - Summary: connections listed by appliance for one day (default)
- Connections
    - Summary: offloaded connections listed by appliance for one day (default)
- Events
    - Alert Settings: list of alerts, interval, destination, and configuration details
    - Current Alerts: list of alerts with their severity, names, descriptions, and connectwise ticket

Unit Level Reports:

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

- Data Usage
    - Timeline: total connections listed by hour
    - Users: connections listed by user
- User Activity
    - Details: a detailed report of activity for the specified user
- Access Method
    - Summary: connections per connection protocol (HTTPS, NetExtender, and so on.)

    - Users: top users by protocol
- Authentication
    - User login: authenticated user logins by time and IP protocol. User Login reports combine admin users with all other users in the same report.
    - Failed login: Failed login attempts with initiator IP address.
- WAF
    - Timeline: Total threats detected per appliance
    - Threats Detected: Top threats detected per day
    - Threats Prevented: Top threats prevented per day
    - Apps Detected: Top applications detected per day
    - Apps Prevented: Top applications blocked per day
    - Users Detected: Number of concurrent users per day
    - Users Prevented: Number of blocked users prevented per day
- Connections
    - Timeline: a summary of offloaded connections under the group node per SMA appliance, listed for one day.
    - Applications: offloaded connections by application
    - Users: offloaded connections by user
- Up/Down Status
    - Timeline: uptime and downtime by hour for one day
- Custom Reports
    - Manage Report: manage your custom reports
- Analyzers
    - Log Analyzer: logs of all activity
- Configuration: allow setting Report display options
    - Syslog Filter: applies filters to the system logs uploaded to the reporting database
- Events: allow setting options
    - Alert Settings: provides search functions, adding or removing Alerts
    - Current Alerts: displays current applicable Alerts

ⓘ **NOTE:** You can use the Date Selector to select reports covering other intervals than those listed here.

Configuring SMA Scheduled Reports

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

To configure SMA scheduled reports and summarization, log into the Universal Scheduled Reports interface and click on the **Schedule Report** icon to view the Universal Scheduled Report menu.

Navigating Through Detailed SMA Reports

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

Drillable reports give access to additional information by clicking on hyperlinks to go to the Detail view. Data filtering can be applied either by using the Filter Bar, drilling down through hyperlinked data, or applying a filter to a drillable data column.

Viewing SMA Summary Reports

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

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

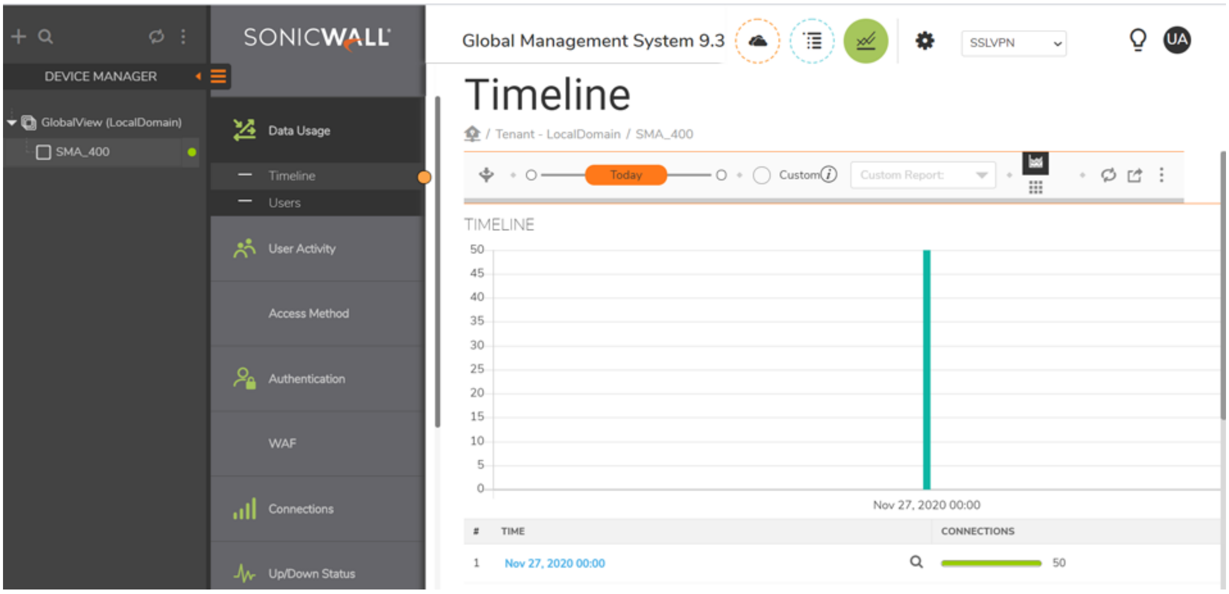
You can also do the following:

- Click ✣ to filter data.
- Click ⟳ to reload the page.
- Click ↗ to export the data into PDF, XML, or CSV formats.
- Click ⋮ to go to **Schedules** or **Archives**.

To view the Data Usage Summary report:

1. Navigate to **SMA | Syslogs Panel**.
2. Click on the TreeControl Panel ☰ icon. The TreeControl Panel appears.
3. Select the **GlobalView** icon and choose a group from the TreeControl menu to view the reports.

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



#	TIME	CONNECTIONS
1	Nov 27, 2020 00:00	50

Viewing SMA Unit-Level Reports

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

Topics:

- Viewing Unit-Level Data Usage Reports
- Viewing SMA Top Users Reports
- Viewing Access Method Reports
- Viewing SMA Authentication User Login Report
- Viewing SMA Authentication Failed Login Report
- Viewing Web Application Firewall (WAF) Reports
- Viewing Connection Reports

Viewing Unit-Level Data Usage Reports

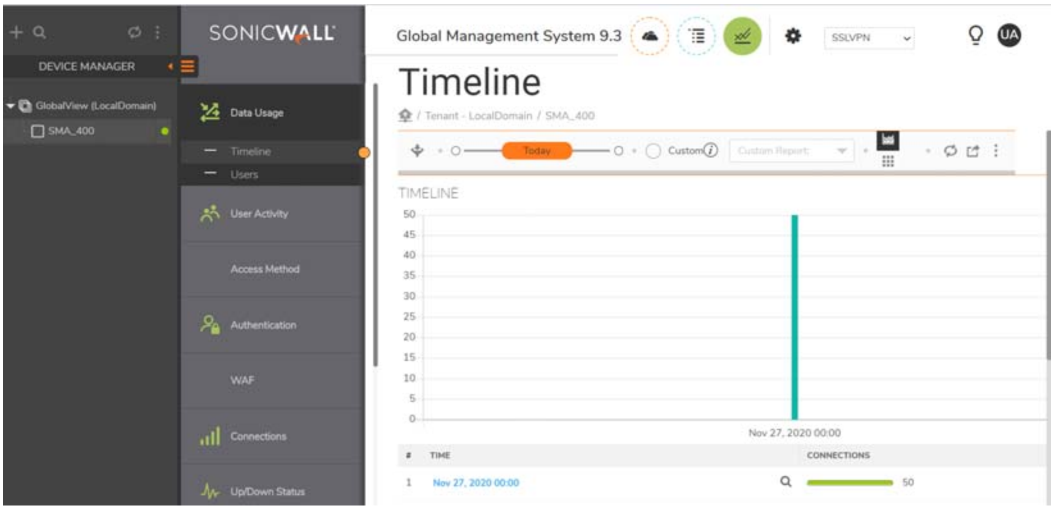
To view the data usage timeline:

1 Navigate to **SMA | Syslogs Panel | Data Usage > Timeline.** The timeline report displays.

2 Click on the TreeControl Panel ☰ icon. The TreeControl Panel appears.

3 Select the desired Unit in the TreeControl menu.

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



#	TIME	CONNECTIONS
1	Nov 27, 2020 00:00	50

The timeline contains the following information:

- **Time**—when the sample was taken.
- **Connections**—number of connections to the SMA appliance.

