SONICWALL®

# SonicWall® Global Management System 8.7

## Release Notes

### March 2019

These release notes provide information about the SonicWall® Global Management System (GMS) 8.7 release.

ⓘ **IMPORTANT:** Critical Hotfix 215547 is required for a successful upgrade to GMS 8.7. See Upgrading to GMS 8.7 for additional information.

**Topics:**

- About GMS 8.7
- New Features
- Resolved Issues
- Known Issues
- Platform Compatibility
- Upgrading to GMS 8.7
- Product Licensing
- SonicWall Support

# About GMS 8.7

SonicWall® Global Management System(GMS) is a Web-based application that can configure and manage thousands of SonicWall firewall appliances and monitor non-SonicWall appliances from a central location. GMS can be used as a Management Console in an enterprise network containing a single SonicWall E-Class NSA or SuperMassive. GMS can also be used as a Remote Management System for managing multiple unit deployments for enterprise and service provider networks consisting of hundreds and thousands of firewalls, Email Security appliances, and Secure Mobile Access (SMA) appliances.

GMS enables administrators to monitor the status of and apply configurations to all managed SonicWall appliances, groups of SonicWall appliances, or individual SonicWall appliances. GMS also provides centralized management of scheduling and pushing firmware updates to multiple appliances and to apply configuration backups of appliances at regular intervals. GMS has monitoring features so you can view the current status of SonicWall appliances and non-SonicWall appliances, pending tasks, and log messages. It also provides graphical reporting of Firewall, SMA, and Email Security (ES) appliance and network activities for the SonicWall appliances.

A wide range of informative real-time and historical reports can be generated to provide insight into usage trends and security events. Network administrators can also configure multiple site VPNs for SonicWall appliances. From the GMS user interface (UI), you can add VPN licenses to SonicWall appliances, configure VPN settings, and enable or disable remote-client access for each network.

GMS 8.7 is a new feature release that includes a number of resolved and known issues. Refer to New Features, Resolved Issues, and Known Issues for additional information.

ⓘ **NOTE:** GMS can be deployed a number of different ways, and numerous requirements apply. Refer to Platform Compatibility for detailed information.

# New Features

GMS 8.7 releases several new features including:

- Zero Touch Support
- ConnectWise Integration
- Firewall Sandwich Group Reporting
- Group Level Interface Support
- Group Level Reporting
- Adding, Modifying, and Reassigning Agent Screens
- Web Activity Reports Showing URLs
- Version Upgrades for Tomcat and MySQL
- SonicOS 6.5.3 Support

## Zero Touch Support

GMS has automated the process of acquiring and configuring your firewalls with the Zero Touch feature as well as providing the mechanism to manage your firewalls with "zero" touch when you are setting it up for management. Simply put, the unit need only be plugged in for power and connected to the Internet for this feature to operate. Beyond that, the firewall, GMS, and other entities within the eco-system, function together to bring the unit under management.

**Topics:**

- Provisioning and Configuration
- DHCP/Auto IP Assignment
- Configuring Zero Touch with GMS

### Provisioning and Configuration

You are also able to optionally choose to pre-configure your unit before it is even delivered. This feature requires the following changes in GMS:

- After GMS discovers the new unit and automatically adds it using data from MySonicWall, you are able to make group level configuration changes in GMS. The group already has the default configuration present depending on the firmware version of the unit.
- After the unit is online and acquired by GMS, you are able to push all configuration changes that were made using the Inheritance feature of GMS.

The unit can then be ready for use (with all the required configuration) within a few minutes of being plugged in.

### DHCP/Auto IP Assignment

Configure a WAN IP for your device before connecting it to the Internet or any SonicWall services including MySonicWall, License Manager, and GMS.

As part of Zero Touch Management, automatic assignment of the WAN IP using DHCP is also possible. You need only to plug in the device to both a LAN and WAN and the IP assignment automatically takes place.

# Configuring Zero Touch with GMS

Depending on the type of setup you intend to establish with Zero Touch, whether an All-In-One (AIO) or Distributed deployment, your work environment must meet particular requirements.

***To install and configure GMS 8.7 with Zero Touch, complete the following steps.***

1 Download GMS 8.7 from MySonicWall and follow the steps for installation to a virtual environment as detailed in Installing GMS 8.7 on VMware ESXi. Refer to the following matrix for deployment requirements:

| Features | Deployment Mode |
|---|---|
| ConnectWise Integration | AIO or Distributed |
| Zero Touch | AIO or Distributed |
| Firewall Sandwich Reporting | Distributed (AIO + one agent with role: Flow server) |
| ConnectWise Integration, Zero-Touch, and Firewall Sandwich Reporting | Distributed (AIO + flow server agent)<br>Distributed (Database + Console + flow server agent) |

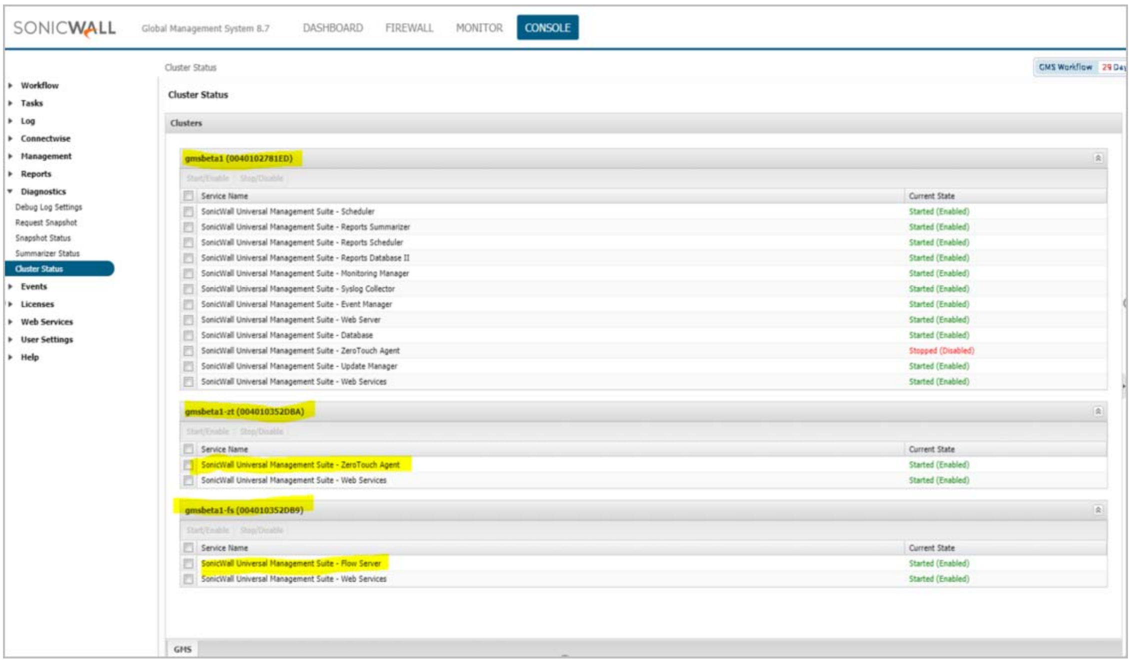
2 For testing the features, complete the steps in the sections that follow.

## Enabling Zero Touch

For the Zero Touch feature to function correctly, you should have SonicOS 6.5.3.1-48n or newer running on your firewall. New firewall shipments already have that version and Zero Touch enabled in the firmware.

**NOTE:** Zero Touch was available in SonicOS 6.5.1.1-42n, but for best results, use the recommendation.

1 After you have installed the correct version of GMS and before enabling Zero Touch, you can optionally check **CONSOLE | Diagnostics > Cluster Status** to verify the Zero Touch services are running.



Cluster Status

Clusters

gmsbeta1 (0040102781ED)

| Service Name | Current State |
|---|---|
| SonicWall Universal Management Suite - Scheduler | Started (Enabled) |
| SonicWall Universal Management Suite - Reports Summarizer | Started (Enabled) |
| SonicWall Universal Management Suite - Reports Scheduler | Started (Enabled) |
| SonicWall Universal Management Suite - Reports Database II | Started (Enabled) |
| SonicWall Universal Management Suite - Monitoring Manager | Started (Enabled) |
| SonicWall Universal Management Suite - Syslog Collector | Started (Enabled) |
| SonicWall Universal Management Suite - Event Manager | Started (Enabled) |
| SonicWall Universal Management Suite - Web Server | Started (Enabled) |
| SonicWall Universal Management Suite - Database | Started (Enabled) |
| SonicWall Universal Management Suite - ZeroTouch Agent | Stopped (Disabled) |
| SonicWall Universal Management Suite - Update Manager | Started (Enabled) |
| SonicWall Universal Management Suite - Web Services | Started (Enabled) |

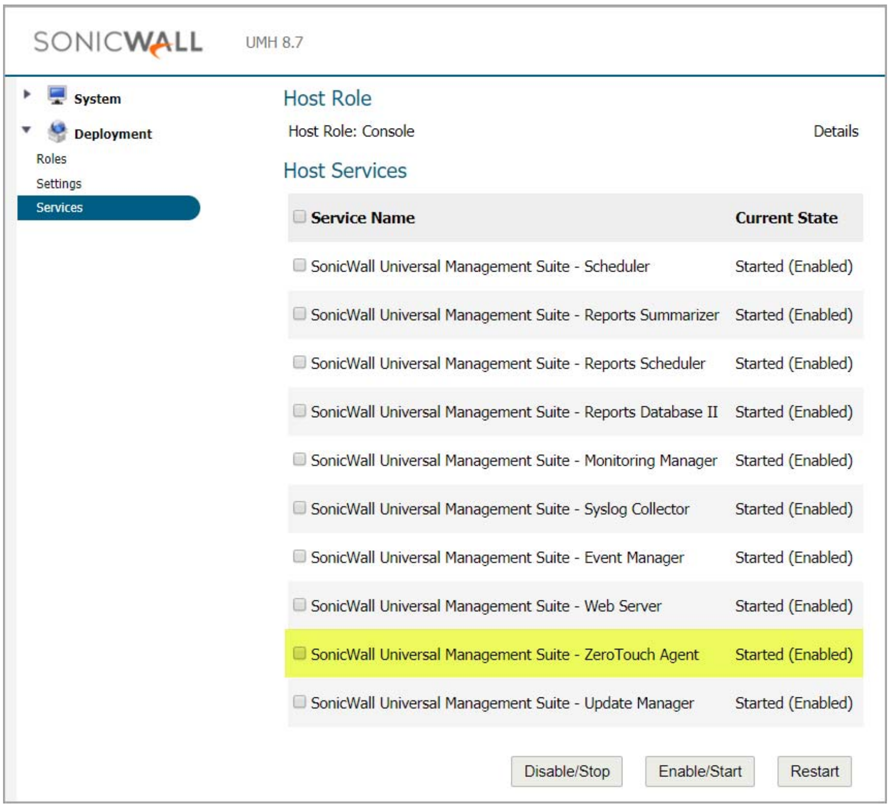
gmsbeta1-zt (004010352DBA)

| Service Name | Current State |
|---|---|
| SonicWall Universal Management Suite - ZeroTouch Agent | Started (Enabled) |
| SonicWall Universal Management Suite - Web Services | Started (Enabled) |

gmsbeta1-fs (004010352DB9)

| Service Name | Current State |
|---|---|
| SonicWall Universal Management Suite - Flow Server | Started (Enabled) |
| SonicWall Universal Management Suite - Web Services | Started (Enabled) |

2 You can also optionally check the agent console at **Deployment | Services** to determine whether the Zero Touch services are running in that environment.



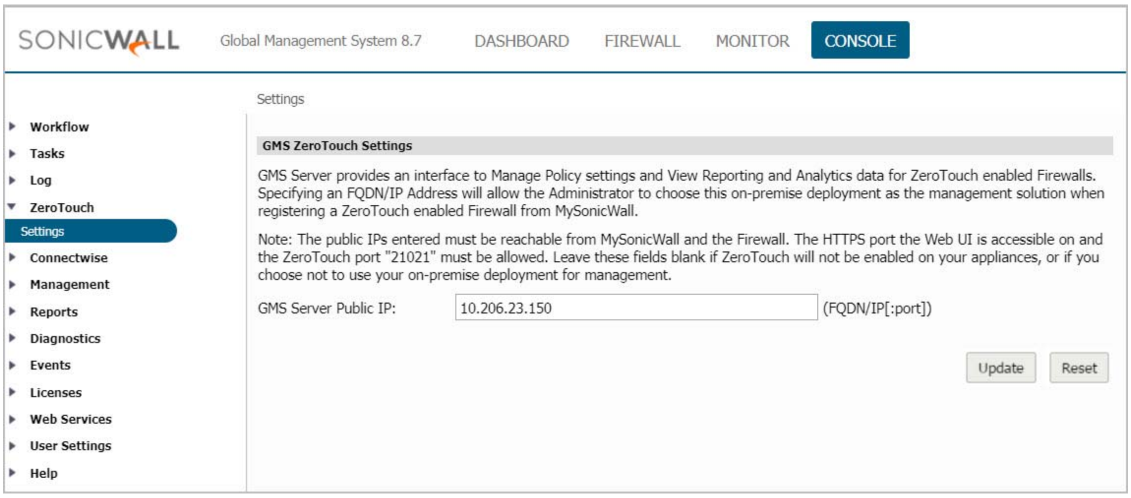
Host Role

Host Role: Console Details

Host Services

| Service Name | Current State |
|---|---|
| □ SonicWall Universal Management Suite - Scheduler | Started (Enabled) |
| □ SonicWall Universal Management Suite - Reports Summarizer | Started (Enabled) |
| □ SonicWall Universal Management Suite - Reports Scheduler | Started (Enabled) |
| □ SonicWall Universal Management Suite - Reports Database II | Started (Enabled) |
| □ SonicWall Universal Management Suite - Monitoring Manager | Started (Enabled) |
| □ SonicWall Universal Management Suite - Syslog Collector | Started (Enabled) |
| □ SonicWall Universal Management Suite - Event Manager | Started (Enabled) |
| □ SonicWall Universal Management Suite - Web Server | Started (Enabled) |
| □ SonicWall Universal Management Suite - ZeroTouch Agent | Started (Enabled) |
| □ SonicWall Universal Management Suite - Update Manager | Started (Enabled) |

3 Navigate to **CONSOLE | Zero Touch > Settings**.



Settings

GMS ZeroTouch Settings

GMS Server provides an interface to Manage Policy settings and View Reporting and Analytics data for ZeroTouch enabled Firewalls. Specifying an FQDN/IP Address will allow the Administrator to choose this on-premise deployment as the management solution when registering a ZeroTouch enabled Firewall from MySonicWall.

Note: The public IPs entered must be reachable from MySonicWall and the Firewall. The HTTPS port the Web UI is accessible on and the ZeroTouch port "21021" must be allowed. Leave these fields blank if ZeroTouch will not be enabled on your appliances, or if you choose not to use your on-premise deployment for management.

GMS Server Public IP: 10.206.23.150 (FQDN/IP[:port])

4 Before providing the FQDN/IP address for your GMS server, consider the following:

- The GMS server IP must be a reachable IP (publicly) for the AIOP or Console on ports 443 (or custom) and 21021 for the firewall.

5 After you have entered a valid FQDN/IP address, click **Update**. Click **OK** to confirm changes or **Cancel** to start over.

6 If you are running earlier versions of SonicWall firewalls, complete the following steps. If you are running a brand new firewall, skip to the second bullet.

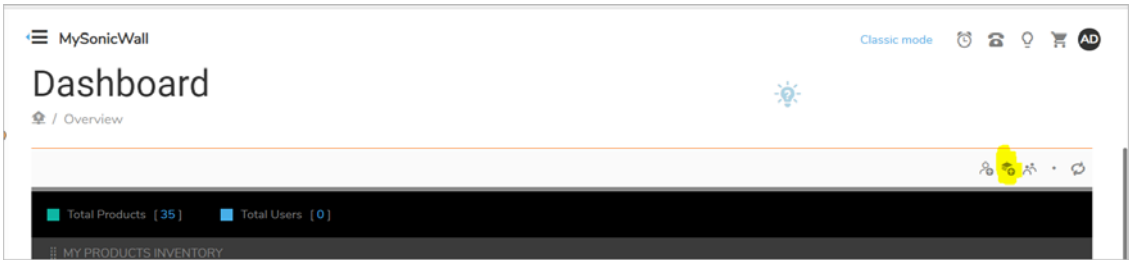
- Delete the firewall from your MySonicWall account and then make sure it is updated to and running SonicOS version 6.5.3.1-48n. Reboot the firewall using the factory default settings.

- While registering the firewall on MySonicWall, be sure to enable the Zero Touch checkbox.
- Choose the GMS On-Prem policy server from the drop-down menu.

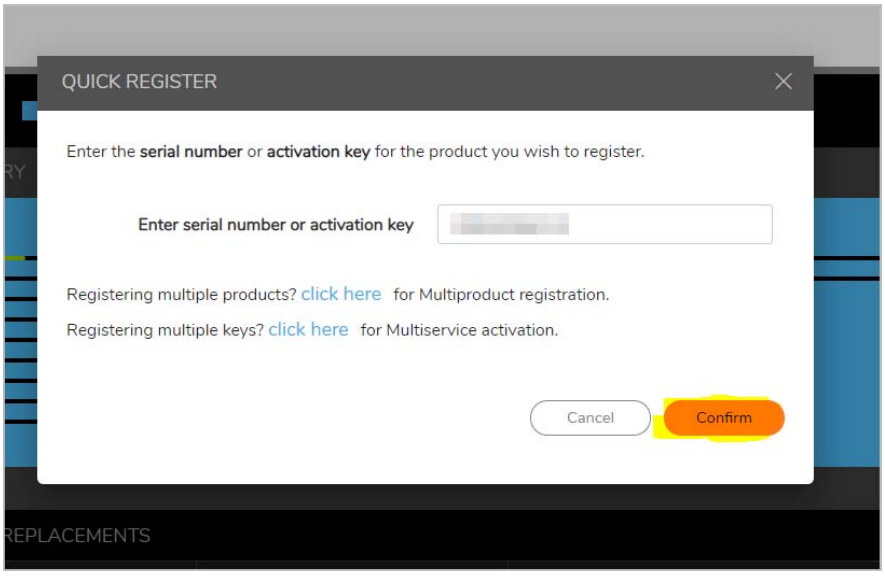
ⓘ **NOTE:** Bulk deployment for Zero Touch is not supported in the this version of the software.

- You can specify values different from those already present. Edit the fields to specify the new IP addresses.

7 From the MySonicWall Dashboard, click the **Register** icon in the top right button bar.



8 In the Quick Register form that appears, enter the **serial number** or **activation key** (usually located on the bottom of your firewall) for the product you wish to register.


QUICK REGISTER

Enter the **serial number** or **activation key** for the product you wish to register.

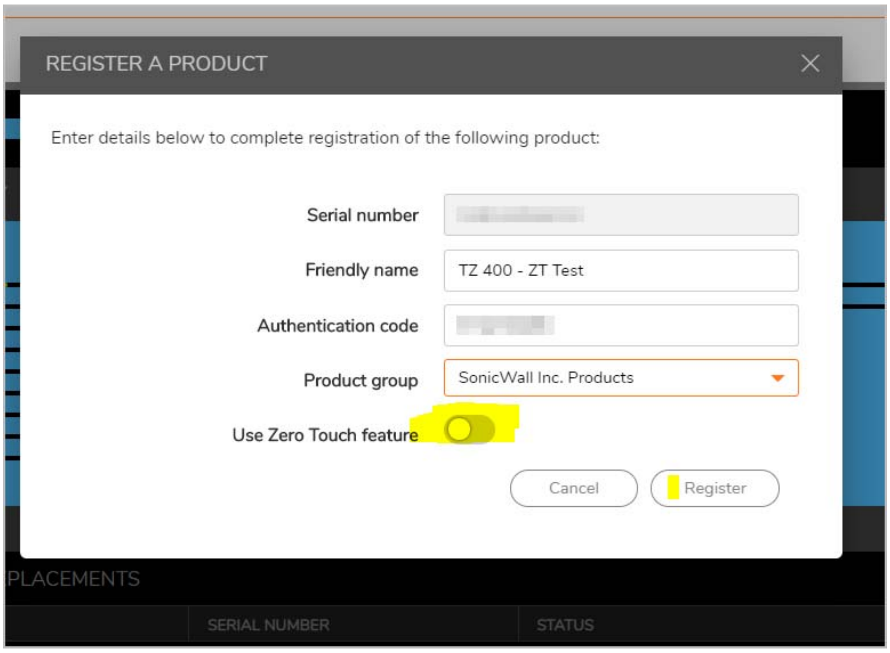
Enter serial number or activation key

Registering multiple products? click here for Multiproduct registration.

Registering multiple keys? click here for Multiservice activation.

9 Click **Confirm**.

10 To complete the registration, enter a **Friendly name** for the specific firewall, an **Authentication code** (received from your vendor at the time of purchase), and a **Product group** for this particular firewall in the remaining fields.



REGISTER A PRODUCT

Enter details below to complete registration of the following product:

| | |
|---|---|
| Serial number | [redacted] |
| Friendly name | TZ 400 - ZT Test |
| Authentication code | [redacted] |
| Product group | SonicWall Inc. Products |
| Use Zero Touch feature | ○ |

11 To use the **Zero Touch** feature, be sure to enable the slider button.

12 Click **Register**.

13 A drop-down box appears where you can choose GMS. Select GMS and provide the required details in the available fields.

After you have completed registration, the firewall appears on the GMS console (one to two minutes).

# ConnectWise Integration

GMS integrates with the ConnectWise Manage platform to provide you with the ability to synchronize basic firewall details into the ConnectWise platform. This integration includes the capability of managing security events and SonicWall assets and provides the ability to create automated service tickets for alerts in the ConnectWise Manage platform. Features also include:

- **Asset Synchronization** - Assets managed by GMS (firewalls, Email Security, Secure Mobile Access) can synchronize with ConnectWise Manage.
- **Automated Ticketing** - GMS automatically creates and deletes tickets in ConnectWise Manage when alerts have been generated in GMS.