5 To change the interval of the report, use the left arrow on the **Time Bar** to click back a day at a time, or select **Custom** to access the calendar for customizing the date or date range.

6 Select a reporting interval from the drop-down menu, choose a start and end date, then select number of rows from the drop-down.

7 Click **OK** to perform search The GMS Reporting Module displays the report for the selected day.

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

8 Click **CANCEL** to close the menu and return to the summary page.

Viewing SMA Top Users Reports

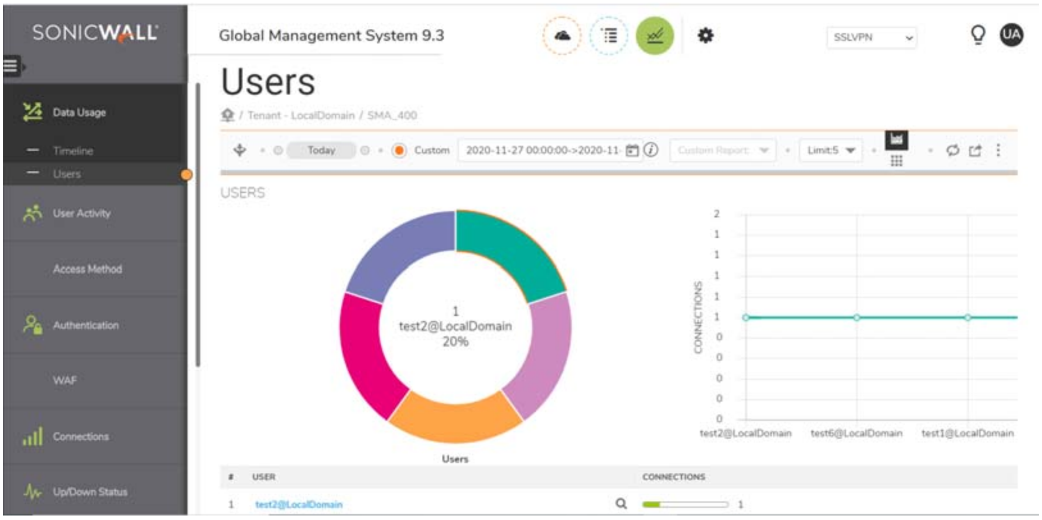
The Top Users report displays the users who used the most connections on the specified date.

To view the Top Users report:

1 Navigate to **SMA | Syslogs Panel | Data Usage > Users.**

2 Click on the TreeControl Panel icon. The TreeControl Panel appears.

3 Select the desired SMA appliance from the TreeControl menu. The Top Users page displays.



#	USER	CONNECTIONS
1	test2@LocalDomain	1

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

The table contains the following information for all users:

- **User**—the user name
- **Connections**—number of connection events or "hits"

By default, the GMS Reporting Module shows yesterday's report, a pie chart for the top six users, and a table for all users. To change the date of the report, click **Custom** to access the pull-down calendar. You can customize the date or date range if required.

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

> ⓘ **NOTE:** This report allows you to drill down by user. Click on a user in either the chart or grid to view the Log Analyzer.

Viewing User Activity Logs

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

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

You can also do the following:

- Click to save the reports.
- Click to remove all the filters.

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

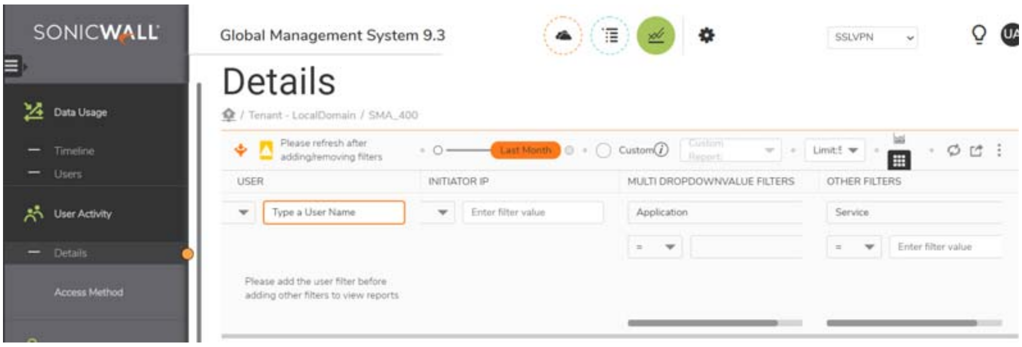
To create a new report:

1 Navigate to **SMA | Syslogs Panel | User Activity > Details**.

2 Click on the TreeControl Panel icon. The TreeControl Panel appears.

3 Select the desired SMA appliance from the TreeControl menu.

4 The **User Activity Analyzer** appears. The User Activity Analyzer generates a Detail report based on the user name.



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

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

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

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

Viewing Access Method Reports

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

Viewing the Access Summary Report

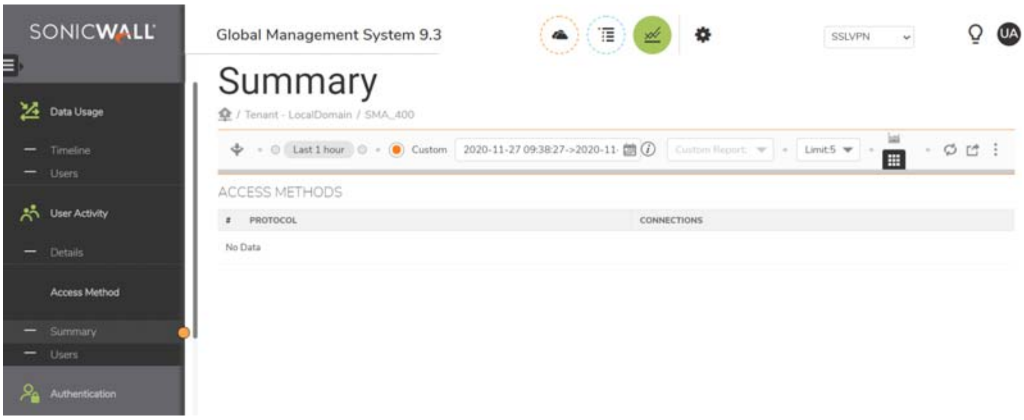
The Access Summary report provides an overview of the types of access protocols used. Click on a protocol hyperlink entry to view the Log Analyzer for more details.