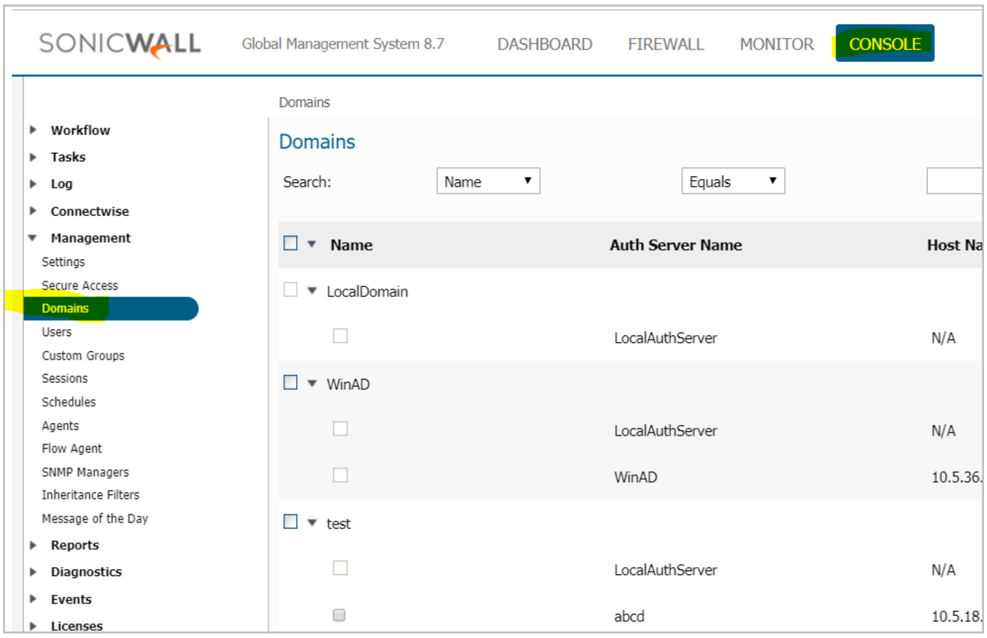
**Topics:**

- Configuring ConnectWise Settings
- Configuring Alerts
- Deleting ConnectWise from GMS

# Configuring ConnectWise Settings

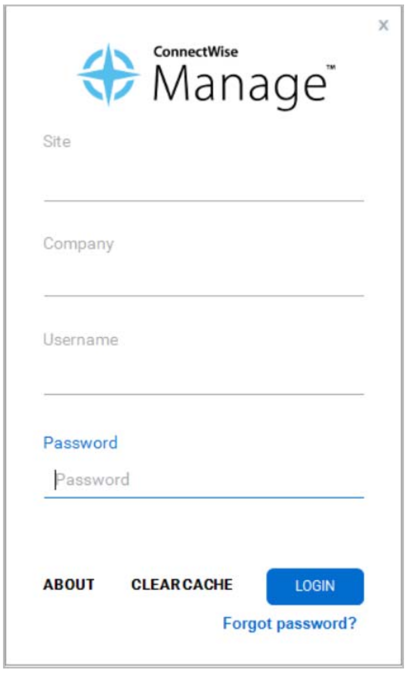
***To setup integration between GMS and ConnectWise:***

1 Navigate to **CONSOLE | Management > Domains** and create a domain for managed companies. (Domains in GMS map to managed companies in ConnectWise Manage).

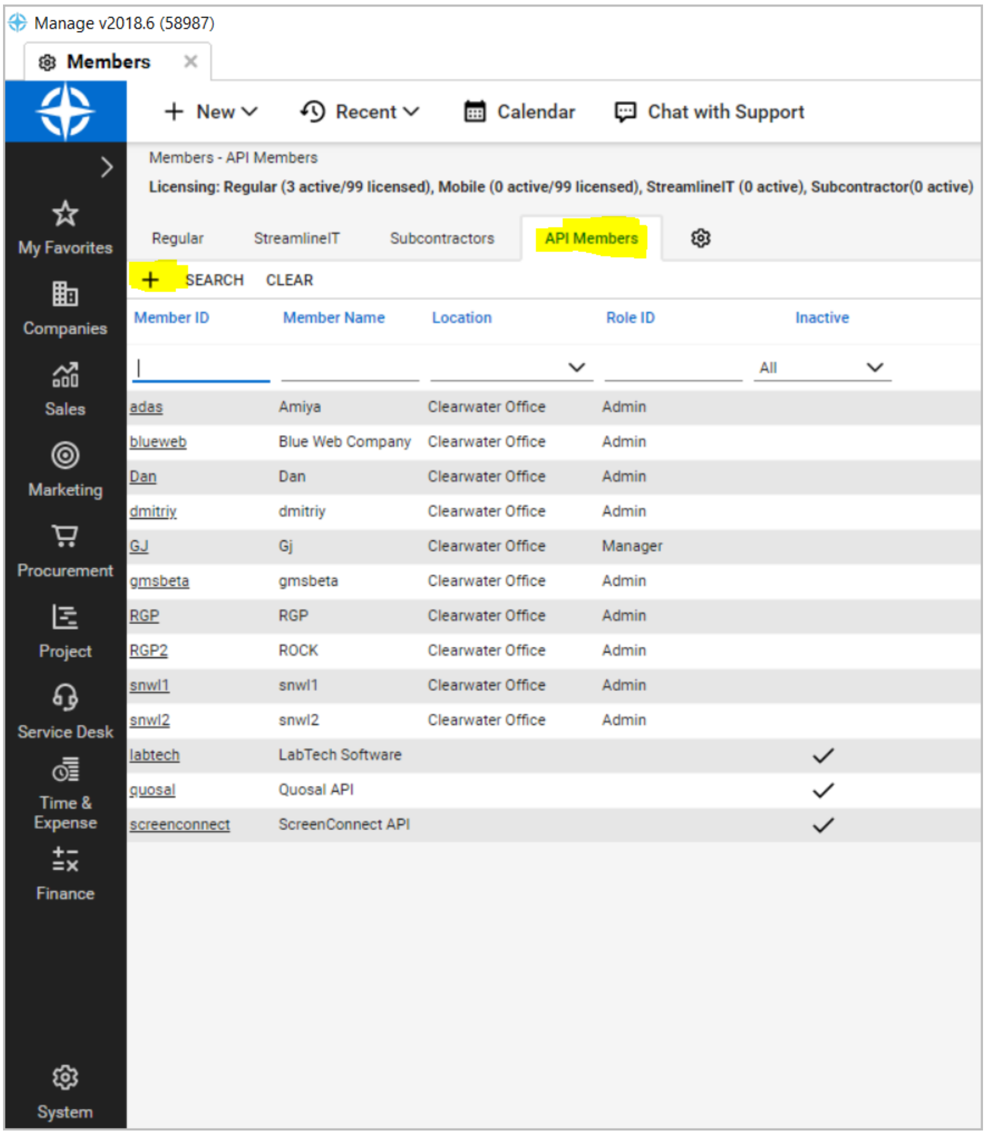


| Name | Auth Server Name | Host Na |
|---|---|---|
| LocalDomain | | |
| | LocalAuthServer | N/A |
| WinAD | | |
| | LocalAuthServer | N/A |
| | WinAD | 10.5.36. |
| test | | |
| | LocalAuthServer | N/A |
| | abcd | 10.5.18. |

2 Log in to **ConnectWise Manage**. Enter your company's **Site** location, **Company** name, **Username**, and **Password**.



3 In ConnectWise, navigate to **System > Manage > API Members**.



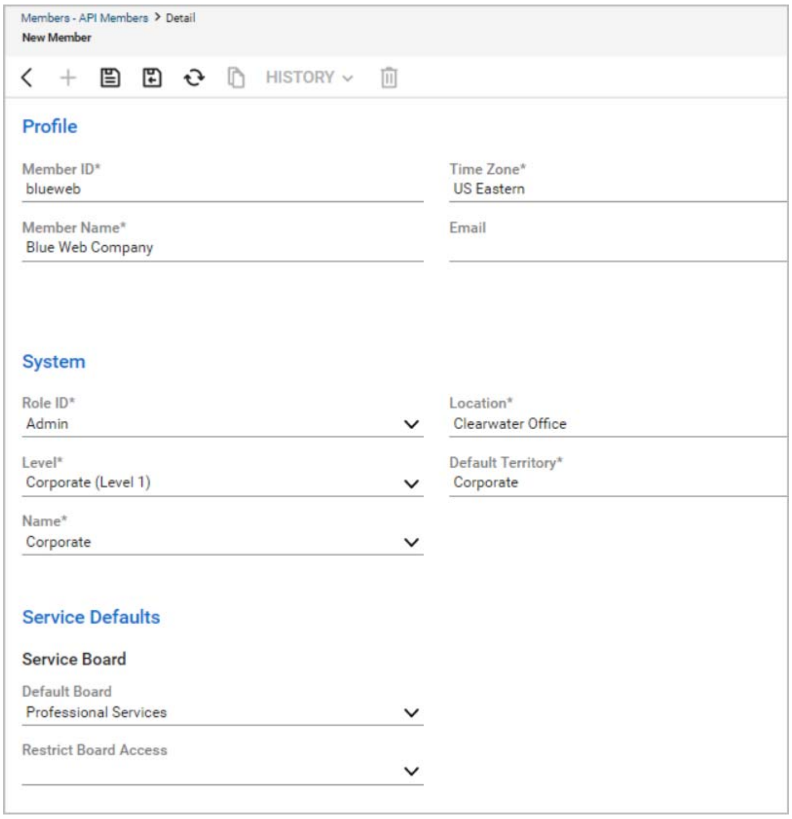
Members - API Members

Licensing: Regular (3 active/99 licensed), Mobile (0 active/99 licensed), StreamlineIT (0 active), Subcontractor(0 active)

| Member ID | Member Name | Location | Role ID | Inactive |
|---|---|---|---|---|
| adas | Amiya | Clearwater Office | Admin | |
| blueweb | Blue Web Company | Clearwater Office | Admin | |
| Dan | Dan | Clearwater Office | Admin | |
| dmitriy | dmitriy | Clearwater Office | Admin | |
| GJ | Gj | Clearwater Office | Manager | |
| gmsbeta | gmsbeta | Clearwater Office | Admin | |
| RGP | RGP | Clearwater Office | Admin | |
| RGP2 | ROCK | Clearwater Office | Admin | |
| snwl1 | snwl1 | Clearwater Office | Admin | |
| snwl2 | snwl2 | Clearwater Office | Admin | |
| labtech | LabTech Software | | | ✓ |
| quosal | Quosal API | | | ✓ |
| screenconnect | ScreenConnect API | | | ✓ |

4 On the API Members tab, click the **+** sign to create a new API member profile for the managed company administrator.

5 In the System section, add an Admin profile for the managed company.



Members - API Members > Detail

New Member

Profile

Member ID*: blueweb

Time Zone*: US Eastern

Member Name*: Blue Web Company

Email:

System

Role ID*: Admin

Location*: Clearwater Office

Level*: Corporate (Level 1)

Default Territory*: Corporate

Name*: Corporate

Service Defaults

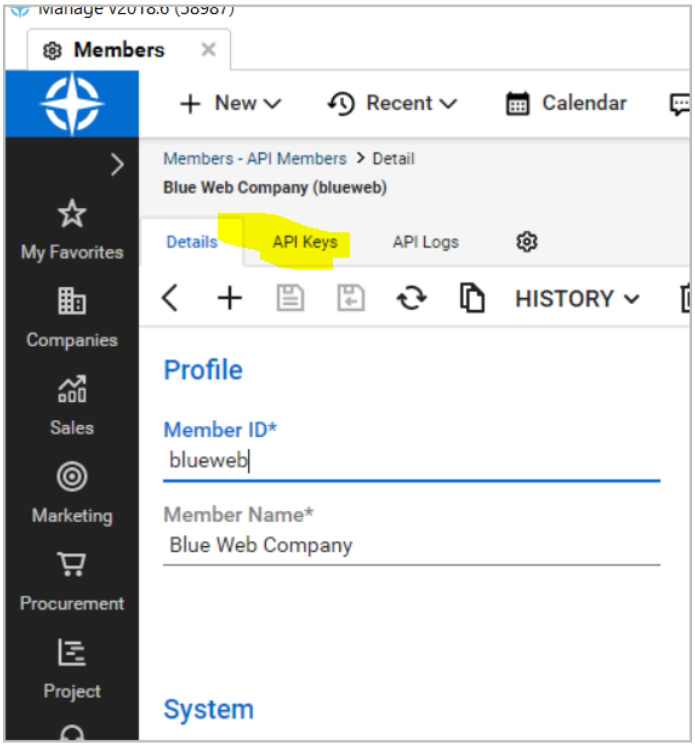
Service Board

Default Board: Professional Services

Restrict Board Access:

6 Click **Save**.

7 Click the **API Keys** tab.



Manage v2018.6 (58987)

Members - API Members > Detail

Blue Web Company (blueweb)

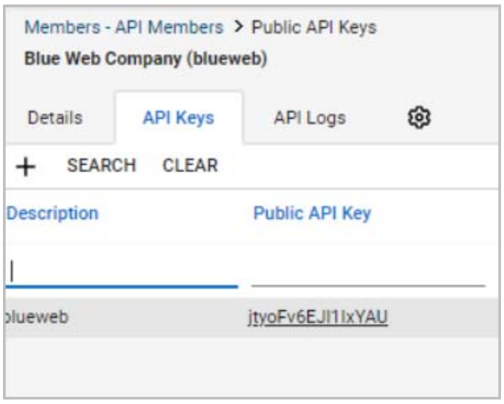
Profile

Member ID*: blueweb

Member Name*: Blue Web Company

System

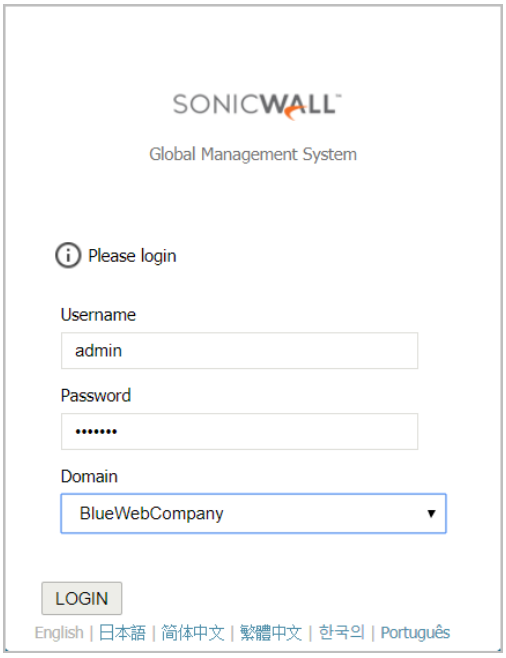
8 Generate a **Public API Key** and a **Private API Key** for the Administrator.



Blue Web Company (blueweb)

| Description | Public API Key |
|---|---|
| blueweb | jtyoFv6EJI1IxYAU |

9 Log back in to GMS using your newly created Domain (for the managed company).



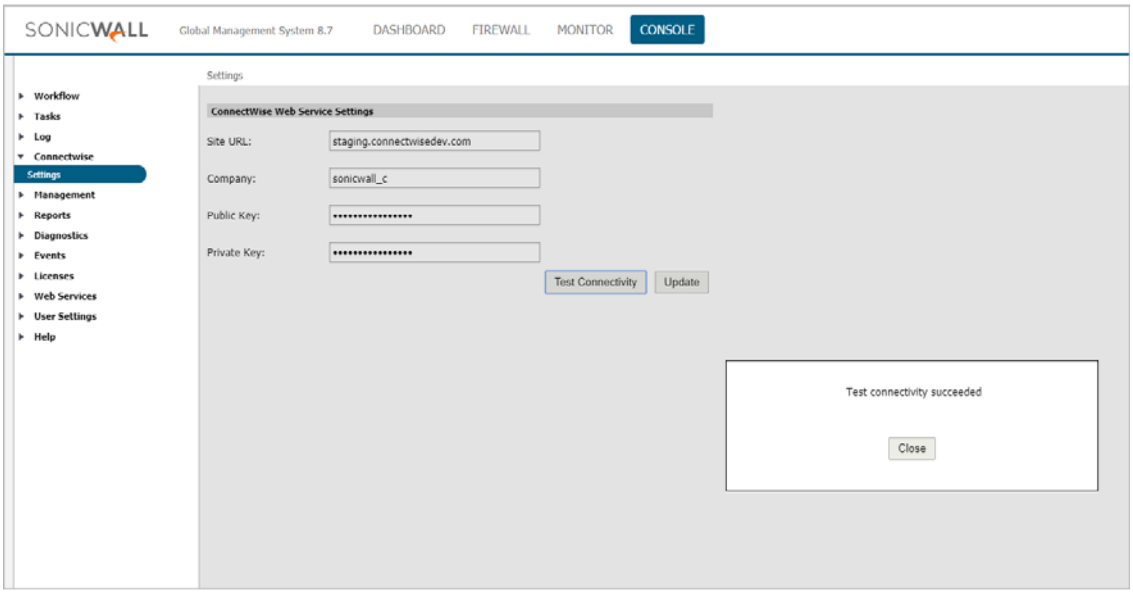
Please login

Username: admin

Password: •••••••

Domain: BlueWebCompany

10 Navigate to **CONSOLE | ConnectWise > Settings**.



ConnectWise Web Service Settings

Site URL: staging.connectwisedev.com

Company: sonicwall_c

Public Key: ••••••••••••••••

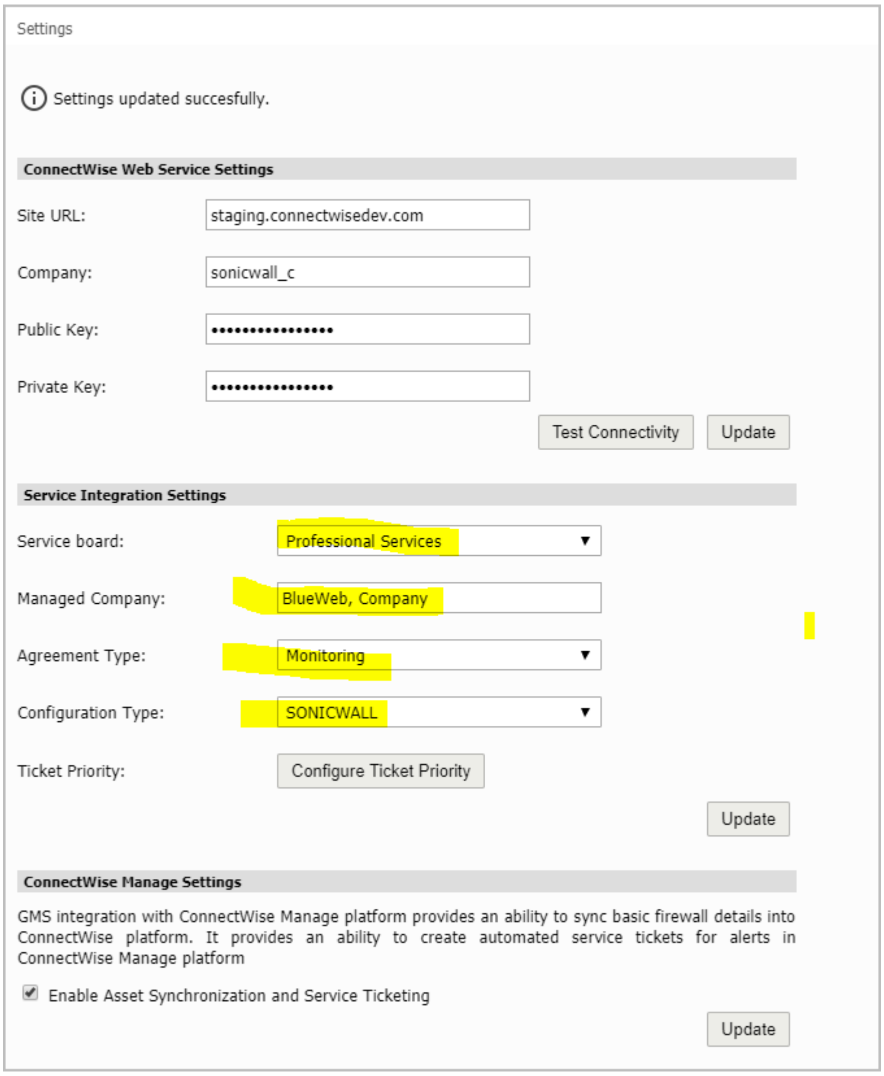
Private Key: ••••••••••••••••

Test connectivity succeeded

11 Complete the screen by entering the **Site URL**, your **Company Name**, the **Public Key** and the **Private key** you created for ConnectWise.

12 Click **Test Connectivity**.

13 If the connection is successful, click **Update** to move forward. Additional Service Integration Settings appear.



Settings

ⓘ Settings updated succesfully.