To view the Summary Report:

1 Navigate to **SMA | Syslogs Panel | Access Method > Summary**.

2 Click on the TreeControl Panel icon. The TreeControl Panel appears.

3 Select the desired SMA appliance from the TreeControl menu. The Access Method Summary page appears.



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

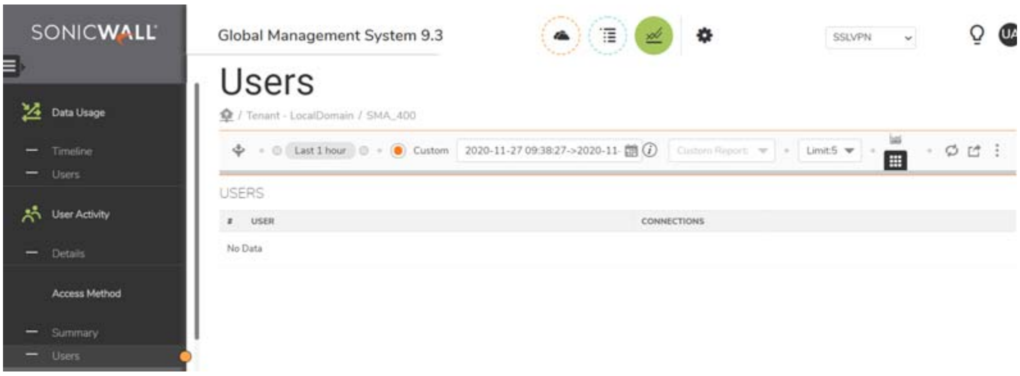
Viewing the Top Users Access Report

To view the top users access report:

1 Navigate to **SMA | Syslogs Panel | Access Method > Users.**

2 Click on the TreeControl Panel icon. The TreeControl Panel appears.

3 Select the desired SMA appliance from the TreeControl menu. The Top Users report appears.



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

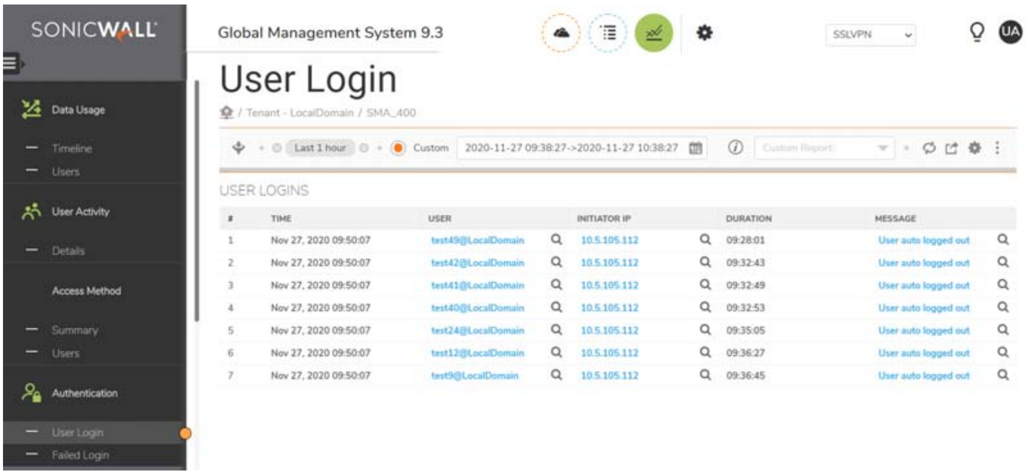
Alternatively, you can hover your mouse over a user in the User column of the grid view, then right click to filter results. For full details on that user, drill down by clicking on the user name in the column.

Viewing SMA Authentication User Login Report

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

To view the User Login Report:

1. Navigate to **SMA | Syslogs Panel | Authentication > User Login.**
2. Click on the TreeControl Panel icon. The TreeControl Panel appears.
3. Select the desired SMA appliance from the TreeControl menu. The Authenticated User Login report appears.



User Login

/ Tenant - LocalDomain / SMA_400

Last 1 hour ● Custom 2020-11-27 09:38:27->2020-11-27 10:38:27

USER LOGINS

#	TIME	USER	INITIATOR IP	DURATION	MESSAGE
1	Nov 27, 2020 09:50:07	test49@LocalDomain	10.5.105.112	09:28:01	User auto logged out
2	Nov 27, 2020 09:50:07	test42@LocalDomain	10.5.105.112	09:32:43	User auto logged out
3	Nov 27, 2020 09:50:07	test41@LocalDomain	10.5.105.112	09:32:49	User auto logged out
4	Nov 27, 2020 09:50:07	test40@LocalDomain	10.5.105.112	09:32:53	User auto logged out
5	Nov 27, 2020 09:50:07	test24@LocalDomain	10.5.105.112	09:35:05	User auto logged out
6	Nov 27, 2020 09:50:07	test12@LocalDomain	10.5.105.112	09:36:27	User auto logged out
7	Nov 27, 2020 09:50:07	test9@LocalDomain	10.5.105.112	09:36:45	User auto logged out

ⓘ **NOTE:** All reports appear in the appliance's time zone.

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

The Report contains the following information:

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

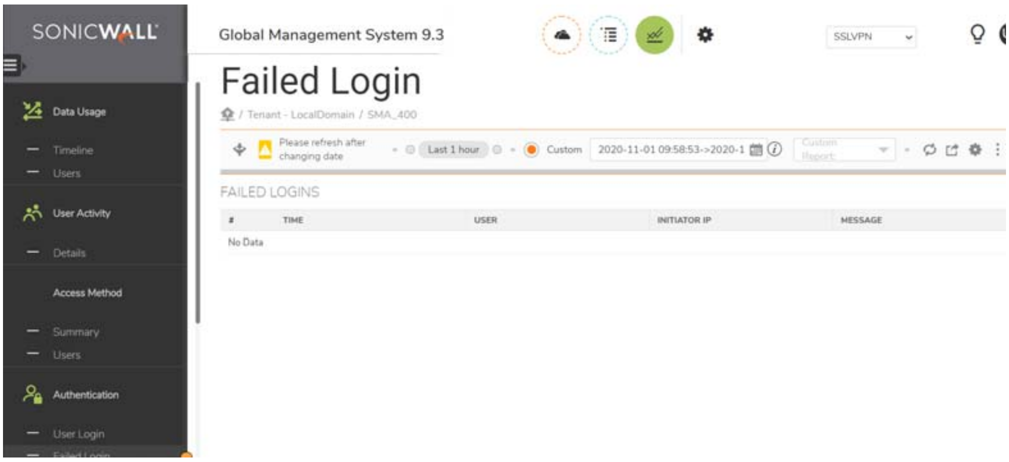
Viewing SMA Authentication Failed Login Report

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

To view SMA Authentication Failed Login Reports:

1. Navigate to **SMA | Reports | Authentication > Failed Login.**
2. Click on the TreeControl Panel icon. The TreeControl Panel appears.

3 Select the desired SMA appliance from the TreeControl menu. The Failed Logins report appears.



Failed Login

/ Tenant - LocalDomain / SMA_400

FAILED LOGINS

#	TIME	USER	INITIATOR IP	MESSAGE
No Data				

NOTE: All reports appear in the appliance’s time zone.

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

The Report contains the following information:

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

Viewing Web Application Firewall (WAF) Reports

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

The Web Application Firewall provides the following Reports:

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

Click on hyperlinks in these reports to view the Log Analyzer, for more details.