**ConnectWise Web Service Settings**

| | |
|---|---|
| Site URL: | staging.connectwisedev.com |
| Company: | sonicwall_c |
| Public Key: | •••••••••••••••• |
| Private Key: | •••••••••••••••• |

**Service Integration Settings**

| | |
|---|---|
| Service board: | Professional Services ▼ |
| Managed Company: | BlueWeb, Company |
| Agreement Type: | Monitoring ▼ |
| Configuration Type: | SONICWALL ▼ |
| Ticket Priority: | Configure Ticket Priority |

**ConnectWise Manage Settings**

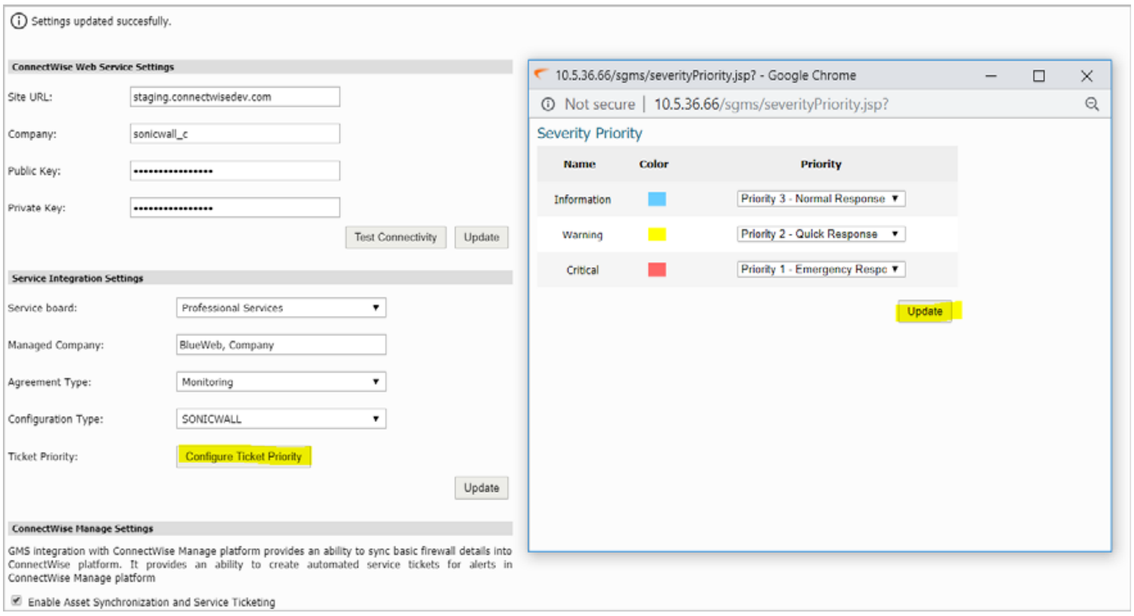
GMS integration with ConnectWise Manage platform provides an ability to sync basic firewall details into ConnectWise platform. It provides an ability to create automated service tickets for alerts in ConnectWise Manage platform

☑ Enable Asset Synchronization and Service Ticketing

14 Complete the additional settings as follows:

- **Service Board** - From the drop-down menu, choose the service board you are managing.
- **Managed Company** - Enter the name of the company you want to map to the GMS domain you logged in to.
- **Agreement Type** - Select an Agreement Type from the drop-down menu.
- **Configuration Type** - By selecting SONICWALL from the drop-down menu, SonicWall assets can be filtered on the ConnectWise Manage configuration dashboard.

15 Click **Configure Ticket Priority** to assign severity priorities.



Settings updated succesfully.

**ConnectWise Web Service Settings**

Site URL: staging.connectwisedev.com

Company: sonicwall_c

Public Key: ••••••••••••••••

Private Key: ••••••••••••••••

**Service Integration Settings**

Service board: Professional Services

Managed Company: BlueWeb, Company

Agreement Type: Monitoring

Configuration Type: SONICWALL

Ticket Priority: Configure Ticket Priority

**ConnectWise Manage Settings**

GMS integration with ConnectWise Manage platform provides an ability to sync basic firewall details into ConnectWise platform. It provides an ability to create automated service tickets for alerts in ConnectWise Manage platform

☑ Enable Asset Synchronization and Service Ticketing

10.5.36.66/sgms/severityPriority.jsp? - Google Chrome

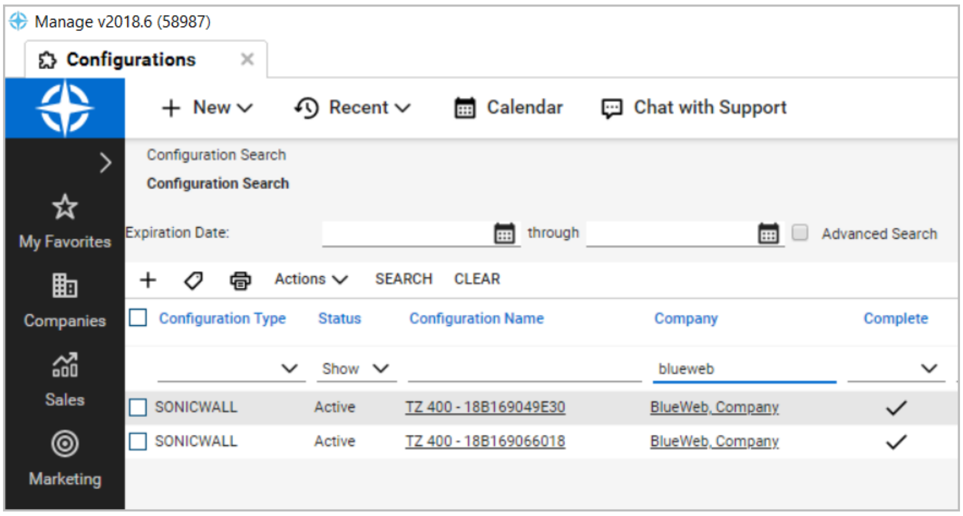
Not secure | 10.5.36.66/sgms/severityPriority.jsp?

Severity Priority

| Name | Color | Priority |
|---|---|---|
| Information | 🟦 | Priority 3 - Normal Response |
| Warning | 🟨 | Priority 2 - Quick Response |
| Critical | 🟥 | Priority 1 - Emergency Respo |

16 Click **Update**. The integration setup is complete.

You can log back in to ConnectWise to see that your assets (firewalls and so on) are synchronized with ConnectWise Manage.



Manage v2018.6 (58987)

Configuration Search

**Configuration Search**

Expiration Date: through ☐ Advanced Search

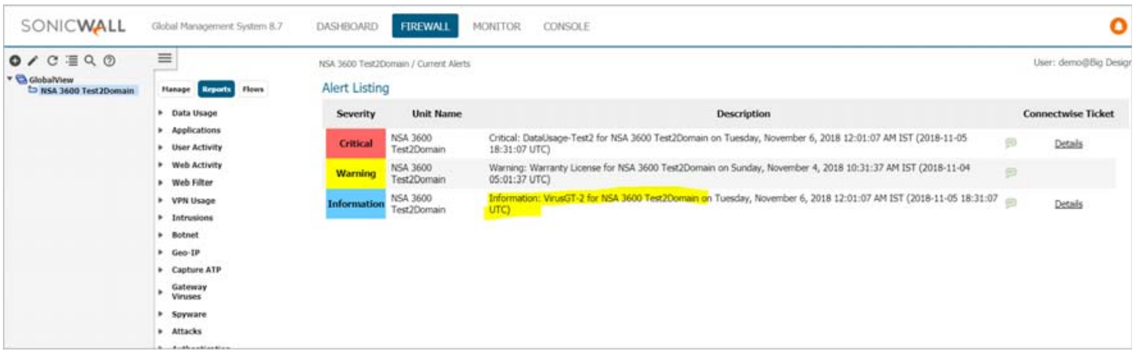
| ☐ Configuration Type | Status | Configuration Name | Company | Complete |
|---|---|---|---|---|
| | Show | | blueweb | |
| ☐ SONICWALL | Active | TZ 400 - 18B169049E30 | BlueWeb, Company | ✓ |
| ☐ SONICWALL | Active | TZ 400 - 18B169066018 | BlueWeb, Company | ✓ |

## Configuring Alerts

You can configure alerts in GMS, so that when events are triggered, tickets are then created in ConnectWise Manage. When alerts are deleted in GMS, the corresponding ticket in ConnectWise Manage are also deleted. See the *FIREWALL: Reports Administration Guide* for additional details on configuring alert settings.

*To configure alerts in GMS:*

1 Navigate to **FIREWALL | Reports | Events > Current Alerts**.



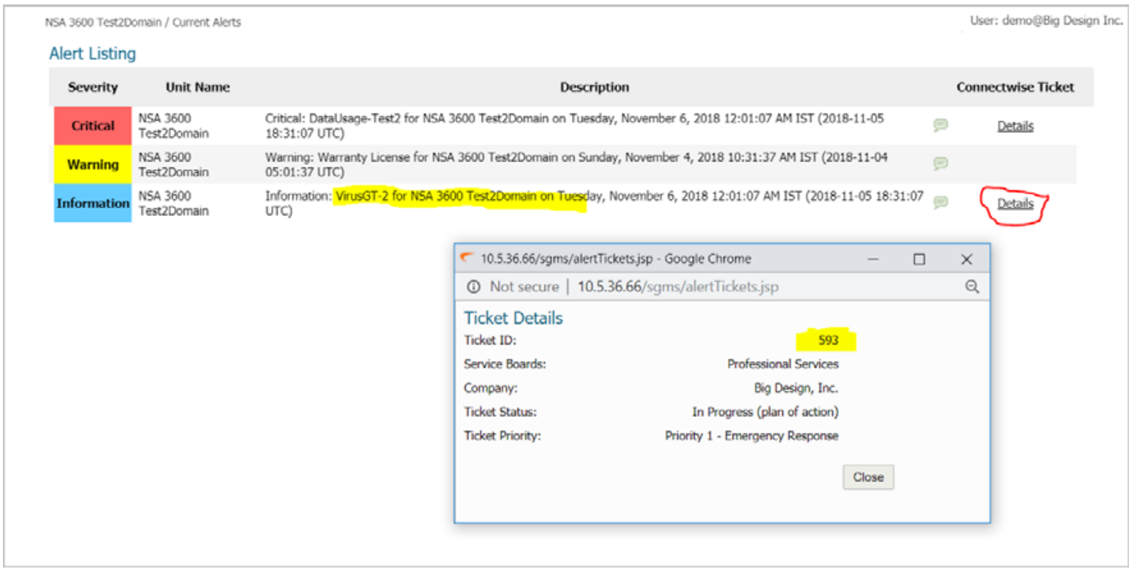
NSA 3600 Test2Domain / Current Alerts

User: demo@Big Design

Alert Listing

| Severity | Unit Name | Description | Connectwise Ticket |
|---|---|---|---|
| Critical | NSA 3600 Test2Domain | Critical: DataUsage-Test2 for NSA 3600 Test2Domain on Tuesday, November 6, 2018 12:01:07 AM IST (2018-11-05 18:31:07 UTC) | Details |
| Warning | NSA 3600 Test2Domain | Warning: Warranty License for NSA 3600 Test2Domain on Sunday, November 4, 2018 10:31:37 AM IST (2018-11-04 05:01:37 UTC) | |
| Information | NSA 3600 Test2Domain | Information: VirusGT-2 for NSA 3600 Test2Domain on Tuesday, November 6, 2018 12:01:07 AM IST (2018-11-05 18:31:07 UTC) | Details |

2 In Alert Listing, click the **Ticket Number** to see more information about the generated ticket.



NSA 3600 Test2Domain / Current Alerts

User: demo@Big Design Inc.

Alert Listing

| Severity | Unit Name | Description | Connectwise Ticket |
|---|---|---|---|
| Critical | NSA 3600 Test2Domain | Critical: DataUsage-Test2 for NSA 3600 Test2Domain on Tuesday, November 6, 2018 12:01:07 AM IST (2018-11-05 18:31:07 UTC) | Details |
| Warning | NSA 3600 Test2Domain | Warning: Warranty License for NSA 3600 Test2Domain on Sunday, November 4, 2018 10:31:37 AM IST (2018-11-04 05:01:37 UTC) | |
| Information | NSA 3600 Test2Domain | Information: VirusGT-2 for NSA 3600 Test2Domain on Tuesday, November 6, 2018 12:01:07 AM IST (2018-11-05 18:31:07 UTC) | Details |

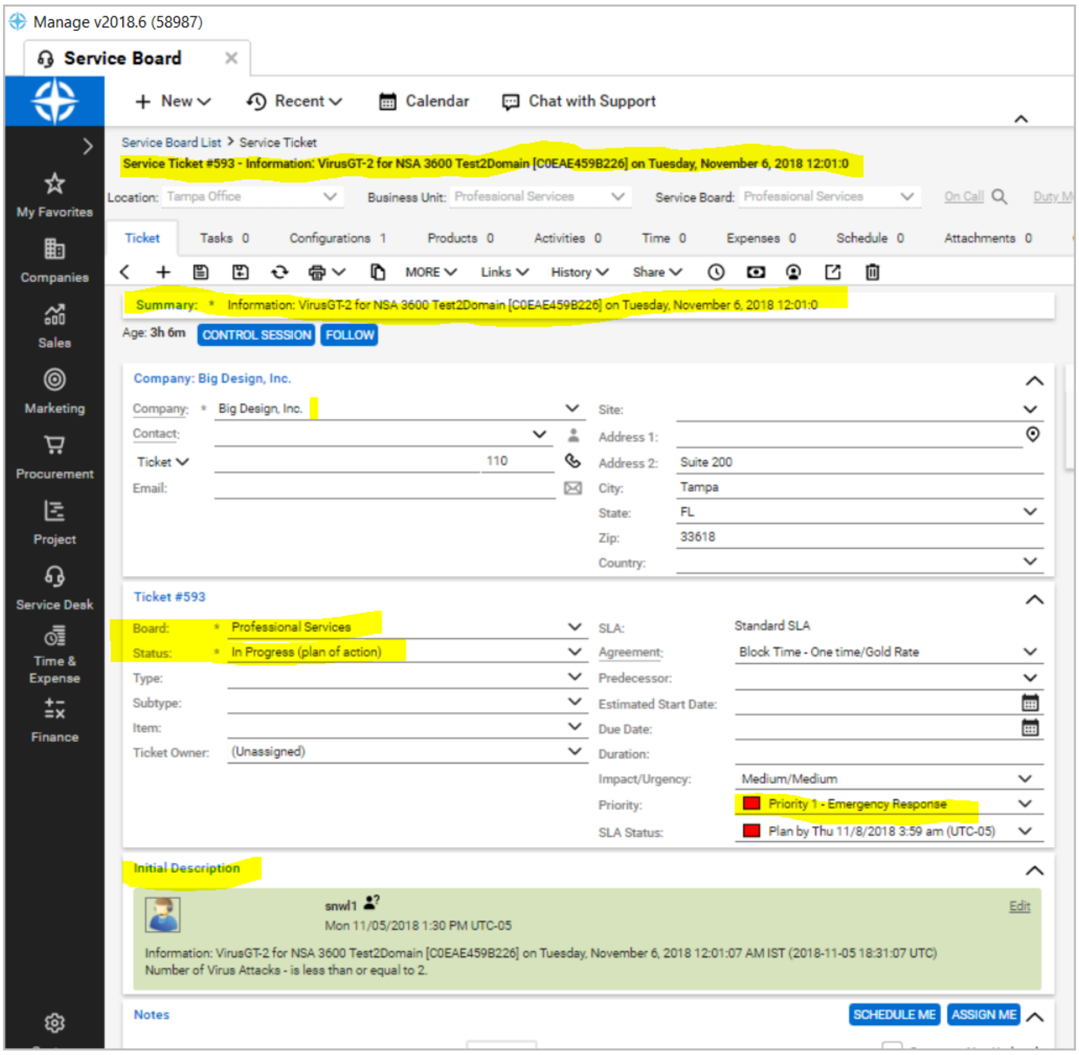
10.5.36.66/sgms/alertTickets.jsp - Google Chrome

Not secure | 10.5.36.66/sgms/alertTickets.jsp

Ticket Details

| | |
|---|---|
| Ticket ID: | 593 |
| Service Boards: | Professional Services |
| Company: | Big Design, Inc. |
| Ticket Status: | In Progress (plan of action) |
| Ticket Priority: | Priority 1 - Emergency Response |

3 In ConnectWise Manage at **Service Board List > Service Ticket**, locate the same Ticket ID as found in GMS to view the status, summary, priority, and description of the ticket and related information.



Service Board List > Service Ticket

Service Ticket #593 - Information: VirusGT-2 for NSA 3600 Test2Domain [C0EAE459B226] on Tuesday, November 6, 2018 12:01:0

Location: Tampa Office
Business Unit: Professional Services
Service Board: Professional Services

Summary: * Information: VirusGT-2 for NSA 3600 Test2Domain [C0EAE459B226] on Tuesday, November 6, 2018 12:01:0

Age: 3h 6m

Company: Big Design, Inc.

Company: * Big Design, Inc.
Contact:
Ticket 110
Email:
Site:
Address 1:
Address 2: Suite 200
City: Tampa
State: FL
Zip: 33618
Country:

Ticket #593

Board: * Professional Services
Status: * In Progress (plan of action)
Type:
Subtype:
Item:
Ticket Owner: (Unassigned)
SLA: Standard SLA
Agreement: Block Time - One time/Gold Rate
Predecessor:
Estimated Start Date:
Due Date:
Duration:
Impact/Urgency: Medium/Medium
Priority: 🟥 Priority 1 - Emergency Response
SLA Status: 🟥 Plan by Thu 11/8/2018 3:59 am (UTC-05)

Initial Description

snwl1
Mon 11/05/2018 1:30 PM UTC-05

Information: VirusGT-2 for NSA 3600 Test2Domain [C0EAE459B226] on Tuesday, November 6, 2018 12:01:07 AM IST (2018-11-05 18:31:07 UTC)
Number of Virus Attacks - is less than or equal to 2.

4 In ConnectWise Manage, make assignments and scheduling solutions and then click **Schedule Me** or **Assign Me** as appropriate.

## Deleting ConnectWise from GMS

Upon unit deletion, the ConnectWise configuration is also deleted.

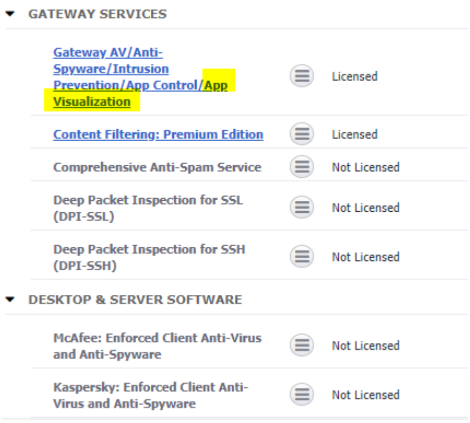
# Firewall Sandwich Group Reporting

GMS 8.7 introduces Firewall Sandwich Group Reporting to complement the Sandwich support added in GMS 8.6 by adding flow-based group reporting to firewalls using the Sandwich mode. This can provide aggregate reports at the Sandwich level.

**NOTE:** This feature is only enabled for flow-based reporting.

## Prerequisites:

Firewalls included in a Sandwich must have the App Visualization license enabled.



| GATEWAY SERVICES | |
|---|---|
| Gateway AV/Anti-Spyware/Intrusion Prevention/App Control/App Visualization | Licensed |
| Content Filtering: Premium Edition | Licensed |
| Comprehensive Anti-Spam Service | Not Licensed |
| Deep Packet Inspection for SSL (DPI-SSL) | Not Licensed |
| Deep Packet Inspection for SSH (DPI-SSH) | Not Licensed |
| **DESKTOP & SERVER SOFTWARE** | |
| McAfee: Enforced Client Anti-Virus and Anti-Spyware | Not Licensed |
| Kaspersky: Enforced Client Anti-Virus and Anti-Spyware | Not Licensed |

**Topics:**

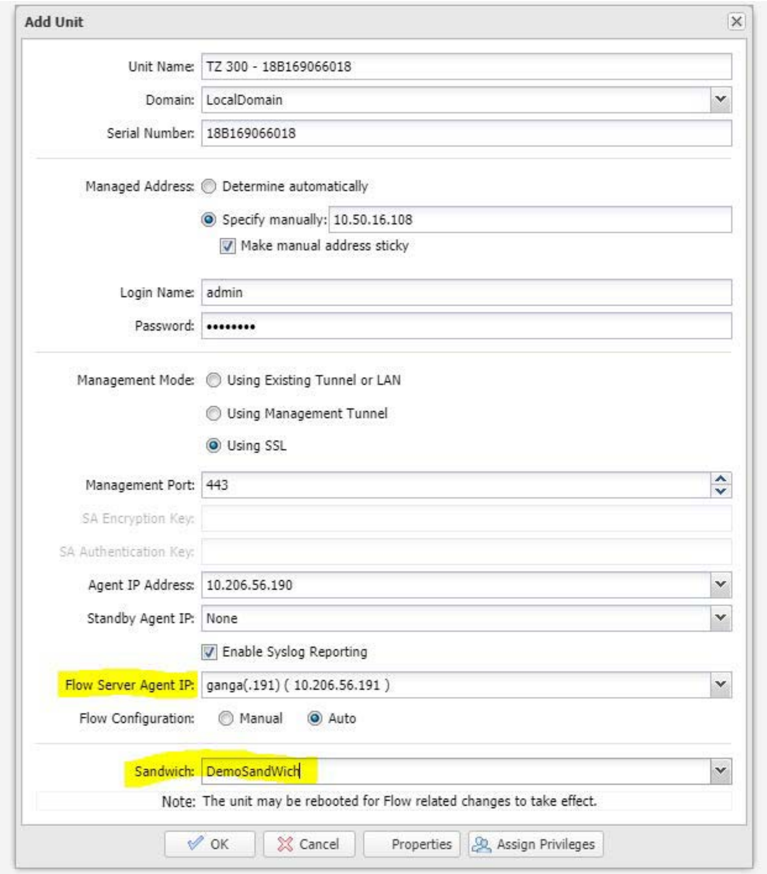
- Adding a Sandwich

# Adding a Sandwich

When adding a unit, first ensure that your deployment includes a flow server, and then you can choose an existing Sandwich or create a new one. When adding a new sandwich, the firewall serial number is assigned to the sandwich. The firewall and sandwich meta information is then added to the flow agent.

1 From the top button bar option in GMS, click the **+** icon, or right-click on the name of a firewall group or a specific firewall and select **Add Unit**.

The Add Unit feature shows the existing sandwiches that are available based on the chosen flow agents.