To view reports:

1 Navigate to **SMA | Syslogs Panel | WAF** and select an option from the available reports.

2 Click on the TreeControl Panel ☰ icon. The TreeControl Panel appears.

3 Select the desired SMA appliance from the TreeControl menu. The selected report appears.

Viewing Connections Timeline

The WAF Connections Timeline displays connections to the web firewall over time.

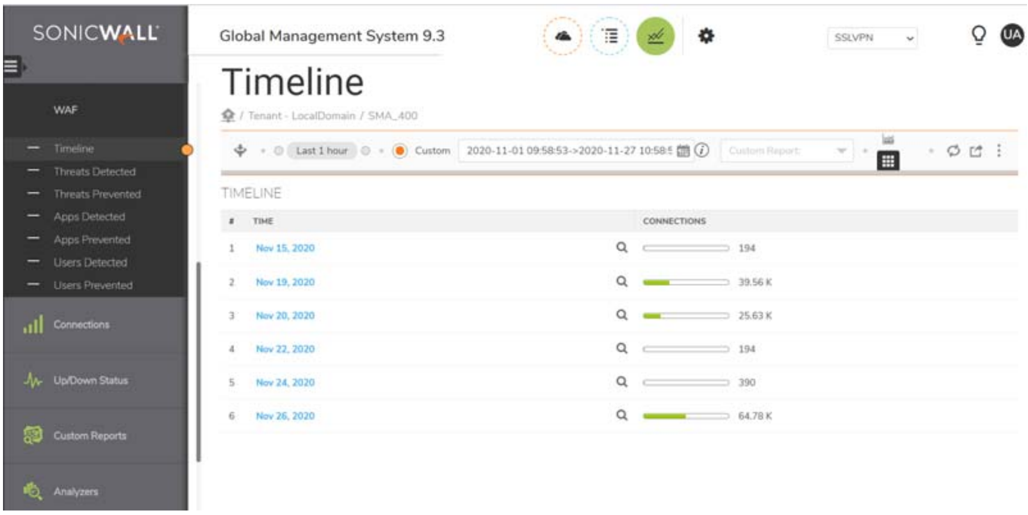
To view the Web Application Firewall Timeline Summary report:

1 Navigate to **SMA | Syslogs Panel | WAF > Timeline.**

2 Click on the TreeControl Panel ☰ icon. The TreeControl Panel appears.

3 Select the desired SMA appliance from the TreeControl menu. The Timeline report appears.

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



Timeline

/ Tenant - LocalDomain / SMA_400

2020-11-01 09:58:53->2020-11-27 10:58:5

TIMELINE

#	TIME	CONNECTIONS
1	Nov 15, 2020	194
2	Nov 19, 2020	39.56 K
3	Nov 20, 2020	25.63 K
4	Nov 22, 2020	194
5	Nov 24, 2020	390
6	Nov 26, 2020	64.78 K

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

Viewing WAF Top Threats Detected

The Threats Detected report displays the threats detected, according to signature, classification, and severity.

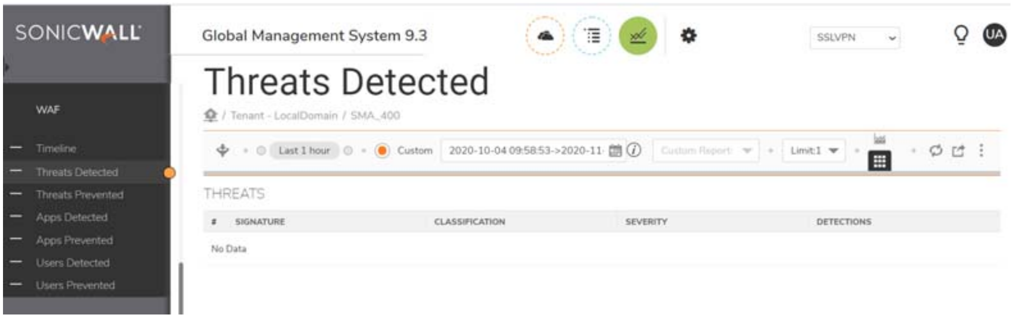
To view the Web Application Firewall Top Threats Detected report:

1 Navigate to **SMA | Syslogs Panel | WAF > Threats Detected.**

2 Click on the TreeControl Panel ☰ icon. The TreeControl Panel appears.

3 Select the desired SMA appliance from the TreeControl menu. The Threats Detected report appears.

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



Threats Detected

/ Tenant - LocalDomain / SMA_400

THREATS

#	SIGNATURE	CLASSIFICATION	SEVERITY	DETECTIONS
No Data				

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

Viewing WAF Top Threats Prevented

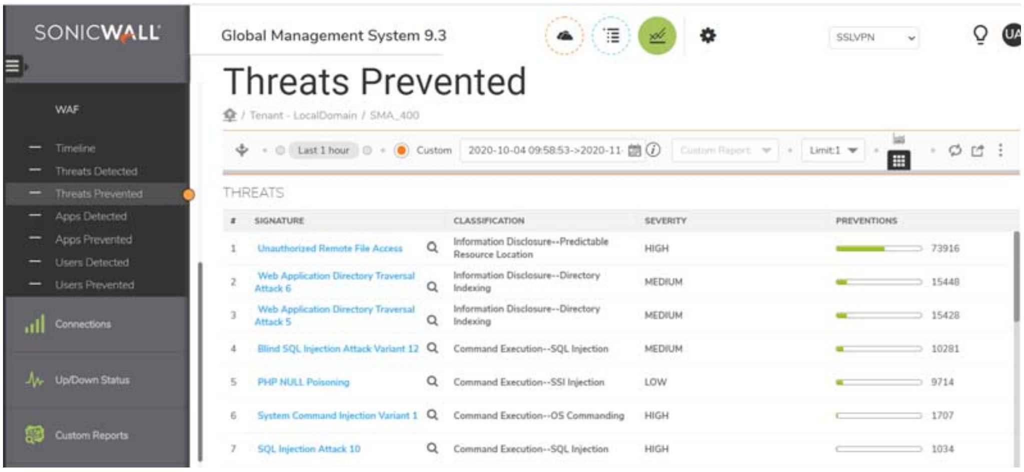
To view the Web Application Firewall Top Threats Prevented report:

1 Navigate to **SMA | Syslogs Panel | WAF > Threats Prevented.**

2 Click on the TreeControl Panel ☰ icon. The TreeControl Panel appears.

3 Select the desired SMA appliance from the TreeControl menu. The Top Threats Prevented report appears.

The Top Threats Prevented view shows Top Threats detected and prevented by the web firewall, with details on the Threat Signature, Threat Classification, Threat Severity, and Prevention.