**Add Unit**

Unit Name: TZ 300 - 18B169066018

Domain: LocalDomain

Serial Number: 18B169066018

Managed Address: ○ Determine automatically

● Specify manually: 10.50.16.108

☑ Make manual address sticky

Login Name: admin

Password: ••••••••

Management Mode: ○ Using Existing Tunnel or LAN

○ Using Management Tunnel

● Using SSL

Management Port: 443

SA Encryption Key:

SA Authentication Key:

Agent IP Address: 10.206.56.190

Standby Agent IP: None

☑ Enable Syslog Reporting

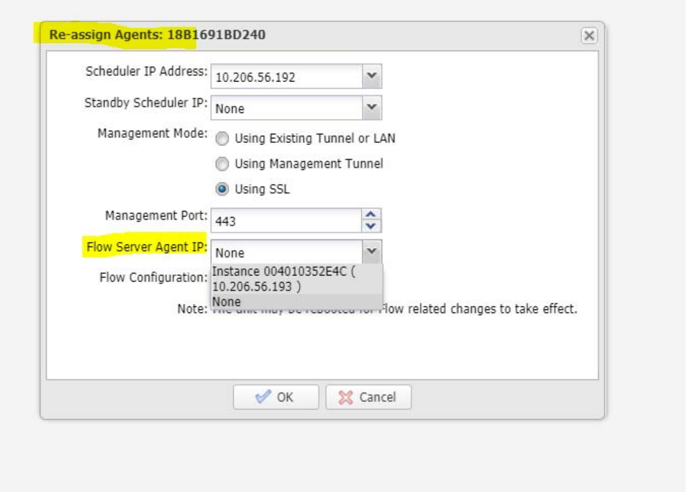
Flow Server Agent IP: ganga(.191) ( 10.206.56.191 )

Flow Configuration: ○ Manual ● Auto

Sandwich: DemoSandWich

Note: The unit may be rebooted for Flow related changes to take effect.

2 Ensure you have chosen the **Flow Server Agent IP** and the **Sandwich** name. (You can also edit the Flow Agent Server IP and the Sandwich later in the Re-assign agents dialog). You must have two firewalls assigned in a Sandwich for this feature to function correctly.



**Re-assign Agents: 18B1691BD240**

Scheduler IP Address: 10.206.56.192

Standby Scheduler IP: None

Management Mode: ○ Using Existing Tunnel or LAN

○ Using Management Tunnel

● Using SSL

Management Port: 443

Flow Server Agent IP: None

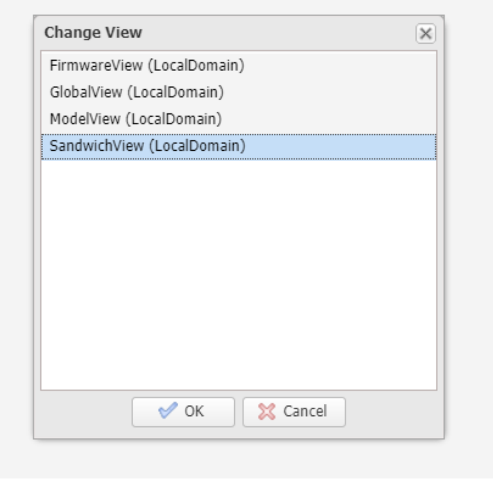
Instance 004010352E4C ( 10.206.56.193 )

None

Flow Configuration:

Note: low related changes to take effect.

3 Change to the **SandwichView**.


Change View

FirmwareView (LocalDomain)
GlobalView (LocalDomain)
ModelView (LocalDomain)
SandwichView (LocalDomain)

You can generate some IPFIX traffic though these firewalls to verify that the data is aggregating for the Sandwich report.

# Group Level Interface Support

The **FIREWALL | Manage | Network > Interfaces** page includes interface objects that have been directly linked to physical interfaces. The firewall scheme of interface addressing works in conjunction with network zones and address objects.

The interface configuration of the firewall data ports enables traffic to enter and exit the firewall. Interfaces in the firewall can be:

- **Interfaces** – Physical interfaces that are bound to a single port.
- **VLAN Interfaces** – Virtual interfaces are assigned as subinterfaces to a physical interface and that allows the physical interface to carry traffic assigned to multiple interfaces.

Previously, GMS already allowed you to configure both physical and virtual interfaces at the unit level, but only a few fields were configurable at the group level. The feature can now configure both interface types at the group level.

VLAN IDs range from 0 – 4094, with the following restrictions:

- VLAN 0 is reserved for QoS
- VLAN 1 is reserved by some switches for native VLAN designation

The group Level feature is supported on the following interfaces.

| | |
|---|---|
| **LAN Interface** | • Static IP Mode support<br>• Transparent IP Mode support (Splice L3 Subnet)<br>• Layer-2 Bridged Mode (IP Route Option) support<br>• Wire Mode support<br>• Tap Mode support<br>• IP Unnumbered Mode support<br>• PortShield Switch Mode support<br>• NativeBridge Mode support |
| **WAN Interface** | • Static Mode support<br>• DHCP Mode support<br>• PPoE Mode support<br>• Wire Mode support<br>• Tap Mode support<br>• PPTP Mode support<br>• L2TP Mode support |
| **WLAN Interface** | • Static IP Mode support<br>• Layer-2 Bridged Mode (IP Route Option) support<br>• PortShield Switch Mode support<br>• NativeBridge Mode support |
| **Tunnel Interface** | • IPv4 Tunnel Interface at the Group Level |

# Group Level Reporting

GMS 8.7 introduces Sandwich Group Level Reporting to complement the Sandwich Support that was added in GMS 8.6. When you click the Sandwich, it reveals logs that include all the firewalls belonging to that particular sandwich.

**Topics:**

- Adding a Sandwich
- Modifying a Sandwich
- Sandwich Reporting

## Adding a Sandwich

When adding a unit, choose an existing Sandwich or create a new one. When adding a new sandwich, the firewall serial number is assigned to the sandwich. The firewall and sandwich meta information is then added to the flow agent.

The **Add Unit** feature shows the existing sandwiches that are available based on the chosen flow agents.

## Modifying a Sandwich

Select the sandwich you would like to change using **Modify Unit**. Make the changes and save the result. If you want to move the firewall between two sandwiches, first delete and then re-add the firewall to the new location.

## Sandwich Reporting

All unit level reports are shown at the Sandwich level. Logs show results from all firewalls that belong to the sandwich. When reporting on a sandwich, Appflow is activated to generate data for the sandwich.

# Adding, Modifying, and Reassigning Agent Screens

A firewall Sandwich can be included with only one Flow Server ID, but a Flow Server ID can include multiple firewalls.

**Topics:**

- Adding a Unit
- Modifying a Unit
- Re-Assigning Flow Agents

## Adding a Unit

When Reporting is enabled and the Flow Server ID is selected, choose from the following options:

- A list of firewalls that the Flow Server ID includes
- All firewalls that can be added

When the Flow Server ID is NOT assigned, then the firewalls cannot be assigned either (grayed out in the field). Firewalls can only be assigned through with the Modifying Unit action (see below).

## Modifying a Unit

When reporting is enabled, the Flow Server ID is selected or assigned, and the firewalls have not previously been assigned, choose from the following options:

- A list of firewalls that the Flow Server ID includes
- All firewalls that can be added

If the firewall has previously been assigned, the firewalls cannot be changed (the field is grayed out). See the tooltip that reads, “Value cannot be changed since the unit is already assigned to a Flow Agent and is part of the Sandwich.”

When Reporting is re-enabled, it becomes a Modify action when in the **None** state.

## Re?Assigning Flow Agents

If the firewall has not been previously assigned, re-assigning the flow agents is still possible. If the firewall has been previously assigned, you should complete the flow-agent assignment as follows, (but choosing **None** is also permitted):

- From the drop-down menu, select **Current Sandwich** or **None**.
- If you selected **None**, then the sandwich must be changed to the default value (equivalent of **None** for the serial port).

# Web Activity Reports Showing URLs

URL-based reports have been added to GMS and are used to reveal the details of all URLs visited by a particular user. These reports are schedulable.

## URLs by Initiators and URLs by Sites

URL-based reports show the details of all URLS visited by each user, as well as the various URLs that are under a particular site. These reports must be scheduled and include sections and section columns to help organize data.

## Summary Reports

Summary reports can be generated by using referer tags. The reporting database now includes a referer column to help organize data.

# Version Upgrades for Tomcat and MySQL

GMS is compatible with the upgraded and improved versions of Apache Tomcat 9.0 and the latest MySQL.

# SonicOS 6.5.3 Support

This section describes the supported features introduced in SonicOS 6.5.3.1.

**Topics:**

- SD-WAN Features
- Automatic Guest Redirection to Policy Page
- Networking Features
- Wireless Features
- Authentication Features
- Advanced Security Features
- GMS API Enhancements
- External Storage of Trace Logs
- OpenSSL Support
- Configurable Internal VLANs
- 4G/LTE USB Modem Support
- IPv6 Addressing Mode for H.323 ALG
- Enhancements to Reports
- Switch Shield Support (DDOS Protection using Switch Capabilities)
- Pin Friendly Name of Firewall

# SD-WAN Features

SD-WAN (Software-Defined Wide Area Network) provides software-based control over wide area network (WAN) connections. SD-WAN offers these features:

- Application-aware routing
- Dynamic path selection based on:
  - Latency, jitter, and/or packet loss
  - User-defined thresholds for quality assessment
- SD-WAN Interface Groups
  - WAN and VPN
  - Scalable from one to *N* interfaces

- Path Performance Probes for metrics
- Connection-based traffic distribution
- Automatic connection failover over VPN
- Provisioning and management (GMS and Capture Security Center)

SD-WAN is best used for specific traffic types and/or applications requiring dynamically chosen optimal destination interfaces depending on how the network paths are behaving. To operate well, each application has a certain requirement from the network path. For example the network quality for VoIP to operate well requires the optimal latency be 100 ms or less while a latency of 150 ms or higher results in choppy calls. SD-WAN helps in such scenarios by first dynamically measuring the various network performance metrics, such as latency, jitter and packet loss, on multiple network paths. SD-WAN then compares these metrics with the performance threshold for a particular traffic flow and determines the optimal network that meets the flow's network quality accordingly.

GMS supports SD-WAN through several new management interface pages located at **FIREWALL | Manage > SD-WAN**.

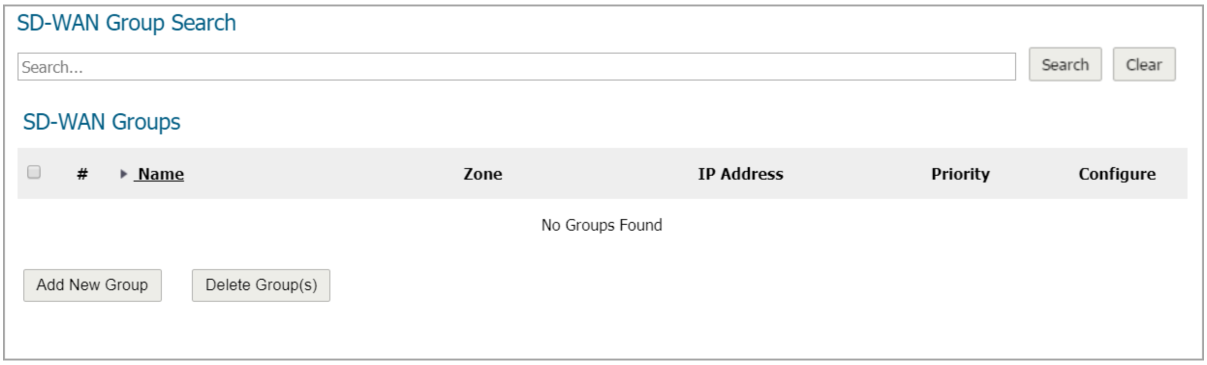
**Topics:**

- SD-WAN Groups
- Performance Probes
- Monitoring the Performance Probes
- Performance Class Objects
- Path Selection Profiles
- SD-WAN Routing
- Monitoring SD-WAN
- Viewing SD-WAN Route Policy Connections

# SD-WAN Groups

SD-WAN Groups are logical groups of interfaces that can be used for load-balancing as well as dynamic path selection based on the performance criterion through each interface path. You can create your own custom groups.

The **SD-WAN Groups** page displays the custom pool of interfaces used for optimized and resilient traffic flow.



SD-WAN Group Search

Search...

Search Clear

SD-WAN Groups

| □ | # | Name | Zone | IP Address | Priority | Configure |
|---|---|---|---|---|---|---|

No Groups Found

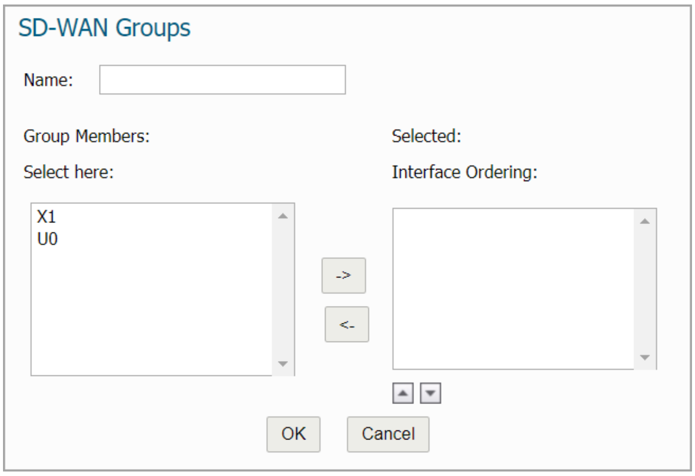
Add New Group Delete Group(s)

You can create multiple SD-WAN Groups to meet your requirements.

***To add an SD-WAN group:***

1 Navigate to **FIREWALL | Manage > SD-WAN > SD-WAN Groups**.

2 Click **Add New Group**. The **Add SD-WAN Group** dialog displays.



3 Enter a descriptive name in the **Name** field.

4 Select one or more interfaces from the **Group Members Select here** column. Member interfaces can be only WAN or Numbered Tunnel Interfaces.

> **IMPORTANT:** An interface cannot be a member of more than one SD-WAN group.

5 Click the **Right Arrow** to move the selected interfaces to the **Selected Interface Ordering** column.

6 To change the priority of the selected group members:

a Select the interface.

b Click the **Up Arrow** or **Down Arrow**.

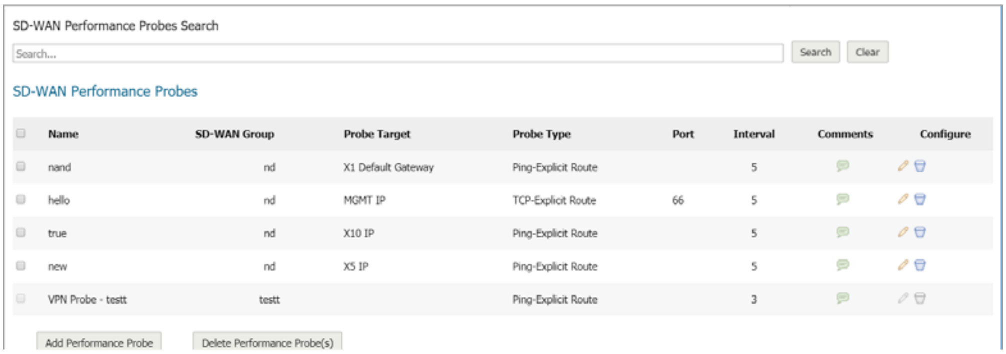
7 Repeat Step 6 for each interface to prioritize.

8 Click **OK**.

# Performance Probes

Network path performance metrics are determined using SD-WAN performance probes, which are similar to Network Monitor Probes. GMS supports ICMP and TCP probe types. A SD-WAN performance probe can be used by multiple Path Selection profiles.

The **FIREWALL | Manage > SD-WAN > Performance Probes** page shows the dynamic performance data (latency/jitter/packet loss) and probe status for each path (interface) in the SD-WAN group, in both tabular and graphic displays. The display can show data for the last minute (default), last day, last week, or last month.


SD-WAN Performance Probes Search
Search...
Search
Clear
SD-WAN Performance Probes

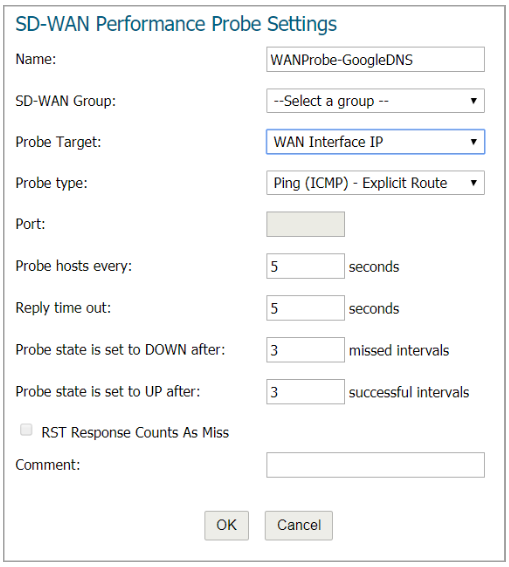
| □ | Name | SD-WAN Group | Probe Target | Probe Type | Port | Interval | Comments | Configure |
|---|---|---|---|---|---|---|---|---|
| □ | nand | nd | X1 Default Gateway | Ping-Explicit Route | | 5 | | |
| □ | hello | nd | MGMT IP | TCP-Explicit Route | 66 | 5 | | |
| □ | true | nd | X10 IP | Ping-Explicit Route | | 5 | | |
| □ | new | nd | X5 IP | Ping-Explicit Route | | 5 | | |
| □ | VPN Probe - testt | testt | | Ping-Explicit Route | | 3 | | |

Add Performance Probe
Delete Performance Probe(s)

***To add a performance probe:***

1 Navigate to **FIREWALL | Manage > SD-WAN > Performance Probes**.

2 Click **Add Performance Probe**. The **Add SD-WAN Performance Probe** dialog displays.



SD-WAN Performance Probe Settings

Name: WANProbe-GoogleDNS

SD-WAN Group: --Select a group --

Probe Target: WAN Interface IP

Probe type: Ping (ICMP) - Explicit Route

Port:

Probe hosts every: 5 seconds

Reply time out: 5 seconds

Probe state is set to DOWN after: 3 missed intervals

Probe state is set to UP after: 3 successful intervals

□ RST Response Counts As Miss

Comment:

3 Enter a meaningful name in the **Name** field.

4 Select a SD-WAN group from **SD-WAN Group**.

5 Select an address object from **Probe Target**.

6 From **Probe Type**, select:

- **Ping (ICMP) - Explicit Route** (default); go to Step 8.
- **TCP - Explicit Route**; the Port field becomes available.

7 Enter the port number of the explicit route in the **Port** field. Values can range from 1 - 65535.

8 Enter the interval between probes in the **Probe hosts every … seconds** field. The minimum is 1 second, the maximum is 3600 seconds, and the default is **3** seconds.

> **TIP:** The probe interval must be greater than the reply timeout.

9 Enter the maximum delay for a response in the **Reply time out … seconds** field. The minimum is 1 second, the maximum is 60 seconds, and the default is **1** second.

10 Enter the maximum number of missed intervals before the probe is set to the DOWN state in the **Probe state is set to DOWN after … missed intervals** field. The minimum number is 1, the maximum is 100, and the default is **3**.

11 Enter the maximum number of successful intervals before the probe is set to the UP state in the **Probe state is set to UP after … successful intervals** field. The minimum number is 1, the maximum is 100, and the default is **1**.

12 If you selected **TCP - Explicit Route** for **Probe Type**, the **RST Response Counts As Miss** and **Port** options become available. Select the option to count RST responses as missed intervals. This option is not selected by default. Port values can range from 1 - 65535.

13 Optionally, enter a comment in the **Comment** field.

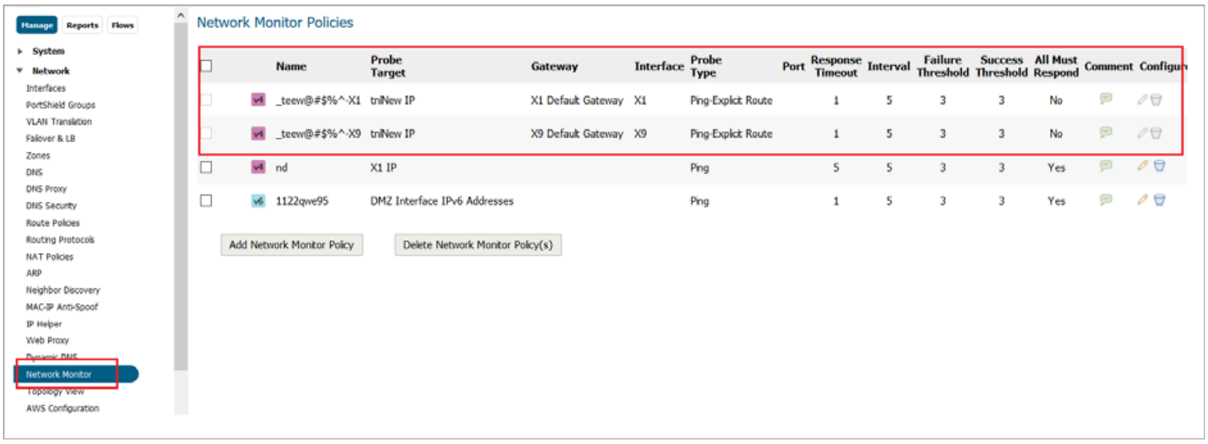
14 Click **OK**.

15 Repeat Step 3 through Step 14 to add more probes.

16 Click **CLOSE**.

# Monitoring the Performance Probes

When you create Performance Probes, default rows are also created in Net Monitor for each of the interfaces used by the SD-WAN group. Navigate to **FIREWALL | Manage | Network > Network Monitor** to see the Performance Probe details.



Network Monitor Policies

| ☐ | | Name | Probe Target | Gateway | Interface | Probe Type | Port | Response Timeout | Interval | Failure Threshold | Success Threshold | All Must Respond | Comment | Configu |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | v4 | _teew@#$%^-X1 | tnlNew IP | X1 Default Gateway | X1 | Ping-Explicit Route | | 1 | 5 | 3 | 3 | No | | |
| ☐ | v4 | _teew@#$%^-X9 | tnlNew IP | X9 Default Gateway | X9 | Ping-Explicit Route | | 1 | 5 | 3 | 3 | No | | |
| ☐ | v4 | nd | X1 IP | | | Ping | | 5 | 5 | 3 | 3 | Yes | | |
| ☐ | v6 | 1122qwe95 | DMZ Interface IPv6 Addresses | | | Ping | | 1 | 5 | 3 | 3 | Yes | | |

Add Network Monitor Policy | Delete Network Monitor Policy(s)

# Performance Class Objects

A Performance Class specifies the performance criterion for selecting the optimal path. It could be the:

- Best latency/jitter/packet loss among the existing paths.
- Performance class object that defines the metric thresholds for latency, jitter and packet loss.

Use SD-WAN Performance Class Objects to configure the desired performance characteristics for the application/traffic categories. These objects are used in the Path Selection Profile to automate the selection of paths based on these metrics.

There are three Performance Class Objects:

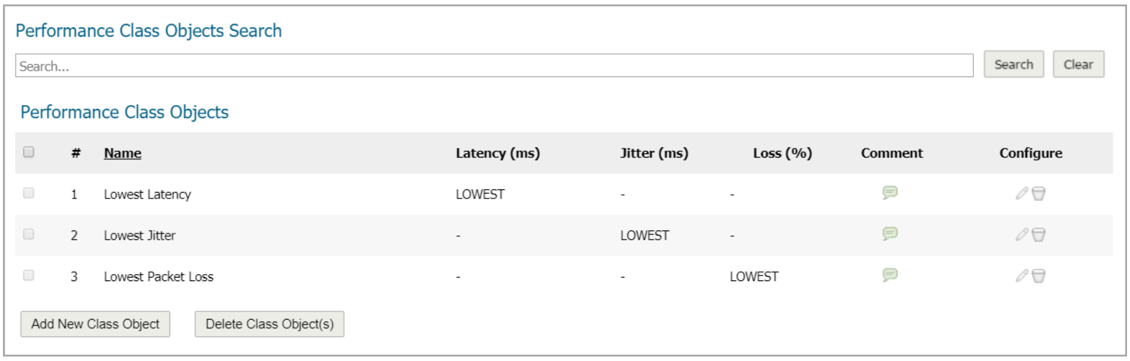
- **Latency (ms)**
- **Jitter (ms)**
- **Loss (%)**

**NOTE:** These default Performance Class Objects cannot be edited or deleted.

Configure custom performance thresholds that best meet the needs of your application or traffic categories with Performance Class Objects.

***To add a Performance Class Object:***

1 Navigate to **FIREWALL | Manage > SD-WAN > Performance Class Object**.



Performance Class Objects Search

Search...

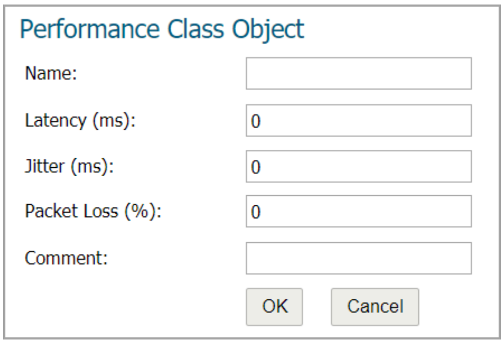
Search | Clear

Performance Class Objects

| ☐ | # | Name | Latency (ms) | Jitter (ms) | Loss (%) | Comment | Configure |
|---|---|---|---|---|---|---|---|
| ☐ | 1 | Lowest Latency | LOWEST | - | - | | |
| ☐ | 2 | Lowest Jitter | - | LOWEST | - | | |
| ☐ | 3 | Lowest Packet Loss | - | - | LOWEST | | |

Add New Class Object | Delete Class Object(s)

2 Click **Add New Class Object**. The **Add Performance Class Object** dialog displays.



Performance Class Object

| | |
|---|---|
| Name: | |
| Latency (ms): | 0 |
| Jitter (ms): | 0 |
| Packet Loss (%): | 0 |
| Comment: | |

3 Enter a meaningful name in the **Name** field.

4 Enter the acceptable latency, in milliseconds, in the **Latency (ms)** field. The minimum is 0 milliseconds, the maximum is 1000, and the default is **0**.

5 Enter the acceptable jitter, in milliseconds, in the **Jitter (ms)** field. The minimum is 0 milliseconds, the maximum is 100 milliseconds, and the default is **0** milliseconds.

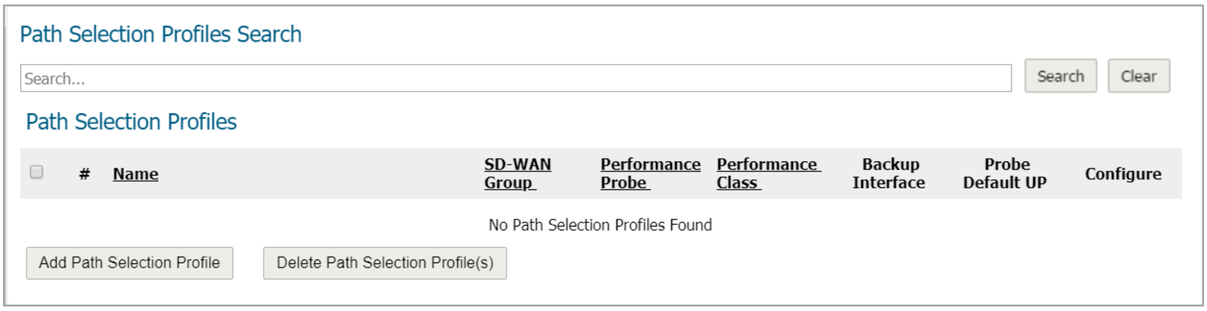
6 Enter the acceptable percentage of packet loss in the **Packet Loss (%)** field. The minimum is 0, the maximum is 100, and the default is **0**.

7 Optionally, enter a comment in the **Comment** field.

8 Click **OK**.

# Path Selection Profiles

Path Selection Profiles (PSPs) are the settings that help to determine the network path that satisfies a specific network performance criteria, from a pool of available network paths. The dynamic path selection mechanism is implemented using the PSP settings when they are associated with Policy Based Routes (PBR). When more than one network path meets the criterion (as per the performance class in the PSP), then traffic is load balanced among the network paths. When associated with a policy-based routing policy, a path selection profile helps select the optimal path among the SD-WAN interfaces for the application or service.



Path Selection Profiles Search

Search...

Path Selection Profiles

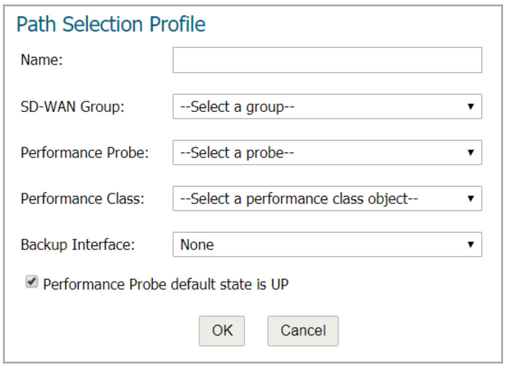
| □ | # | Name | SD-WAN Group | Performance Probe | Performance Class | Backup Interface | Probe Default UP | Configure |
|---|---|---|---|---|---|---|---|---|

No Path Selection Profiles Found

*To add a Performance Class Object:*

1 Navigate to **FIREWALL | Manage > SD-WAN > Path Selection Profiles**.

2 Click **Add Path Selection Profile**. The **Add Path Selection Profile** dialog displays.



Path Selection Profile

Name:

SD-WAN Group: --Select a group--

Performance Probe: --Select a probe--

Performance Class: --Select a performance class object--

Backup Interface: None

☑ Performance Probe default state is UP

3 Add a meaningful name in the **Name** field.

4 From **SD-WAN Group**, select the group to which the profile applies.

5 From **Performance Probe**, select the probe to use in the profile.

6 From **Performance Class**, select the Performance Class Object for the dynamic selection of the optimal network path:

- **Lowest Latency**
- **Lowest Jitter**
- **Lowest Packet Loss**
- **Custom Performance Class Object**

7 From **Backup Interface**, select the interface to use when all the SD-WAN Group interfaces fail to meet the performance criteria specified **Performance Class**; in or all the interfaces are down:

- **None** (default)
- Individual interfaces
- **Drop_TunnelIf**

8 To specify whether the default state of the performance probe should be treated as Up, select **Performance Probe default state is UP**. If this option is not selected, the performance probe is treated as DOWN. This option is selected by default.

9 Click **OK**.

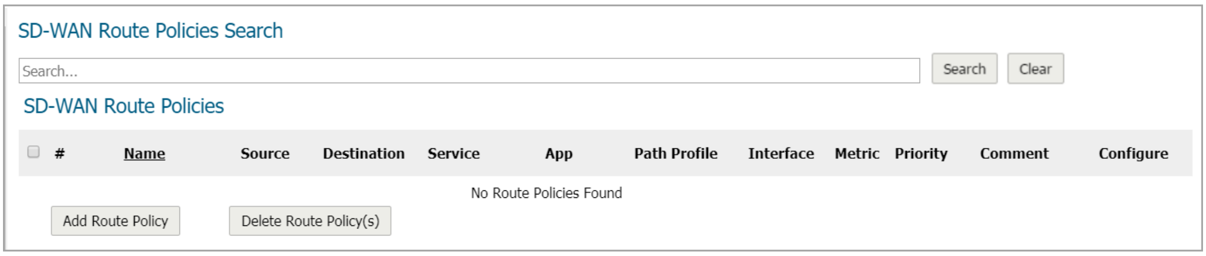
10 To add more Path Selection Profiles, repeat Step 3 through Step 9 for each additional profile.

11 Click **CLOSE**.

# SD-WAN Routing

Dynamic Path selection for specific traffic flows uses Policy Based Routes. A SD-WAN Policy Based Route is used to configure the route policy for the specific source/destination service/app combination, with a corresponding Path Selection Profile that determines the outgoing path dynamically based on the Path Selection Profile. If there is more than one path qualified by the Path Selection Profile, the traffic is automatically load balanced among the qualified paths. If none of the paths are qualified by the path selection profile and the backup interface in the profile is not configured or is down, the route is disabled.

SD-WAN routing can be configured from the **FIREWALL | Manage | Network > Route Policies** page or **FIREWALL | Manage > SD-WAN > SD-WAN Routing** page. The **SD-WAN > SD-WAN Routing** page only shows the SD-WAN Routes and only allows configuration of SD-WAN-type routes.



SD-WAN Route Policies Search

Search...

SD-WAN Route Policies

| □ | # | Name | Source | Destination | Service | App | Path Profile | Interface | Metric | Priority | Comment | Configure |
|---|---|---|---|---|---|---|---|---|---|---|---|---|

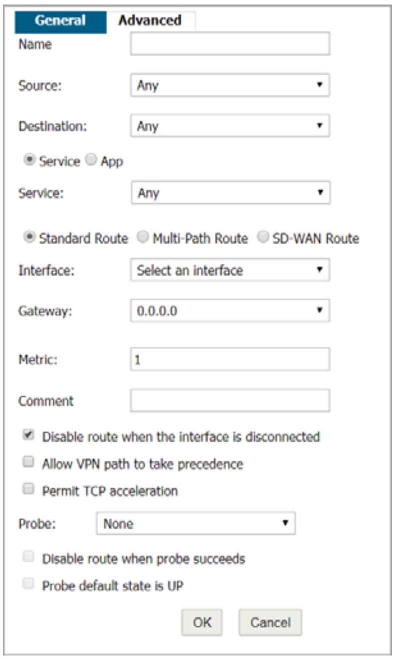
No Route Policies Found

***To add an SD-WAN route policy:***

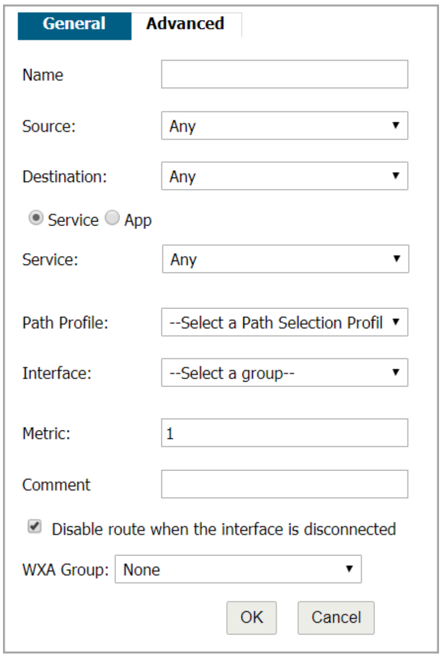
1 Navigate to **FIREWALL | Manage > SD-WAN > SD-WAN Routing**.

2 Click **Add Route Policy**. The **Add SD-WAN Route Policy** dialog displays.

> **IMPORTANT:** When configuring an SD-WAN route from the **FIREWALL | Manage > Network > Route Policies** page, choose **SD-WAN Route** on the **Add Route Policy** dialog; the options change to match those of the **Add SD-WAN Route Policy** dialog.



Name
Source: Any
Destination: Any
● Service ○ App
Service: Any
● Standard Route ○ Multi-Path Route ○ SD-WAN Route
Interface: Select an interface
Gateway: 0.0.0.0
Metric: 1
Comment
☑ Disable route when the interface is disconnected
□ Allow VPN path to take precedence
□ Permit TCP acceleration
Probe: None
□ Disable route when probe succeeds
□ Probe default state is UP

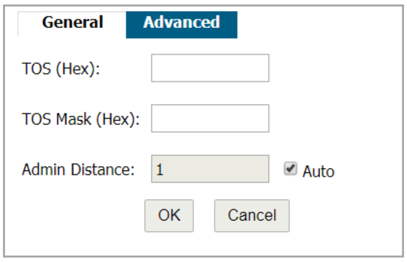


Name
Source: Any
Destination: Any
● Service ○ App
Service: Any
Path Profile: --Select a Path Selection Profil
Interface: --Select a group--
Metric: 1
Comment
☑ Disable route when the interface is disconnected
WXA Group: None

3 Configure the options as you would for a regular route.

> **NOTE:** The **Interface** and **Disable route when the interface is disconnected** options are dimmed because these options cannot be edited in SD-WAN policies. The **Interface** option is populated with the SD-WAN group name in the associated Path Selection Profile (PSP) and cannot be changed. The interface for the SD-WAN route is selected from the SD-WAN group that is part of the PSP associated with the SD-WAN route and, therefore, cannot be configured.

4  Click **Advanced**.



General | Advanced

TOS (Hex):

TOS Mask (Hex):

Admin Distance: 1 ☑ Auto

5  Configure the options as you would for a regular route.

6  Click **OK**.

# Monitoring SD-WAN

The (software defined) SD-WAN solution allows you to steer traffic away from latency issues, remotely detect optimal traffic routes for your data packets, and then send those packets automatically through preapproved network pipes based on your own configuration settings. You can monitor SD-WAN traffic from the **MONITOR | SD-WAN Monitor** page:

- **Latency**

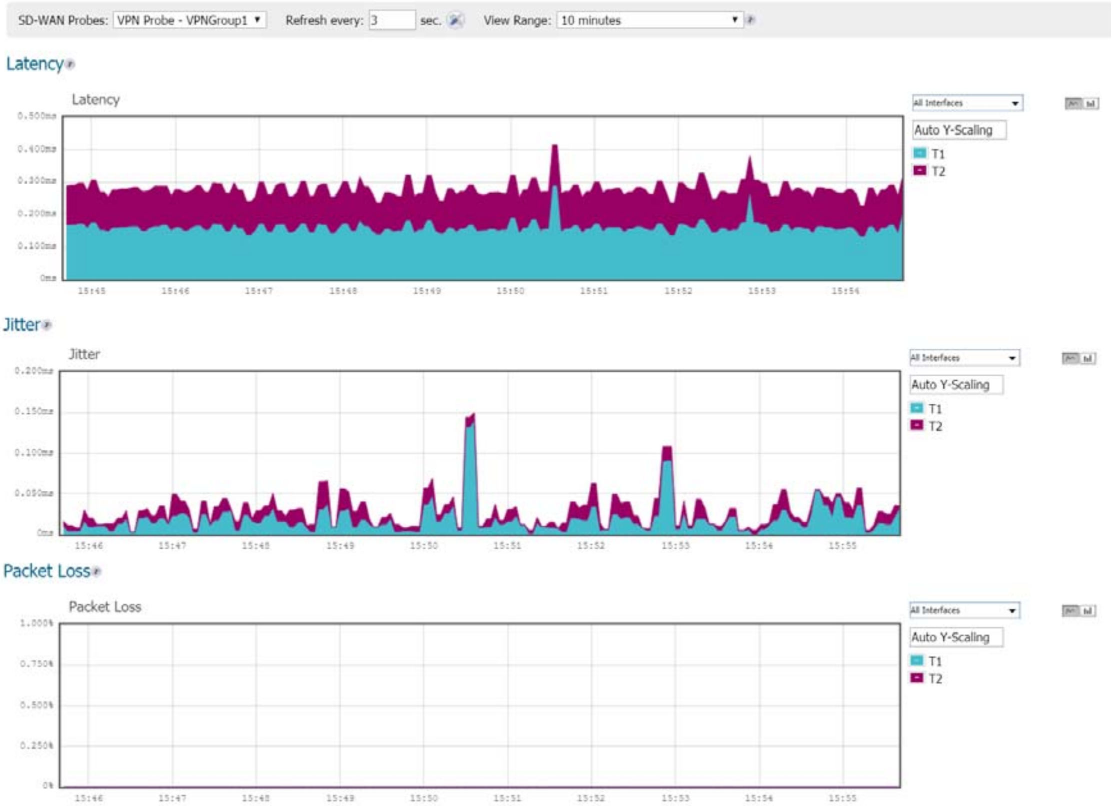
  This probe delivers a clear view into your network pipes by showing the time required for a packet of data to travel across your network on its way to its final destination. High latency times are blamed for poor communication, work disruption, and result in a negative end-user experience, or negative impact to your network. Monitoring latency helps you detect trouble areas in real-time so that you can avoid them when sending packets. This allows you to pinpoint and fix traffic issues quickly without a lot of disruption.

- **Jitter**

The jitter probe provides a real-time view into any disruptions happening to the data flow across your network. These disruptions usually occur because of network traffic jams, improper packet queuing, and setup errors. SD-WAN allows you to remotely detect optimal traffic routes for your data packets.

- **Packet Loss**

  Packet loss can greatly affect your performance for the worse. Packet loss occurs when your sent packets do not reach their intended destinations. Your network could experience packet loss because of faulty cabling, strained bandwidth, or software problems.



SD-WAN Probes: VPN Probe - VPNGroup1 Refresh every: 3 sec. View Range: 10 minutes

**NOTE:** A chart could be empty or blank if no recent data entries are received within the viewing range.

### *To monitor SD-WAN performance:*

1 Navigate to **MONITOR | SD-WAN Monitor.**

2 From the **SD-WAN Probes** drop-down menu, select the performance probe you would like to use to monitor.

3 Indicate the Refresh rate in seconds in the **Refresh every:** field.

4 Select a **View Range**. Options include **60 seconds**, **2 Minutes**, **5 minutes**, and **10 minutes** (default).

5 Choose an interface to track or select **All Interfaces** from the drop-down menu on the right side.

6 For scaling ratios, you can enter values such as:

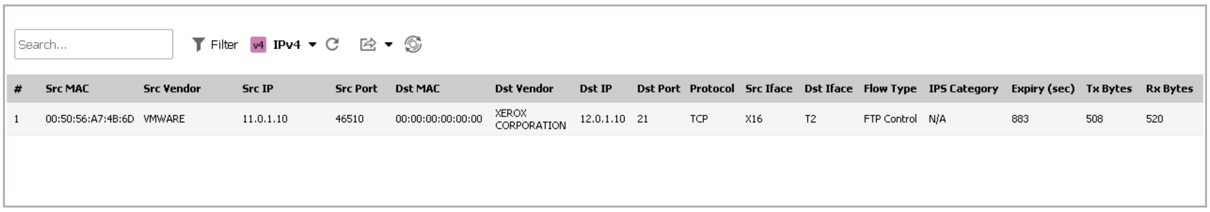
- **Auto** - Auto Y-Scaling
- **<num>[<unit>]** - num is a numeric integer. The unit is optional but can also be empty, K for Kilo, M for Mega, G for Giga, or % for percentages.

  **NOTE:** An invalid value defaults to Auto Y-scaling.

7 The two small icons on the right allow you to toggle between line and block displays.

## Viewing SD-WAN Route Policy Connections

You can view the connections that have been associated with SD-WAN Route policies on the **FIREWALL | Manage | SD-WAN > SD-WAN Connection Logs** page.



| # | Src MAC | Src Vendor | Src IP | Src Port | Dst MAC | Dst Vendor | Dst IP | Dst Port | Protocol | Src Iface | Dst Iface | Flow Type | IPS Category | Expiry (sec) | Tx Bytes | Rx Bytes |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 00:50:56:A7:4B:6D | VMWARE | 11.0.1.10 | 46510 | 00:00:00:00:00:00 | XEROX CORPORATION | 12.0.1.10 | 21 | TCP | X16 | T2 | FTP Control | N/A | 883 | 508 | 520 |

# Automatic Guest Redirection to Policy Page

GMS allows you to redirect a guest automatically to your guest-user policy page. If you enable this feature, also known as the zero-touch policy page redirection, the guest user is redirected automatically to your guest-user policy page. If you disable the feature, the guest must click **Accept**.

***To enable automatic redirection to the user-policy page:***

1 Navigate to **FIREWALL | Manage | Network > Zones**.

2 Click either:

- **Add New Zone** to add a new zone.
- The **Edit** icon of an existing zone.