Threats Prevented

/ Tenant - LocalDomain / SMA_400

THREATS

#	SIGNATURE	CLASSIFICATION	SEVERITY	PREVENTIONS
1	Unauthorized Remote File Access	Information Disclosure--Predictable Resource Location	HIGH	73916
2	Web Application Directory Traversal Attack 6	Information Disclosure--Directory Indexing	MEDIUM	15448
3	Web Application Directory Traversal Attack 5	Information Disclosure--Directory Indexing	MEDIUM	15428
4	Blind SQL Injection Attack Variant 12	Command Execution--SQL Injection	MEDIUM	10281
5	PHP NULL Poisoning	Command Execution--SSI Injection	LOW	9714
6	System Command Injection Variant 1	Command Execution--OS Commanding	HIGH	1707
7	SQL Injection Attack 10	Command Execution--SQL Injection	HIGH	1034

Viewing WAF Top Applications Detected

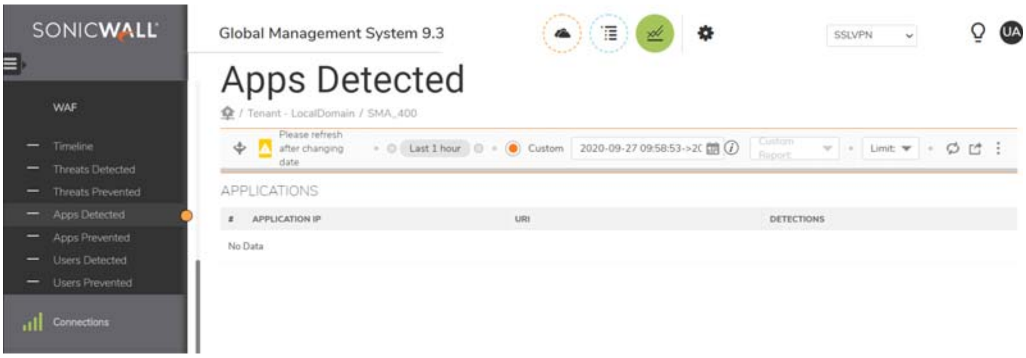
To view the Web Application Firewall Top Applications Detected report:

1 Navigate to **SMA | Syslogs Panel | WAF > Apps Detected.**

2 Click on the TreeControl Panel ☰ icon. The TreeControl Panel appears.

3 Select the desired SMA appliance from the TreeControl menu. The Apps Detected report appears.

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



Apps Detected

/ Tenant - LocalDomain / SMA_400

APPLICATIONS

#	APPLICATION IP	URI	DETECTIONS
No Data			

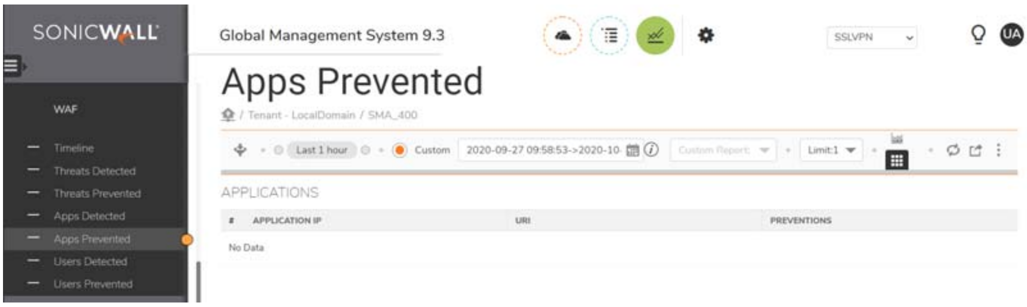
Click on the hyperlinks available in this report to view the Log Analyzer.

Viewing WAF Top Applications Prevented

To view the Web Application Firewall Top Applications Prevented report:

1. Navigate to **SMA | Syslogs Panel | WAF > Apps Prevented.**
2. Click on the TreeControl Panel ☰ icon. The TreeControl Panel appears.
3. Select the desired SMA appliance from the TreeControl menu. The Apps Prevented report appears.

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



Apps Prevented

/ Tenant - LocalDomain / SMA_400

APPLICATIONS

#	APPLICATION IP	URI	PREVENTIONS
No Data			

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

Viewing WAF Top Users Detected

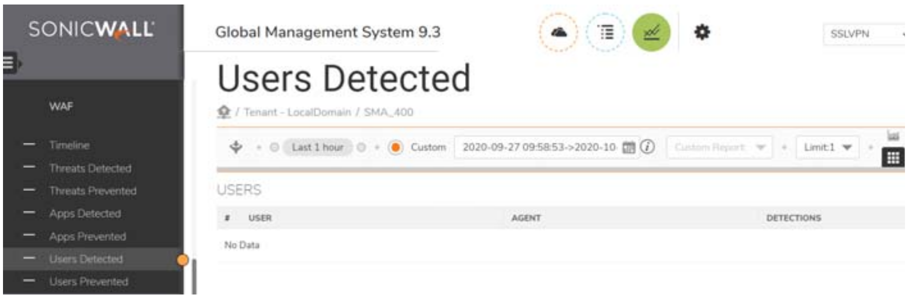
The Top Users Detected report lists the top authenticated users from whom threats have been detected by the Web firewall. It displays the User Name, User Agent and the Detections in order of the number of detections.

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

To view the Top Users report:

1. Navigate to **SMA | Syslogs Panel | WAF > Users Detected.**
2. Click on the TreeControl Panel ☰ icon. The TreeControl Panel appears.

3 Select the desired SMA appliance from the TreeControl menu. The Top Users Detected page displays.



Users Detected

USERS

#	USER	AGENT	DETECTIONS
No Data			

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

5 The table contains the following information by default:

- **Users**—the user's login. You can drill down to learn the IP address of the user.
- **Agent**—the User agent and version being used.
- **Detections**—the number of VPN connections in order of number of detections.
- **MBytes**—the number of megabytes transferred.

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

Viewing WAF Top Users Prevented

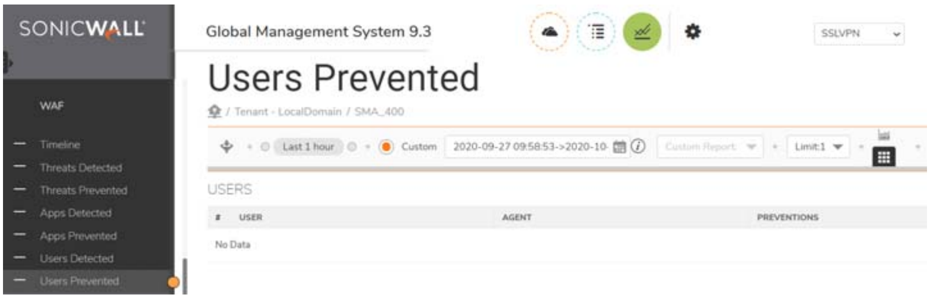
To view the Web Application Firewall Top Users Prevented report:

1 Navigate to **SMA | Syslogs Panel | WAF > Users Prevented.**

2 Click on the TreeControl Panel ☰ icon. The TreeControl Panel appears.

3 Select the desired SMA appliance from the TreeControl menu. The Top Users Prevented page displays.

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



Users Prevented

USERS

#	USER	AGENT	PREVENTIONS
No Data			

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

Viewing Connection Reports

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

Viewing the Offloaded Connection Timeline

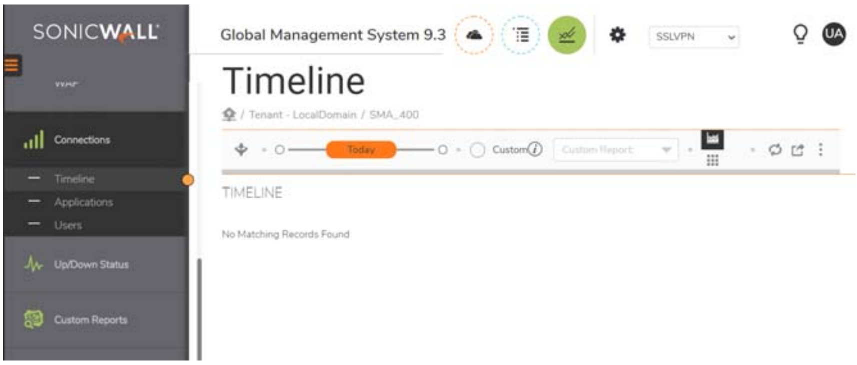
The Offloaded Connection Summary report lists the total connections made for all offloaded applications for one day, displayed per hour per day. The grid section displays peak connections per second, peak throughput, average connections per second, and average throughput per hour.