The **Add Zone/Edit Zone** dialog displays.

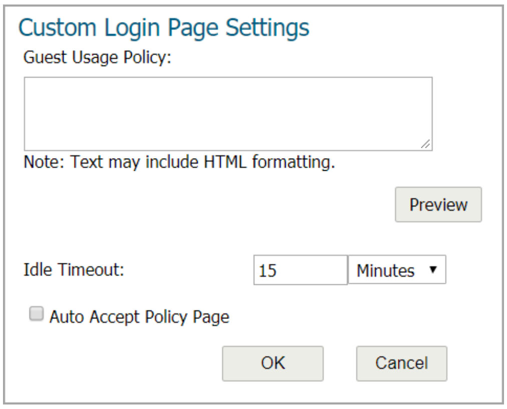
3 Select a **Security Type**, (Trusted, Public, or Wireless).

4 Click **Guest Services**.

5 Click **Enable Guest Services**.

6 Click **Enable Policy Page without authentication**.

7 Click **Configure**. The **Customize Policy Message** dialog displays.


Custom Login Page Settings

Guest Usage Policy:

Note: Text may include HTML formatting.

Idle Timeout: 15 Minutes

□ Auto Accept Policy Page

8 Select **Auto Accept Policy Page**. This option is not selected by default.

9 Click **OK**.

10 Finish configuring the zone.

11 Click **OK**.

# Networking Features

**Topics:**

- High Availability Encryption
- Support of Large-Scale Static and Dynamic Routes

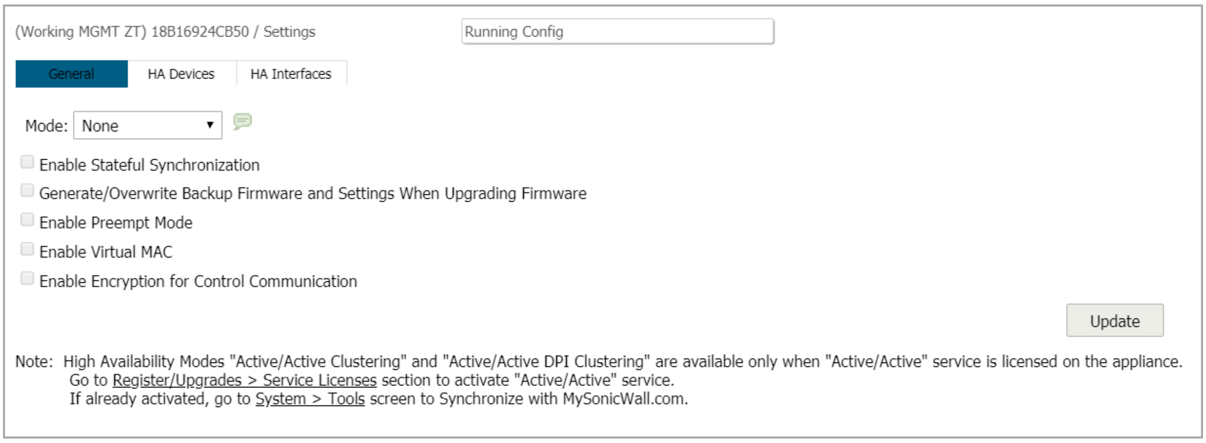
## High Availability Encryption

High Availability (HA) encryption adds security to the communication between appliances in an HA pair. HA controls messages between active and standby firewalls, such as heartbeats, configuration synchronization, and HA state information that are all encrypted to ensure security for inter-node communication.

This option is available in Active-Standby HA mode only and does not apply to messages exchanged for stateful synchronization even in Active-Standby mode. Discovery messages (find-peer and found-peer) are transmitted without encryption. After the discovery stage, however, all control messages are encrypted between the firewalls:

- Heartbeats
- Messages used for incremental configuration updates
- prefSync messages
- Various messages for sending HA commands between the firewall pair
- Firmware synchronization messages

To support this feature, the **Enable Encryption for Control Communication** option was added to **FIREWALL | Manage | High Availability > Settings**:



Mode: None

□ Enable Stateful Synchronization
□ Generate/Overwrite Backup Firmware and Settings When Upgrading Firmware
□ Enable Preempt Mode
□ Enable Virtual MAC
□ Enable Encryption for Control Communication

Note: High Availability Modes "Active/Active Clustering" and "Active/Active DPI Clustering" are available only when "Active/Active" service is licensed on the appliance.
Go to Register/Upgrades > Service Licenses section to activate "Active/Active" service.
If already activated, go to System > Tools screen to Synchronize with MySonicWall.com.

## Support of Large-Scale Static and Dynamic Routes

In previous versions of GMS, policy-based routing (PBR) works fine for static routes that are added, deleted, or modified very infrequently and in relatively small numbers. GMS increases performance with dynamic routing that adds, deletes, and modifies routes in the tens of thousands relatively quickly. This feature is transparent except for the addition of a **Tech Support Report** option on the **FIREWALL | Manage | Diagnostics > Network** page.

# Wireless Features

GMS introduces several new wireless features.

**Topics:**

- One-Click Wireless and Non-Wireless Controller Modes
- RF Spectrum Analysis with Real-Time Noise Detection
- Bluetooth Low Energy on SonicWave Series
- SonicWave 432 DFS
- WWAN Cards
- SonicWave Sensor Mode Enhancement
- NAS-ID Support using SSID
- Increase in SonicPoints/SonicWaves Supported

## One-Click Wireless and Non-Wireless Controller Modes

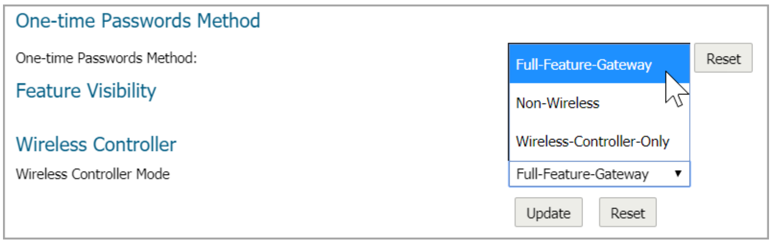
ⓘ **IMPORTANT:** When you change the **Wireless Controller Mode**, you must restart the firewall after clicking **UPDATE** on the **FIREWALL | Manage |System > Administrator** page.

This feature can enable or disable the Wireless Controller Mode as well as enable or disable all wireless functionality with just one click. GMS introduces **Wireless-Controller-Only** for deployments in which the firewall is being solely used for providing secure wireless access. Alternatively, you can select **Non-Wireless** mode for deployments in which the firewall should not provide any wireless access. **Full-Feature Gateway** mode, which allows all wireless and non-wireless functions, is the default.

This feature allows you to either:

- Enable **Wireless-Controller-Only** mode, which disables and renders uneditable:
  - SSL VPN and VPN zones.
  - Group VPN and SSL VPN policies as well as the updating of all zones using these policies.
  - VPN.
  - WAN Acceleration (WXA).
  - SIP and H.323 transformations.
- Enable **Non-Wireless** mode, which disables and renders uneditable:
  - Wireless zones, including the default WLAN zone, as well as disabling the creation of wireless zones.
  - Internal wireless functions.
  - Access points, including L2 and L3.

A new section, **Wireless Controller**, has been added to the **FIREWALL | Manage | System > Administrator** page.



One-time Passwords Method

One-time Passwords Method:

Feature Visibility

Wireless Controller

Wireless Controller Mode: Full-Feature-Gateway

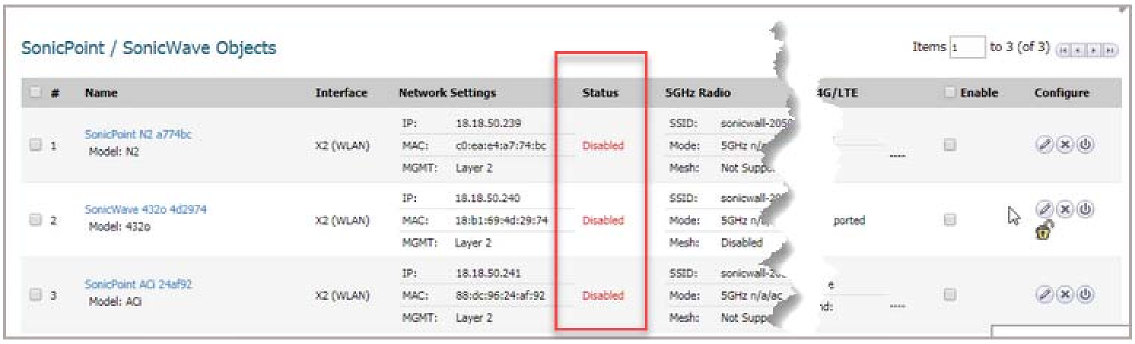
**Topics:**

- Effects of Enabling Non-Wireless Controller Mode
- Effects of Enabling Wireless Controller Mode
- Enabling Wireless Controller Mode
- Enabling Non-Wireless Controller Mode
- Enabling Full-Feature-Gateway Mode

## Effects of Enabling Non-Wireless Controller Mode

Enabling Non Wireless Mode affects several management interface pages.

- The **Edit** and **Delete** icons for wireless zones become dimmed on the **FIREWALL | Manage | Network > Zones** page.
- The status of access point objects becomes **Disabled** on the **FIREWALL | Manage | Access Points > SonicPoints** page.

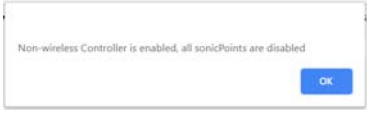


SonicPoint / SonicWave Objects

Items 1 to 3 (of 3)

| □ | # | Name | Interface | Network Settings | Status | 5GHz Radio | 4G/LTE | □ Enable | Configure |
|---|---|---|---|---|---|---|---|---|---|
| □ | 1 | SonicPoint N2 a774bc<br>Model: N2 | X2 (WLAN) | IP: 18.18.50.239<br>MAC: c0:ea:e4:a7:74:bc<br>MGMT: Layer 2 | Disabled | SSID: sonicwall-205<br>Mode: 5GHz n/<br>Mesh: Not Supp.. | ---- | □ | |
| □ | 2 | SonicWave 432o 4d2974<br>Model: 432o | X2 (WLAN) | IP: 18.18.50.240<br>MAC: 18:b1:69:4d:29:74<br>MGMT: Layer 2 | Disabled | SSID: sonicwall-2<br>Mode: 5GHz n/<br>Mesh: Disabled | ported | □ | |
| □ | 3 | SonicPoint ACi 24af92<br>Model: ACi | X2 (WLAN) | IP: 18.18.50.241<br>MAC: 88:dc:96:24:af:92<br>MGMT: Layer 2 | Disabled | SSID: sonicwall-2..<br>Mode: 5GHz n/a/ac<br>Mesh: Not Supp | e<br>d: ---- | □ | |

- Any attempt to enable an access point or internal wireless is rejected:

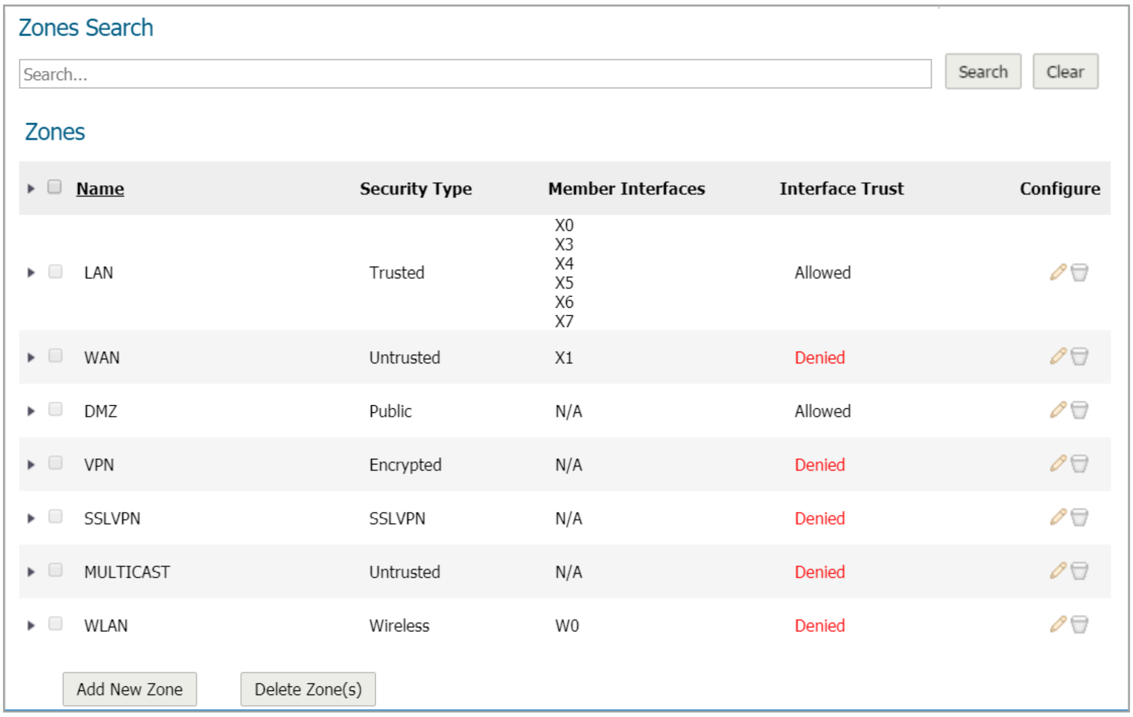


Non-wireless Controller is enabled, all sonicPoints are disabled

## Effects of Enabling Wireless Controller Mode

Enabling Wireless Controller Mode affects several management interface pages. Attempts to enable and/or configure features on these pages are denied.

- The **Edit** and **Delete** icons for VPN and SSL VPN zones become dimmed on the **FIREWALL | Manage | Network > Zones** page.



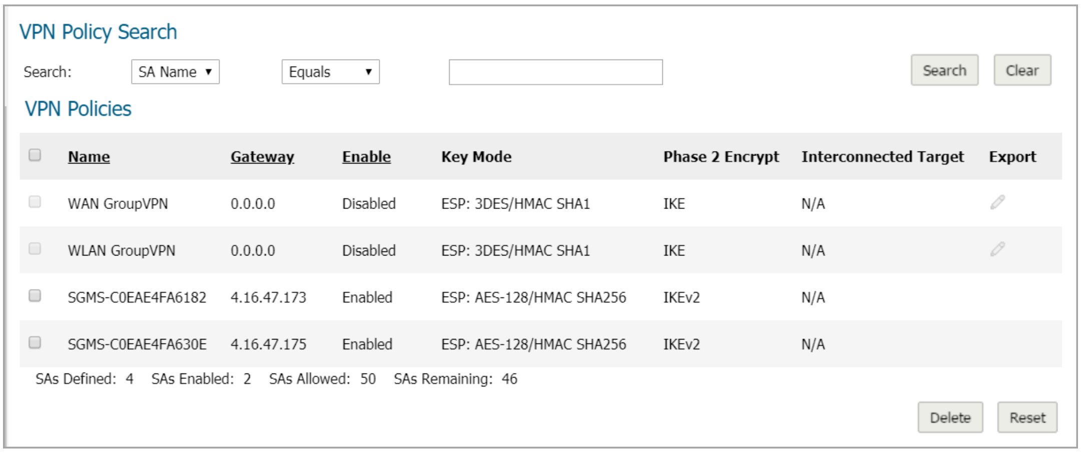
Zones Search

Search...

Zones

| | | Name | Security Type | Member Interfaces | Interface Trust | Configure |
|---|---|---|---|---|---|---|
| ▸ | □ | LAN | Trusted | X0<br>X3<br>X4<br>X5<br>X6<br>X7 | Allowed | ✎ 🗑 |
| ▸ | □ | WAN | Untrusted | X1 | Denied | ✎ 🗑 |
| ▸ | □ | DMZ | Public | N/A | Allowed | ✎ 🗑 |
| ▸ | □ | VPN | Encrypted | N/A | Denied | ✎ 🗑 |
| ▸ | □ | SSLVPN | SSLVPN | N/A | Denied | ✎ 🗑 |
| ▸ | □ | MULTICAST | Untrusted | N/A | Denied | ✎ 🗑 |
| ▸ | □ | WLAN | Wireless | W0 | Denied | ✎ 🗑 |

- VPN is disabled, as shown on the **FIREWALL | Manage | VPN > Summary** page.



VPN Policy Search

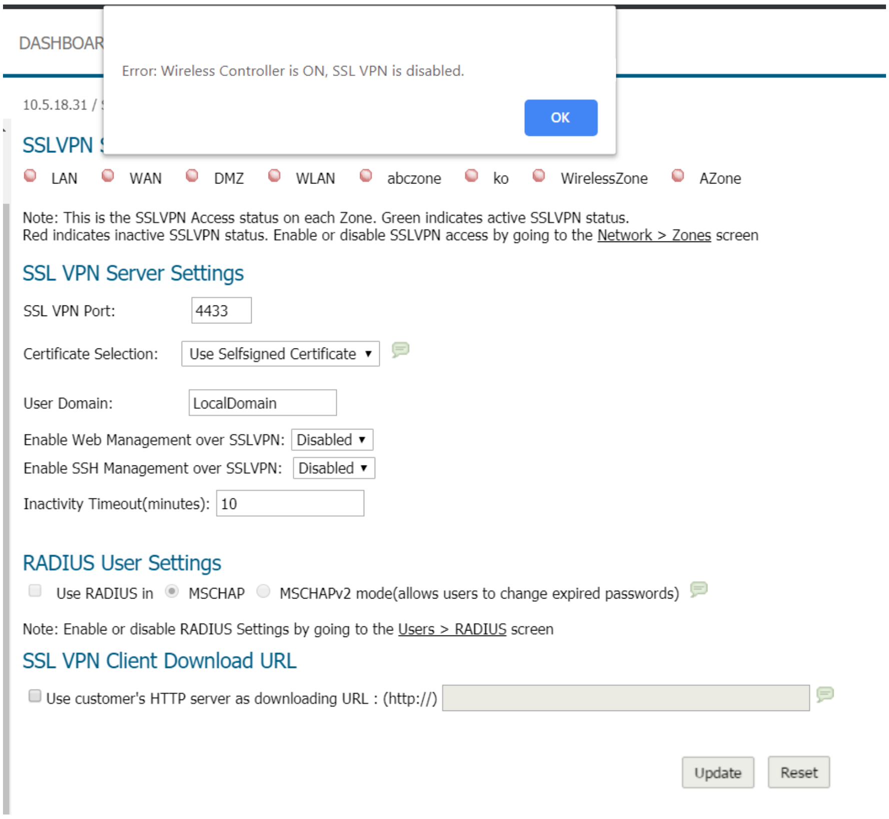
Search: SA Name ▾ Equals ▾

VPN Policies

| □ | Name | Gateway | Enable | Key Mode | Phase 2 Encrypt | Interconnected Target | Export |
|---|---|---|---|---|---|---|---|
| □ | WAN GroupVPN | 0.0.0.0 | Disabled | ESP: 3DES/HMAC SHA1 | IKE | N/A | ✎ |
| □ | WLAN GroupVPN | 0.0.0.0 | Disabled | ESP: 3DES/HMAC SHA1 | IKE | N/A | ✎ |
| □ | SGMS-C0EAE4FA6182 | 4.16.47.173 | Enabled | ESP: AES-128/HMAC SHA256 | IKEv2 | N/A | |
| □ | SGMS-C0EAE4FA630E | 4.16.47.175 | Enabled | ESP: AES-128/HMAC SHA256 | IKEv2 | N/A | |

SAs Defined: 4 SAs Enabled: 2 SAs Allowed: 50 SAs Remaining: 46

- All interfaces to SSL VPN are disabled on the **FIREWALL | Manage | SSL VPN > Server Settings** page. Any attempt to enable SSL VPN would result in an error message.



Error: Wireless Controller is ON, SSL VPN is disabled.

🟥 LAN 🟥 WAN 🟥 DMZ 🟥 WLAN 🟥 abczone 🟥 ko 🟥 WirelessZone 🟥 AZone

Note: This is the SSLVPN Access status on each Zone. Green indicates active SSLVPN status.
Red indicates inactive SSLVPN status. Enable or disable SSLVPN access by going to the Network > Zones screen

SSL VPN Server Settings

SSL VPN Port: 4433

Certificate Selection: Use Selfsigned Certificate ▾

User Domain: LocalDomain

Enable Web Management over SSLVPN: Disabled ▾

Enable SSH Management over SSLVPN: Disabled ▾

Inactivity Timeout(minutes): 10

RADIUS User Settings

□ Use RADIUS in ● MSCHAP ○ MSCHAPv2 mode(allows users to change expired passwords)

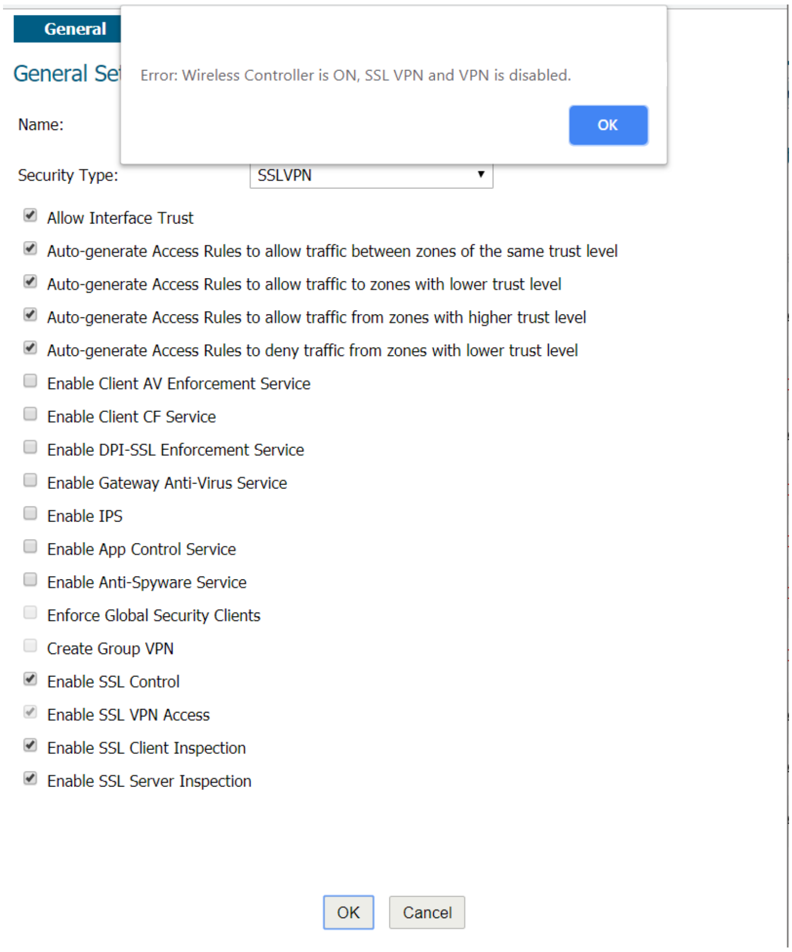
Note: Enable or disable RADIUS Settings by going to the Users > RADIUS screen

SSL VPN Client Download URL

□ Use customer's HTTP server as downloading URL : (http://)

- Any attempt to enable SIP and/or H.323 options on **FIREWALL | Manage | VOIP > Settings** displays an error message.
- WXA is shown as disabled.