To view the Offloaded Connections Timeline report:

1 Navigate to **SMA | Syslogs Panel | Connections > Timeline.**

2 Click on the TreeControl Panel icon. The TreeControl Panel appears.

3 Select the desired SMA appliance from the TreeControl menu. The Offloaded Connections Timeline Summary report displays.



Timeline

/ Tenant - LocalDomain / SMA_400

TIMELINE

No Matching Records Found

Viewing the Offloaded Connections Top Applications Report

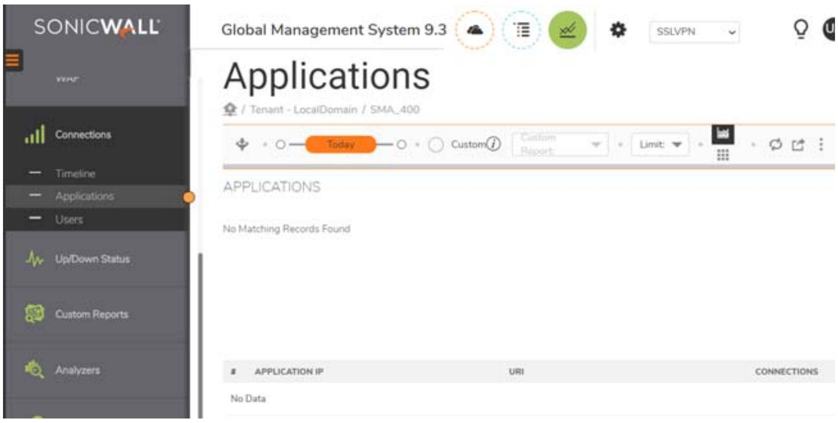
The Top Applications report lists those applications having the most offloaded connections, as well as information about the application and throughput.

To view the report:

1 Navigate to **SMA | Syslogs Panel | Connections > Applications.**

2 Click on the TreeControl Panel icon. The TreeControl Panel appears.

3 Select the desired SMA appliance from the TreeControl menu. The Offloaded Connections Top Applications Summary report displays.



#	APPLICATION IP	URI	CONNECTIONS
No Data			

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

Viewing the Offloaded Connections Top Users Report

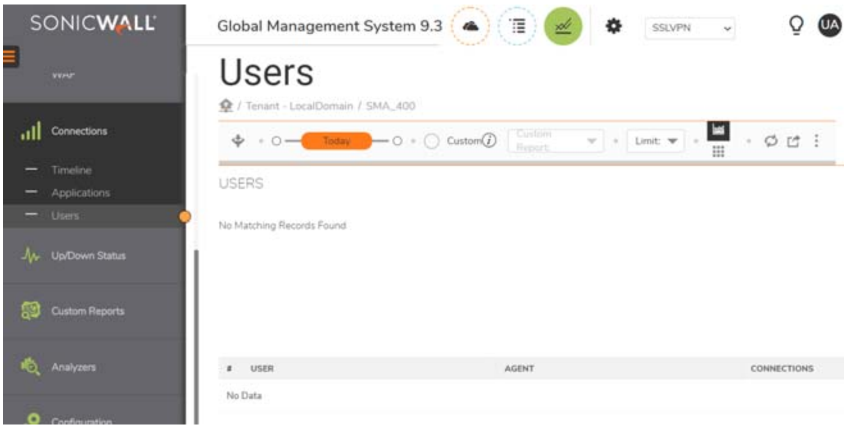
The Top Users report lists the users who have the most offloaded connections It displays the User Name, User agent, and connections, in order of the number of offloaded connections. The report drills down to the Top Applications, filtered by User Name.

To view the report:

1 Navigate to **SMA | Syslogs Panel | Connections > Users.**

2 Click on the TreeControl Panel icon. The TreeControl Panel appears.

3 Select the desired SMA appliance from the TreeControl menu. The Offloaded Connections Top Users Summary report displays.



#	USER	AGENT	CONNECTIONS
No Data			

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

Viewing Uptime/Downtime Reports

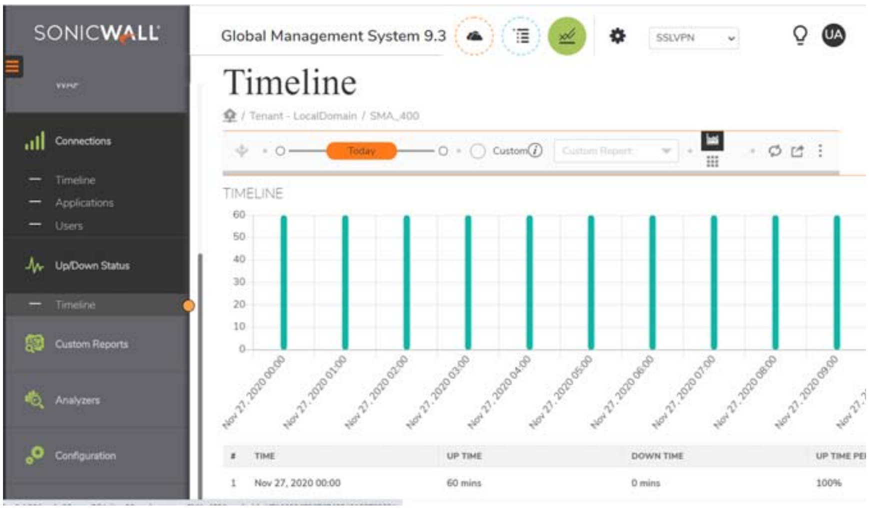
The Uptime/Downtime status timeline displays a timeline of up units in green and down units in red, for a 24-hour period.

To view the Uptime Downtime reports:

1 Navigate to **SMA | Syslogs Panel | Up/Down Status > Timeline.**

2 Click on the TreeControl Panel ☰ icon. The TreeControl Panel appears.

3 Select the desired SMA appliance from the TreeControl menu. The Offloaded Connections Top Users Summary report displays.



#	TIME	UP TIME	DOWN TIME	UP TIME PE
1	Nov 27, 2020 00:00	60 mins	0 mins	100%

The report displays the Time, Uptime, Down Time and Percentage details.

Viewing SMA Log Analyzer

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

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

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

You can filter the log on IP address, Message, User, or Service by clicking on a column heading to sort results by a specific criteria.

Click on hyperlinks on SMA Reports to view the Analyzer Log for more details. Log information can be saved using the Save icon on the Filter Bar for a specific report. This report then appears in the list of Custom Reports.

Topics:

- Saving System Log Reports
- Sysog Exclusion Filter

Saving System Log Reports

To load the report for later viewing:

1 Navigate to **SMA | Syslogs Panel | Analyzers > Log Analyzer**.

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

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

You can also click on the export icons to save a log to PDF, XML, or CSV formats.

> ⓘ **NOTE:** Saved system logs are limited in the number of rows that are saved. If saving to PDF, a maximum of 2,500 rows are saved. If saving to Excel, a maximum of 10,000 rows are saved.

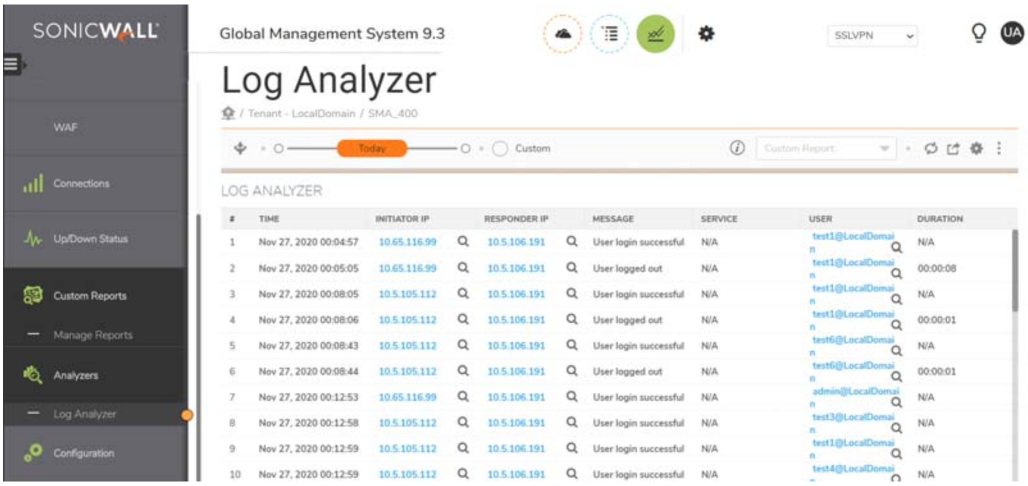
Viewing the Analyzer Log for a SMA Appliance

To view the Log:

1 Navigate to **SMA | Syslogs Panel | Analyzer > Log Analyzer.**

2 Click on the TreeControl Panel ☰ icon. The TreeControl Panel appears.

3 Select the desired SMA appliance from the TreeControl menu. The Log Analyzer Summary report displays.



Log Analyzer

/ Tenant - LocalDomain / SMA_400

LOG ANALYZER

#	TIME	INITIATOR IP	RESPONDER IP	MESSAGE	SERVICE	USER	DURATION
1	Nov 27, 2020 00:04:57	10.65.116.99	10.5.106.191	User login successful	N/A	test1@LocalDomain	N/A
2	Nov 27, 2020 00:05:05	10.65.116.99	10.5.106.191	User logged out	N/A	test1@LocalDomain	00:00:08
3	Nov 27, 2020 00:08:05	10.5.105.112	10.5.106.191	User login successful	N/A	test1@LocalDomain	N/A
4	Nov 27, 2020 00:08:06	10.5.105.112	10.5.106.191	User logged out	N/A	test1@LocalDomain	00:00:01
5	Nov 27, 2020 00:08:43	10.5.105.112	10.5.106.191	User login successful	N/A	test6@LocalDomain	N/A
6	Nov 27, 2020 00:08:44	10.5.105.112	10.5.106.191	User logged out	N/A	test6@LocalDomain	00:00:01
7	Nov 27, 2020 00:12:53	10.65.116.99	10.5.106.191	User login successful	N/A	admin@LocalDomain	N/A
8	Nov 27, 2020 00:12:58	10.5.105.112	10.5.106.191	User login successful	N/A	test3@LocalDomain	N/A
9	Nov 27, 2020 00:12:59	10.5.105.112	10.5.106.191	User login successful	N/A	test1@LocalDomain	N/A
10	Nov 27, 2020 00:12:59	10.5.105.112	10.5.106.191	User login successful	N/A	test4@LocalDomai	N/A

The report displays the details including Time, Initiator IP, Responder IP, Message, Service, User, and Duration.

Sysog Exclusion Filter

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

Use this screen to manage the volume of syslog uploaded to the reporting database. The factory default filters are configured to upload only the syslog needed to generate the reports. This can be fine tuned further, but it requires advanced knowledge of the syslog and consequently should be completed by experts only. Adding a wrong filter could lead to receiving a **"No Matching Records Found"** message.

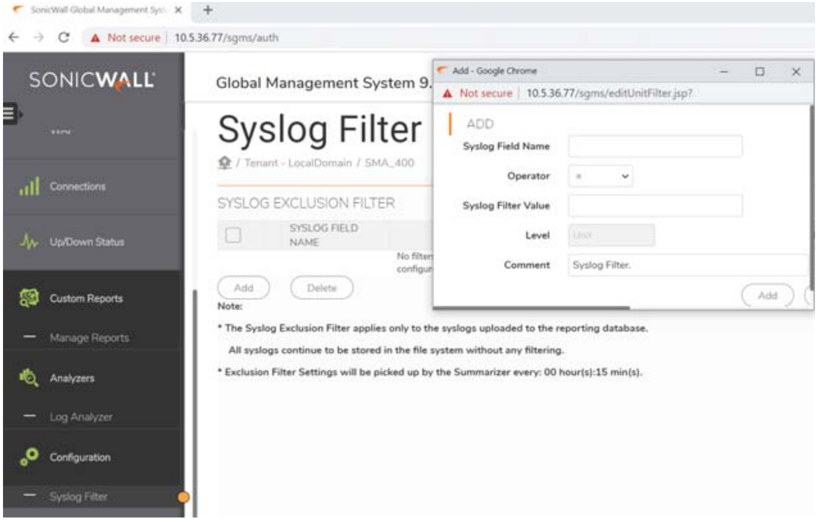
To add a filter:

1 Navigate to **SMA | Syslogs Panel | Configuration > Syslog Filter**.

2 Click on the TreeControl Panel icon. The TreeControl Panel appears.

3 Select the desired SMA appliance from the TreeControl menu. The Syslog Exclusion Filter page displays. This page allows you to view filters currently applied, add filters, or remove filters.

4 Click **Add Filter** to configure and add a filter. The **Add Filter** window appears.


SonicWall Global Management Sys
Not secure | 10.5.36.77/sgms/auth
SONICWALL
Connections
Up/Down Status
Custom Reports
Manage Reports
Analyzers
Log Analyzer
Configuration
Syslog Filter
Global Management System 9.
Add - Google Chrome
Not secure | 10.5.36.77/sgms/editUnitFilter.jsp?
Add
Delete

Syslog Filter

/ Tenant - LocalDomain / SMA_400

SYSLOG EXCLUSION FILTER

□	SYSLOG FIELD NAME

No filter configur

ADD

Syslog Field Name

Operator =

Syslog Filter Value

Level Unit

Comment Syslog Filter.

Note:

* The Syslog Exclusion Filter applies only to the syslogs uploaded to the reporting database.
All syslogs continue to be stored in the file system without any filtering.

* Exclusion Filter Settings will be picked up by the Summarizer every: 00 hour(s):15 min(s).