- Any attempt to enable a zone with VPN and/or SSL VPN results in an error.



General

General Se

Error: Wireless Controller is ON, SSL VPN and VPN is disabled.

OK

Name:

Security Type: SSLVPN

☑ Allow Interface Trust

☑ Auto-generate Access Rules to allow traffic between zones of the same trust level

☑ Auto-generate Access Rules to allow traffic to zones with lower trust level

☑ Auto-generate Access Rules to allow traffic from zones with higher trust level

☑ Auto-generate Access Rules to deny traffic from zones with lower trust level

□ Enable Client AV Enforcement Service

□ Enable Client CF Service

□ Enable DPI-SSL Enforcement Service

□ Enable Gateway Anti-Virus Service

□ Enable IPS

□ Enable App Control Service

□ Enable Anti-Spyware Service

□ Enforce Global Security Clients

□ Create Group VPN

☑ Enable SSL Control

☑ Enable SSL VPN Access

☑ Enable SSL Client Inspection

☑ Enable SSL Server Inspection

OK Cancel

## Enabling Wireless Controller Mode

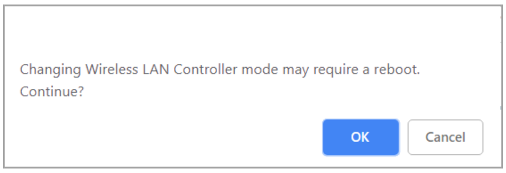
***To enable wireless controller mode:***

ⓘ | **IMPORTANT:** You must reboot the firewall.

1 Navigate to **FIREWALL | Manage | System > Administrator**.

2 Scroll to **Wireless Controller.**

3 From **Wireless Controller Mode**, select **Wireless-Controller-Only**. A warning message displays:



Changing Wireless LAN Controller mode may require a reboot.
Continue?

OK Cancel

4 Click **OK**.

5 Click **Update**.

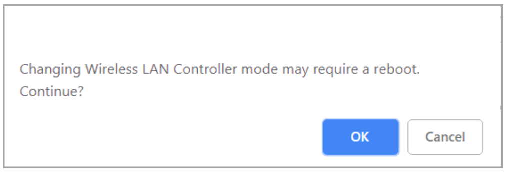
## Enabling Non-Wireless Controller Mode

***To enable non-wireless controller mode:***

1 Navigate to **FIREWALL | Manage | System > Administrator**.

2 Scroll to **Wireless Controller.**

3 From **Wireless Controller Mode**, select **Non-Wireless**. A warning message displays:



Changing Wireless LAN Controller mode may require a reboot. Continue?

4 Click **OK**.

5 Click **Update**. The **Edit** and **Delete** icons for wireless zones become dimmed on the **FIREWALL | Manage | Network > Zones** and **FIREWALL | Manage | Access Points > SonicPoints** pages.

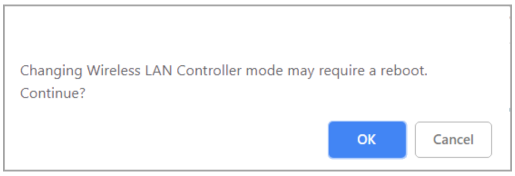
## Enabling Full-Feature-Gateway Mode

***To enable the Full-Feature-Gateway mode:***

1 Navigate to **FIREWALL | Manage | System > Administrator**.

2 Scroll to **Wireless Controller.**

3 From **Wireless Controller Mode**, select **Full-Feature-Gateway**. A warning message displays:



Changing Wireless LAN Controller mode may require a reboot. Continue?

4 Click **OK**.

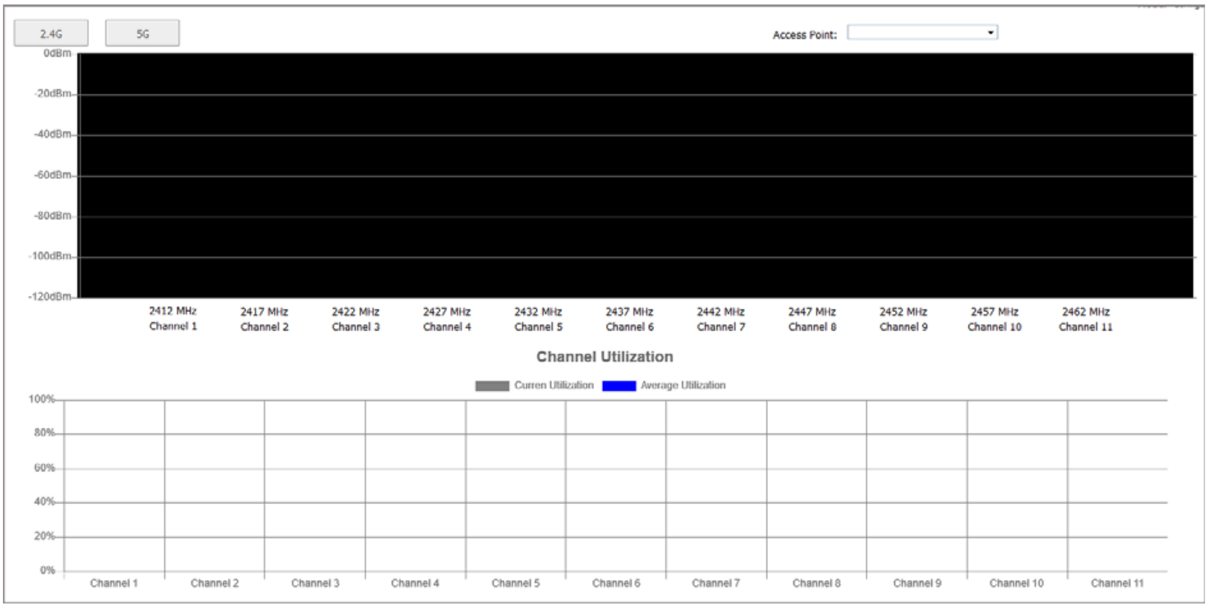
5 Click **Update**.

# RF Spectrum Analysis with Real-Time Noise Detection

Widespread use of Wi-Fi devices, Bluetooth devices, and security cameras has resulted in increased interference that causes performance degradation. GMS provides:

- Automated RF-channel interference detection.
- Power tools to troubleshoot at deeper layers of the RF environment and adjust radio settings accordingly.

To help you troubleshoot problems, there is a new management interface page, **MONITOR | RF Spectrum**:

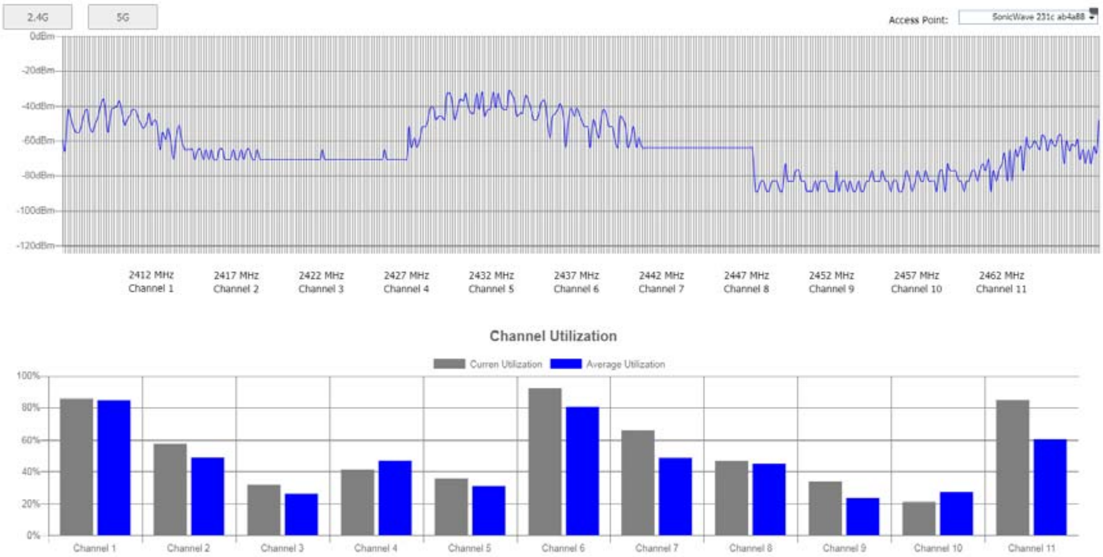


*To monitor RF-channel interference:*

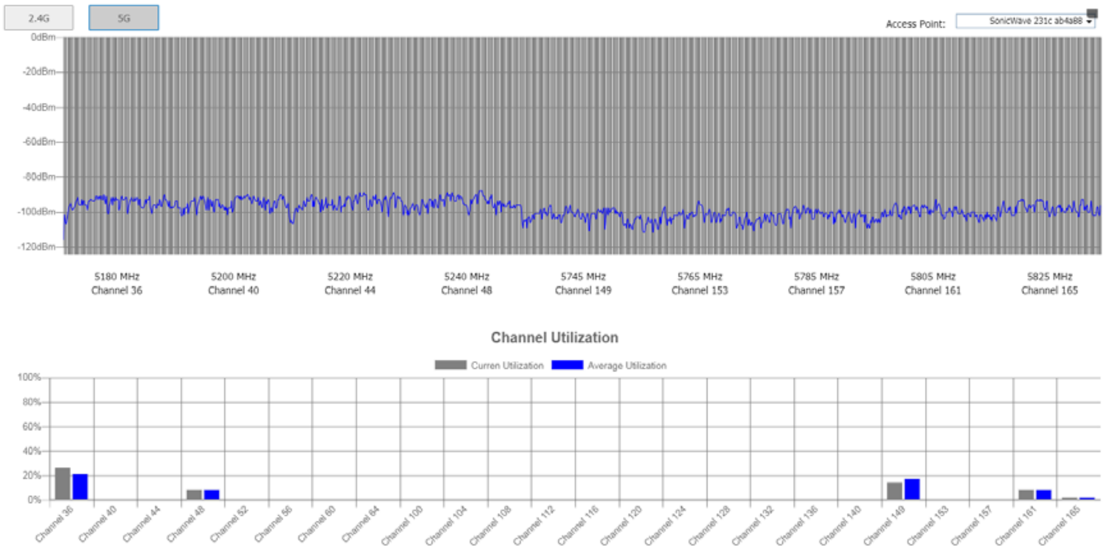
1 Select the bandwidth you would like to monitor, 2.4G or 5G.

2 Select the access point you would to analyze for performance degradation or interference detection from the **Access Point** drop-down menu.

### 2.4G Example



### 5G Example



# Bluetooth Low Energy on SonicWave Series

GMS is equipped with the functionality of Bluetooth Low Energy (BLE), which is a subset of classic Bluetooth. BLE enables smart phones, tablets, SonicWall mobile applications, and other devices (such as other SonicWaves), to easily connect to a SonicWave access point, especially when in close proximity to an iBeacon appliance. BLE also provides location estimation and a simplified SonicWave configuration.

> **NOTE:** IBeacon is a protocol developed by Apple. Various vendors make iBeacon-compatible BLE devices that broadcast their identifier to nearby portable electronic devices. The technology enables smartphones, tablets, and other devices to perform actions when in close proximity to an iBeacon.

**Topics:**

- Enabling BLE
- Viewing BLE Scan Status

## Enabling BLE

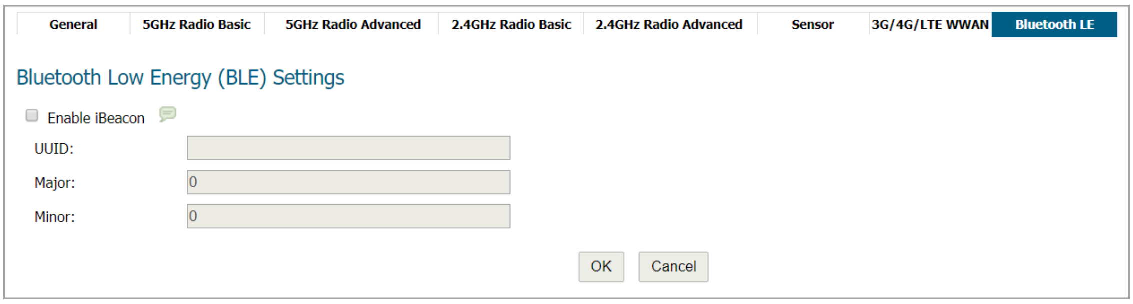
***To enable Bluetooth low energy:***

1 Navigate to **FIREWALL | Manage | Access Points > SonicPoints**.

2 Scroll to the **SonicPoint / SonicWave Provisioning Profiles** section.

3 Click the **Edit** icon for SonicWave. The **Edit SonicWave Profile** dialog displays.

4 Click **Bluetooth LE**.



Bluetooth Low Energy (BLE) Settings

☐ Enable iBeacon

| | |
|---|---|
| UUID: | |
| Major: | 0 |
| Minor: | 0 |

5 To enable BLE, select **Enable iBeacon**. This option is not selected by default. The subordinate fields become available.

6 Complete the fields:

- **UUID** – Enter the 128 hexadecimal digits of the UUID. The UUID displays in five-character groups separated by hyphens.
- **Major** – Enter the significant identity in the same geographical group. The range is 0 to 65535; the default is **0**.
- **Minor** – Enter the secondary identity in the same geographical group. The range is 0 – 65535; the default is **0**.

> **TIP:** Use different UUIDs to distinguish different geographical groups and major and minor options to distinguish areas within the geographical group. For example, when you deploy several SonicWave appliances with BLE in one building, set the same UUID for these SonicWave appliances. The SonicWave appliances on the same floor have the same **Major** number, but have different **Minor** numbers in different places on the same floor. In this way, your mobile device is close to a SonicWave appliance and its location.

7 Click **OK**.

## Viewing BLE Scan Status

This feature allows SonicWave appliances to be aware of the status of nearby Bluetooth low energy devices (BLE), and also know the signal strength of a nearby iBeacon. The SonicWave compares the difference between RSSI and power to estimate the distance to the device emitting an iBeacon. You can also use this feature in the deployment of SonicWave appliances.

***To view BLE scan status:***

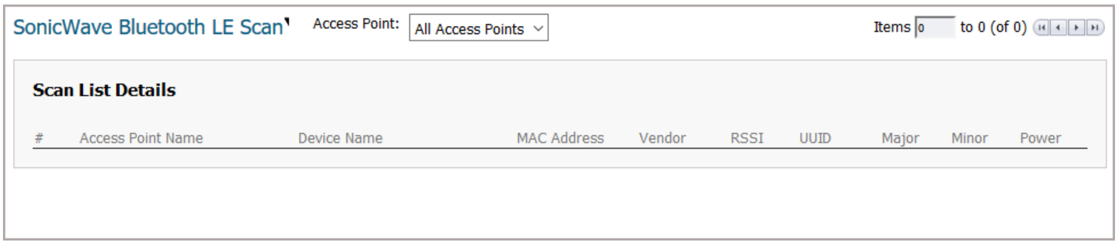
1 Navigate to **FIREWALL | Manage | Access Points > SonicPoints**.

2 Scroll to the **SonicPoint / SonicWave Provisioning Profiles** section.

3 Click the **Edit** icon for SonicWave. The **Edit SonicWave Profile** dialog displays.

4 Click **Bluetooth LE**.

5 When **Enable iBeacon** is selected, the subordinate fields become available.



SonicWave Bluetooth LE Scan

Access Point: All Access Points

Items 0 to 0 (of 0)

**Scan List Details**

| # | Access Point Name | Device Name | MAC Address | Vendor | RSSI | UUID | Major | Minor | Power |
|---|---|---|---|---|---|---|---|---|---|

6 From **Access Points** select either:

- **All Access Points** (default)
- A particular access point

# SonicWave 432 DFS

Dynamic Frequency Selection (DFS) is a technology that allows a device to dynamically select or change the operating frequency to avoid interfering with other systems. For example, the 5 GHz band is used by radar systems in the U.S. and other countries. When DFS is supported, wireless access points operating in the 5 GHz band must be able to detect and avoid interference with these systems.

SonicWave 432 series access points now support DFS and DFS channels when partnered with a SonicWall firewall running GMS.

## WWAN Cards

SonicWall is continually updating the list of supported WWAN devices. For the most up-to-date list of supported WWAN devices, see the Knowledge Base article, *What wireless cards and broadband devices are supported on SonicWall firewalls?*

Newly supported or improved WWAN devices in GMS include:

- Verizon USB730L USB Modem (USA)
- Verizon USB620L USB Modem (USA) supported on all firewall models including the NSA 2600, NSA 3600, NSA series, and SuperMassive series firewalls.
- AT&T Velocity USB Stick (ZTE MF861) (USA)
- Sprint Franklin U772 USB Modem (USA)
- T-mobile Alcatel Linkzone Hotspot; supported in USB tethering mode (USA)
- Telstra 4GX (Huawei E8372) USB Modem (Australia)
- Huawei E3372 - There are numerous variants of the E3372, specific variants tested are: Entel-branded E3372h-510 and MTN-branded E3327h-153

## SonicWave Sensor Mode Enhancement

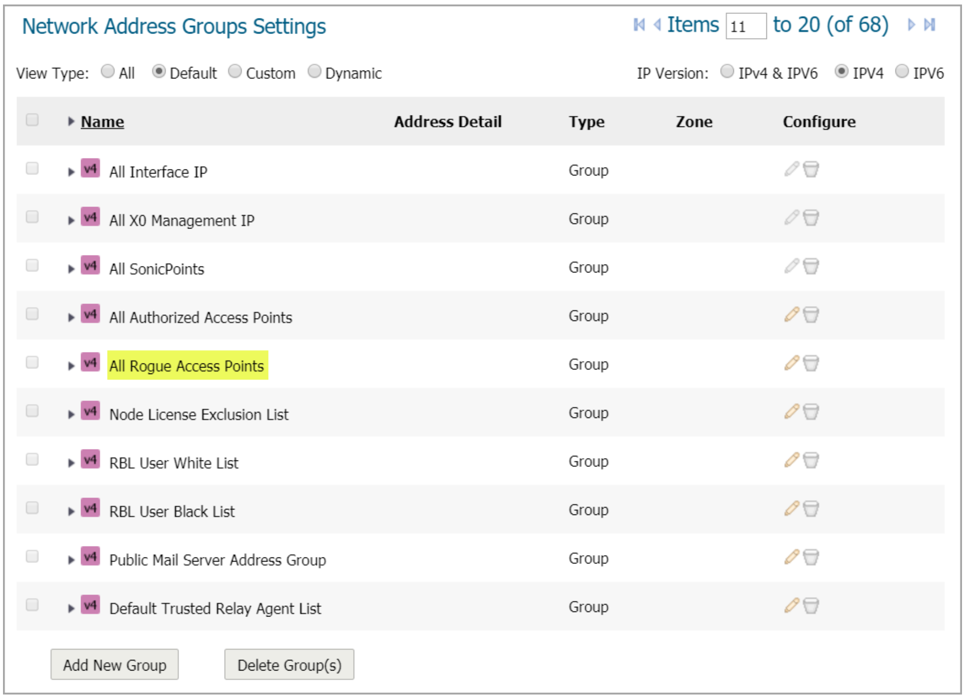
When Wireless Intrusion Detection and Prevention (WIDP) is enabled, SonicWave appliances now act as both an Access Point and as a sensor detecting any unauthorized access point connected to a SonicWall network and acting according its configuration.

There are two new default IPv4 Address Object groups, which you can edit, on the **FIREWALL | Manage | Firewall > Address Objects.**

1 Scroll to the **Network Address Groups Settings** section.

2 For View Type, select Default and for IP Version, select IPv4.

| | |
|---|---|
| **All Rogue Access Points** | MAC address object group listing all rogue APs either added automatically or added by you. |
| **All Rogue Devices** | IP address object group listing the IP of all rogue devices. |



Network Address Groups Settings — Items 11 to 20 (of 68)

View Type: ○ All ● Default ○ Custom ○ Dynamic — IP Version: ○ IPv4 & IPV6 ● IPV4 ○ IPV6

| □ | Name | Address Detail | Type | Zone | Configure |
|---|---|---|---|---|---|
| □ | All Interface IP | | Group | | |
| □ | All X0 Management IP | | Group | | |
| □ | All SonicPoints | | Group | | |
| □ | All Authorized Access Points | | Group | | |
| □ | All Rogue Access Points | | Group | | |
| □ | Node License Exclusion List | | Group | | |
| □ | RBL User White List | | Group | | |
| □ | RBL User Black List | | Group | | |
| □ | Public Mail Server Address Group | | Group | | |
| □ | Default Trusted Relay Agent List | | Group | | |

# NAS-ID Support using SSID

**NOTE:** This feature does not apply to internal WLAN zones used by SonicPointN or SonicPointNDR.

This feature adds a new type of NAS (network attached storage) ID in WP2A-EAP authentication and accounting messages. SonicWall supports the name and MAC address of an access point as its NAS-ID. To support this feature, a new option, **SSID**, has been added to the **NAS Identifier Type** option on the SonicPoint Radius Server Setting dialog and the Add/Edit Virtual Access Point dialog.