5 Specify the field you want to modify, then select an operator, syslog filter value, level, and comment.

6 Press **Enter** on your keyboard to save the filter. The filter is added to the list of Syslog Exclusion Filters.

To delete a filter:

1 Navigate to **SMA | Syslogs Panel | Configuration > Syslog Filter**.

2 Click on the TreeControl Panel icon. The TreeControl Panel appears.

3 Select the desired SMA appliance from the TreeControl menu. The Syslog Exclusion Filter page displays. This page allows you to view filters currently applied, add filters, or remove filters.

4 Select the checkbox next to the filter and click **Delete**. The exclusion filter is deleted.

Events

The Events entry on the Reports tab allows you to configure and view alerts specific to “Reporting for the unit selected.” The **Events** tab allows you to configure and view alerts specific to Reporting for the unit selected, through the **Alert Settings** and **Current Alerts** items.

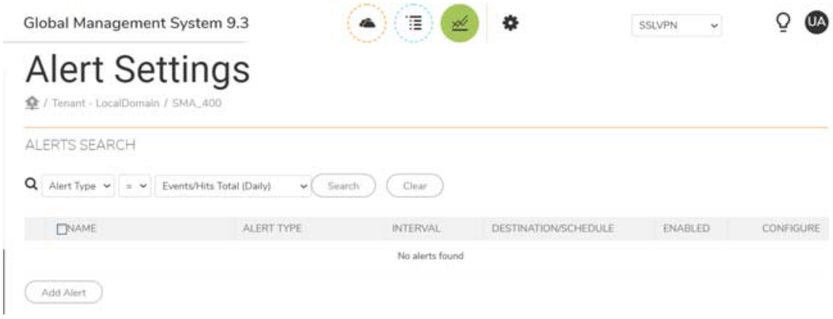
To view the alerts:

1 Navigate to **SMA | Syslogs Panel | Events > Alert Settings.**

2 Click on the TreeControl Panel ☰ icon. The TreeControl Panel appears.

3 Select the desired SMA appliance from the TreeControl menu. The Alert Settings page displays. You can use this menu to search for Alerts by name or type, either by exact match or matching strings.

4 To search for an alert by name, select an alert type from the drop-down menu, select a search value, enter a search term, then click **Search** to find an Alert of interest.



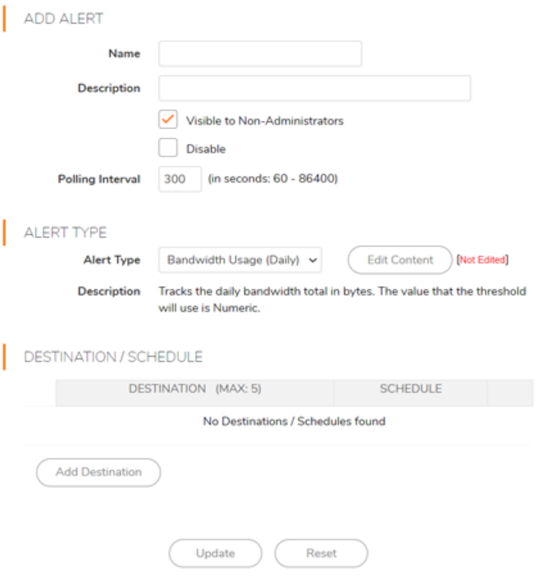
Alert Settings

/ Tenant - LocalDomain / SMA_400

ALERTS SEARCH

□NAME	ALERT TYPE	INTERVAL	DESTINATION/SCHEDULE	ENABLED	CONFIGURE
		No alerts found			

5 You can also add an alert. Click **Add Alert** on the Alerts menu. The Add Alert pop-up menu allows you to specify the type of data you want to track, how often to poll for data, and whether it is visible to only administrators or to non-administrators as well.


ADD ALERT

Name

Description

☑ Visible to Non-Administrators

□ Disable

Polling Interval 300 (in seconds: 60 - 86400)

ALERT TYPE

Alert Type: Bandwidth Usage (Daily)

Description: Tracks the daily bandwidth total in bytes. The value that the threshold will use is Numeric.

DESTINATION / SCHEDULE

DESTINATION (MAX: 5)	SCHEDULE
No Destinations / Schedules found	

Alert Types are pre-defined, static parameters and are not customizable.

The Available Alert types for SMA are:

Available Alert Types for SMA

Alert Type	Description
Bandwidth Usage (Daily)	Tracks the daily bandwidth total in bytes. The value that the threshold uses is Numeric.
Events/Hits Total (Daily)	Tracks the daily events/hits total. The value that the threshold uses is Numeric.

6 Select the Alert Type and click on **Edit Content** to edit threshold values. A popup menu appears. You can choose from the preset Threshold values or create a new threshold value by clicking the icon to the right of the Threshold banner. Only one new threshold can be created at a time.

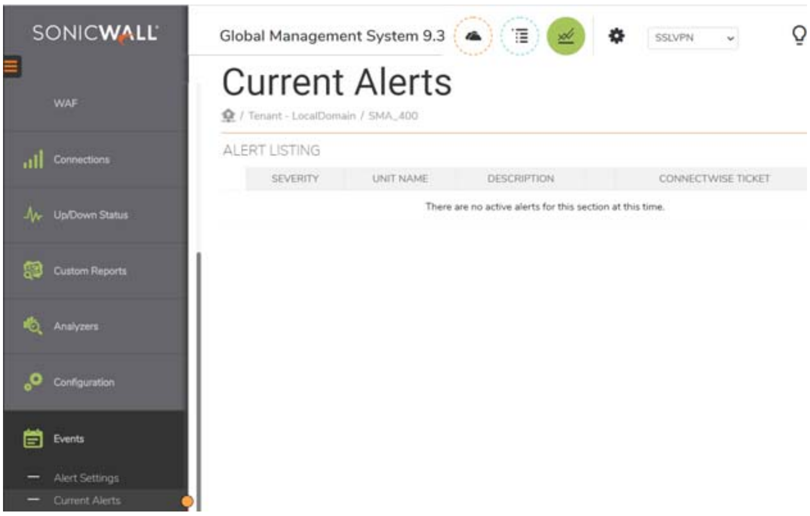
> ⓘ **NOTE:** Threshold values might not be available for all Alert types. In such case, the Edit Content field is not present.

7 Alerts can be emailed to you or a specified destination on a regular schedule. You can specify up to five destinations. Click **Add Destination** to enable and select from the pull-downs of destination and schedule entries.

8 Click **Update** when you have finished configuring the Alert. The alert is added to the list of Alerts on the menu.

Current Alerts

You can view the current alerts from the **Events** tab. Click **SMA| Reports | Events > Current Alerts** and choose from the list of saved Custom reports.



Current Alerts

/ Tenant - LocalDomain / SMA_400

ALERT LISTING

SEVERITY	UNIT NAME	DESCRIPTION	CONNECTWISE TICKET

There are no active alerts for this section at this time.

The details of Severity, Unit Name, Description, and details of Connect Wise Tickets are displayed.

3

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

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 and participate in the Community forum discussions at https://community.sonicwall.com/technology-and-support.
- 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

ⓘ **NOTE:** A NOTE icon indicates supporting information.

ⓘ **IMPORTANT:** An IMPORTANT icon indicates supporting information that may need a little extra attention.

ⓘ **TIP:** A TIP indicates helpful information.

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

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

GMS Administration Guide
Updated - January 2021
Software Version - 9.3
232-005542-00 Rev A

The information in this document is provided in connection with SonicWall 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 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. 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/legal/end-user-product-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