**TIP:** The **NAS Identifier Type** option displays only when an EAP authentication type is selected for the **Authentication Type** option.

***To add the NAS Identifier:***

1 Navigate to **FIREWALL | Manage | Access Points > SonicPoints**.

2 Add or modify a SonicWave.

3 Click **5GHz Radio Basic**.

4 Scroll to **Wireless Security** and select **WPA2 - EAP** from the **Authentication Type** drop-down menu.

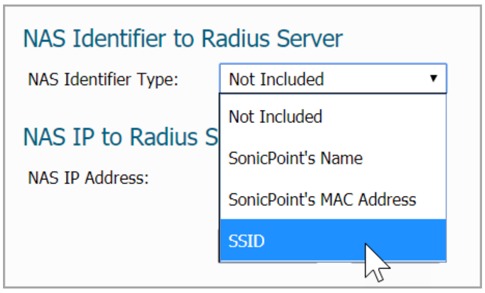
5 The **RADIUS Server Settings** options appear.

6 Click **Configure**. The **SonicPoint Radius Server Settings** appear.

7 Scroll to the **NAS Identifier to Radius Server** section.

8 For **NAS Identifier Type**, select **SSID** from the drop-down menu.

**SonicPoint Radius Server Setting dialog**



NAS Identifier to Radius Server

NAS Identifier Type: Not Included

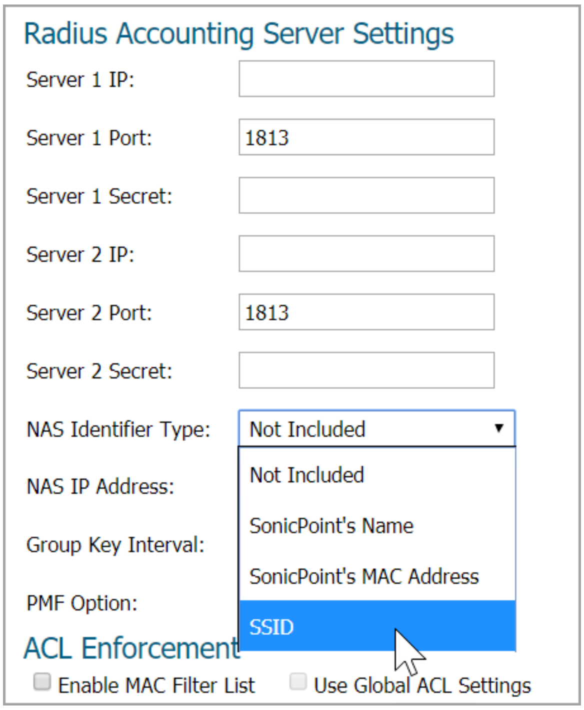
NAS IP to Radius S

NAS IP Address:

***To add the NAS Identifier to a Virtual Access Point:***

1. Navigate to **FIREWALL | Manage | Access Points > Virtual Access Point**.
2. Scroll to **Virtual Access Points**, and edit an existing virtual access point, or click **Add Virtual Access Point**.
3. Click **Advanced**.
4. Scroll to **Virtual Access Point Advanced Settings** and select **WPA2 - EAP** from the **Authentication Type** drop-down menu.
5. Scroll down to Radius Accounting Server Settings and for the **NAS Identifier Type**, select **SSID** from the drop-down menu.

**Add/Edit Virtual Access Point dialog**



Radius Accounting Server Settings

Server 1 IP:

Server 1 Port: 1813

Server 1 Secret:

Server 2 IP:

Server 2 Port: 1813

Server 2 Secret:

NAS Identifier Type: Not Included

NAS IP Address:

Group Key Interval:

PMF Option:

ACL Enforcement

☐ Enable MAC Filter List ☐ Use Global ACL Settings

When the SSID option is selected, both the RADIUS authentication message and RADIUS accounting message carry the access point or VAP SSID.

# Increase in SonicPoints/SonicWaves Supported

GMS supports up to 512 SonicPoints/SonicWaves on NSA series firewalls.

# Authentication Features

**Topics:**

- Two-Factor Authentication (TOTP)
- First Login Password Change
- User Login Record
- TACACS+ Accounting
- Captive Portal Authentication
- Multiple External (LHM) Web Servers

## Two-Factor Authentication (TOTP)

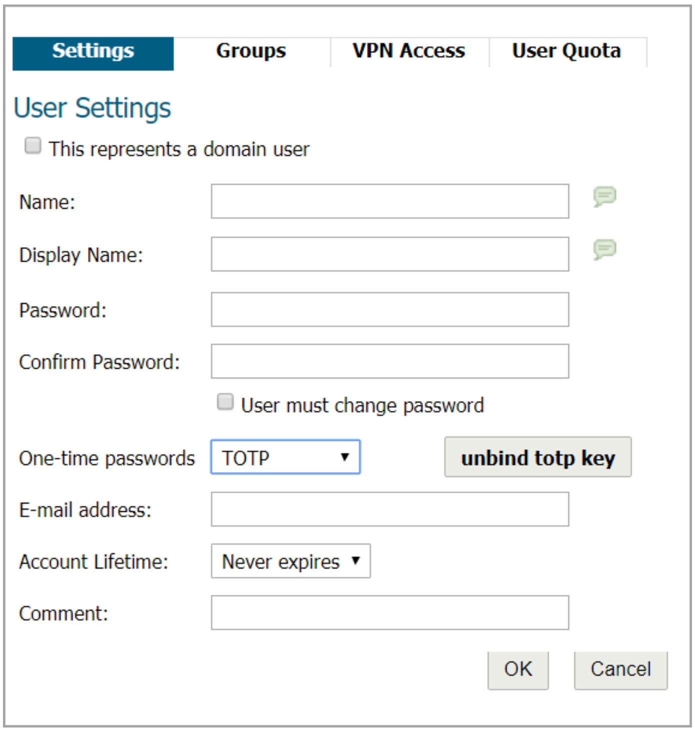
Many user login authentication methods require one-time passwords (OTP). GMS provides an additional method of OTP by way of email: A Time-Based One-Time Password (TOTP) authentication with two-factor authentication.

To use this feature, you must download a TOTP client application (such as Google Authentication, DUO, or Microsoft Authentication) on your smartphone. Select TOTP on the **Add/Edit User** dialog; for more information, see First Login Password Change.

## First Login Password Change

Previously, when you created a user, you could allow other users to change their passwords after first logging in. GMS allows you to force all users to change their passwords before their first login when you create or edit a local user. You can specify the login change for users or for groups. Navigate to **FIREWALL | Manage | Users > Local Users** and edit an existing Local User, or click **Add New Local User**.

- **Local Users**: The **Add/Edit User** dialog has been changed:



User Settings

□ This represents a domain user

Name:

Display Name:

Password:

Confirm Password:

□ User must change password

One-time passwords: TOTP

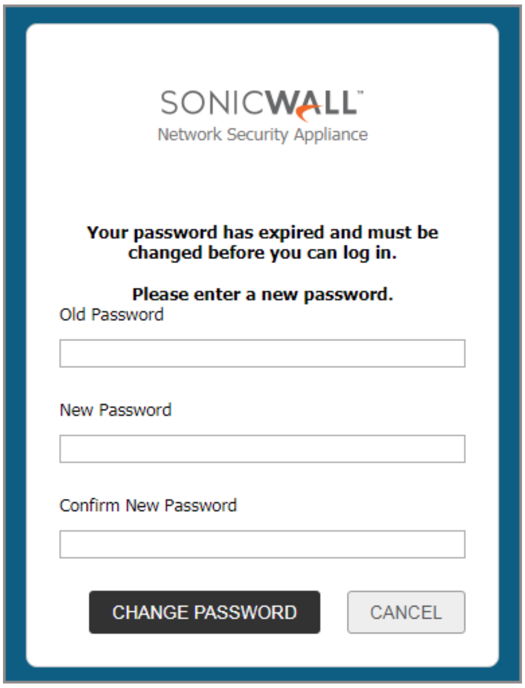
E-mail address:

Account Lifetime: Never expires

Comment:

The **Require one-time passwords** option has been replaced with the **One-time passwords** option, which allows you to select how one-time passwords are processed:

  - **Disabled** (default) – If **User must change password** is selected this dialog displays at the first login attempt:

    Your password has expired and must be changed before you can log in.

    Please enter a new password.

  - **OTP via Mail** – Users receive a temporary password by email after they have input their user name and first password. After receiving the password-containing email, they can enter the second password to complete the login process.
  - **TOTP** – Users receive a temporary password by email after they have input their user names and first passwords, but to use this feature, users must download a TOTP client application (such as Google Authentication, DUO, or Microsoft Authentication) onto their smartphones.

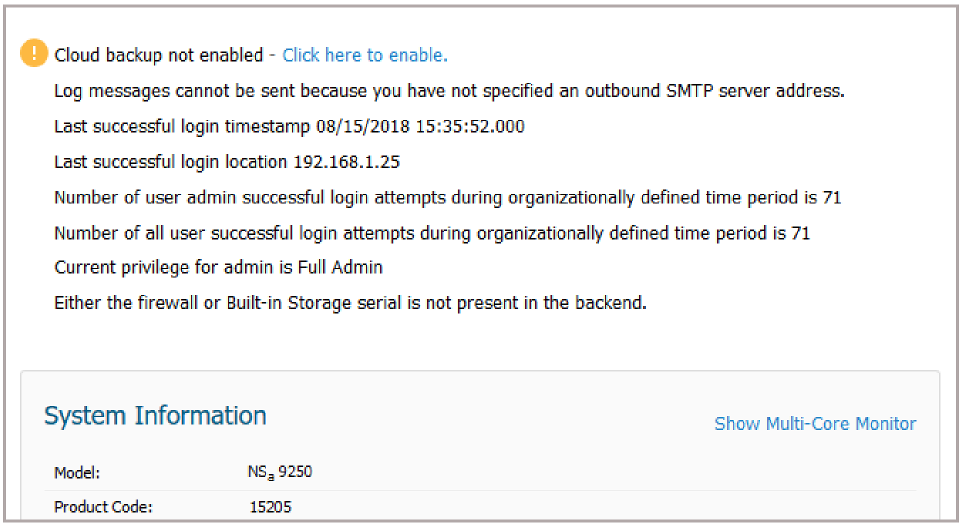
    The **unbind totp key** button displays.

  To avoid another password change request for this user, the option applies only to the first login.

- **FIREWALL | Manage | Users > Local Groups**: On the **Add/Edit Group** dialog, you have the same choices as the **Add/Edit User** dialog. The method chosen affects all members of the user group.

# User Login Record

To support UCAPL certification, GMS displays this information on the **FIREWALL | Manage | System > Status** page:



Cloud backup not enabled - Click here to enable.

Log messages cannot be sent because you have not specified an outbound SMTP server address.

Last successful login timestamp 08/15/2018 15:35:52.000

Last successful login location 192.168.1.25

Number of user admin successful login attempts during organizationally defined time period is 71

Number of all user successful login attempts during organizationally defined time period is 71

Current privilege for admin is Full Admin

Either the firewall or Built-in Storage serial is not present in the backend.

System Information

| | |
|---|---|
| Model: | $NS_a$ 9250 |
| Product Code: | 15205 |

- Total number of all successful users login attempts during the organizationally defined time
- Administrative user’s last login time stamp and location
- Total number of an administrative user's successful login attempts during the organizationally defined time
- Total number of an administrative user's unsuccessful login attempts during the organizationally defined time
- Administrative user's current privilege
- Notification of administrative user's privilege change since last login

**TIP:** This information is displayed only if the **Display user login info since last login** option is selected on the **FIREWALL | Manage | Users > Settings** page.

**NOTE:** The defined time is configured in an internal setting. For information about GMS internal settings, contact SonicWall Support., contact Technical Support.

This information is also available through the CLI.

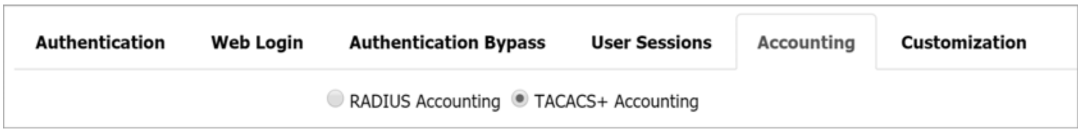
# TACACS+ Accounting

GMS supports TACACS+ accounting Start, Watchdog and Stop messages, but not the TACACS+ accounting proxy, that is, GMS does not forward the accounting request to the accounting server.

If both a RADIUS server and a TACACS+ server are configured, a user’s accounting messages are sent to both servers.

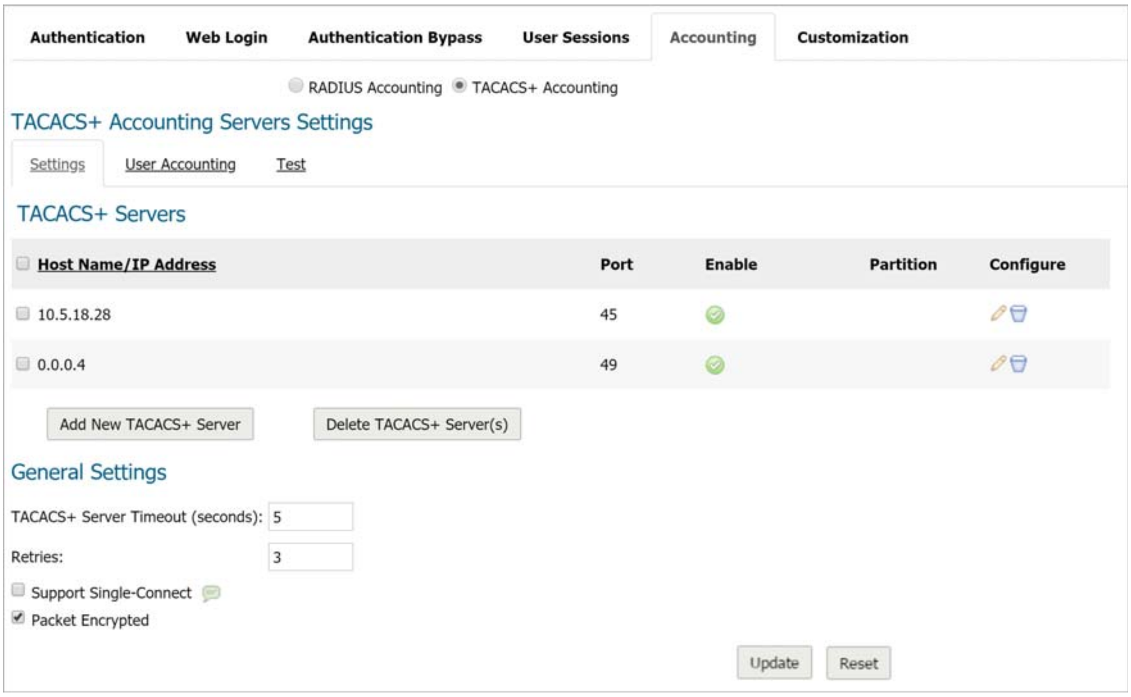
***To configure TACACS+ accounting:***

1. Navigate to **FIREWALL | Manage | Users > Settings**.
2. Click **Accounting**.



○ RADIUS Accounting ● TACACS+ Accounting

3 Click **TACACS+ Accounting**. The **TACACS+ Accounting Server Settings** appear.



○ RADIUS Accounting ● TACACS+ Accounting

TACACS+ Accounting Servers Settings

TACACS+ Servers

| □ Host Name/IP Address | Port | Enable | Partition | Configure |
|---|---|---|---|---|
| □ 10.5.18.28 | 45 | ✓ | | |
| □ 0.0.0.4 | 49 | ✓ | | |

General Settings

TACACS+ Server Timeout (seconds): 5

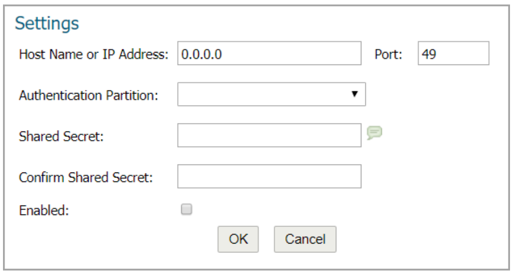
Retries: 3

□ Support Single-Connect

☑ Packet Encrypted

4 To add a TACACS+ server, scroll to **TACACS+ Servers**.

5 Click **Add New TACACS+ Server**. The **Add TACACS+ accounting server** dialog displays.



Settings

Host Name or IP Address: 0.0.0.0 Port: 49

Authentication Partition:

Shared Secret:

Confirm Shared Secret:

Enabled: □

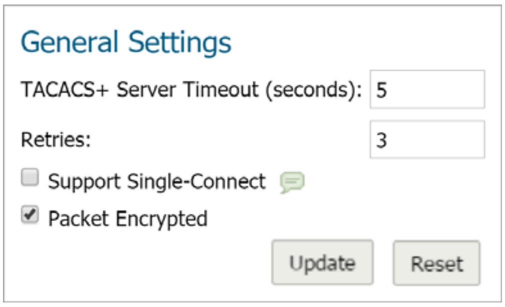
6 Enter the host name or IP address of the TACACS+ server in the **Host Name or IP Address** field.

7 Enter the port number of the server in the **Port** field. The default is **49**.

8 Enter the shared secret in the S**hared Secret** and **Confirm Shared Secret** fields.

9 Click **OK**.

10 Scroll to **General Settings**.



General Settings

TACACS+ Server Timeout (seconds): 5

Retries: 3

□ Support Single-Connect

☑ Packet Encrypted

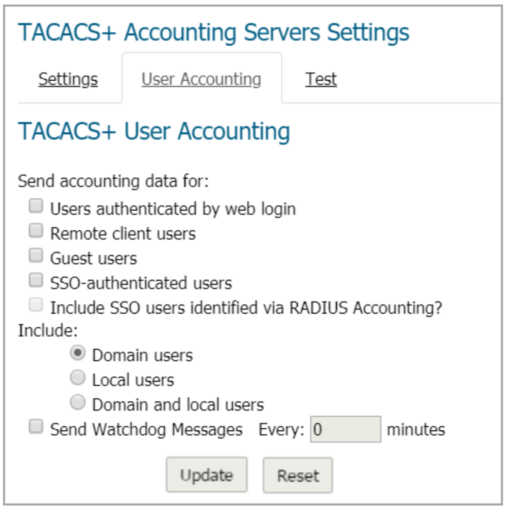
11 Enter the server timeout in the **TACACS+ Server Timeout (seconds)** field. The default is **5** seconds.

12 Enter the maximum number of retries in the **Retries** field. The default is **3**.

13 To support single connect, select **Support Single Connect**. This option is not selected by default.

14 To allow encrypted packets, select **Packet Encrypted**. This option is selected by default.

15 Click **User Accounting**.



TACACS+ Accounting Servers Settings

Settings | User Accounting | Test

TACACS+ User Accounting

Send accounting data for:

□ Users authenticated by web login
□ Remote client users
□ Guest users
□ SSO-authenticated users
□ Include SSO users identified via RADIUS Accounting?

Include:

● Domain users
○ Local users
○ Domain and local users

□ Send Watchdog Messages Every: 0 minutes

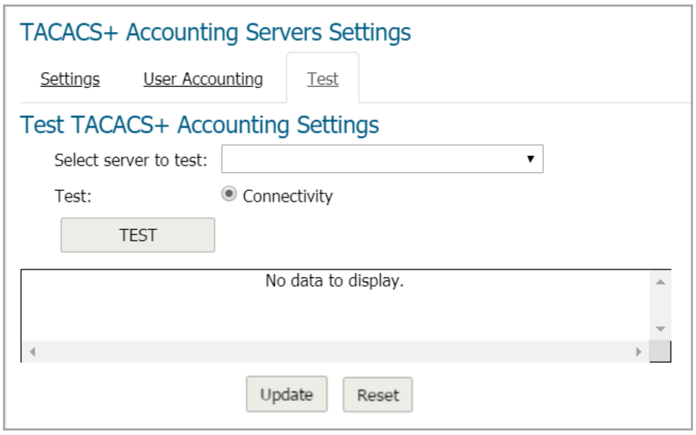
Update | Reset

16 From **Send accounting data for**, select one or more types of users. The **Include SSO users identified via RADIUS Accounting?** option is not available by default. To make the feature editable, click **SSO-authenticated users**.

17 Choose whether to track domain and/or local users from **Include**. **Domain users** is selected by default.

18 To receive watchdog messages, select **Send Watchdog Messages**. This option is not selected by default.

19 Click **Test**.



TACACS+ Accounting Servers Settings

Settings | User Accounting | Test

Test TACACS+ Accounting Settings

Select server to test:

Test: ● Connectivity

TEST

No data to display.

Update | Reset

20 From **Select server to test**, select the IP address of the TACACS+ server.

21 Choose the type of test from **Test**. **Connectivity** is selected by default.

22 Click **Test**. The results of the test display in **Returned User Attributes**.

23 Click **Update**.

# Captive Portal Authentication

Captive Portal Authentication helps a user gain access after being authenticated and authorized. The user who seeks web access to a network is redirected to the authentication web login page hosted on the captive portal server that is integrated with the RADIUS server.

This authentication method is the extension to SonicWall's existing LHM (Lightweight Hotspot Messaging). LHM deployment requires all authentications to be handled by the external LHM server. Captive portal authentication puts more leverage on the firewall itself to communicate with the RADIUS server to complete the authentication process.

***To configure captive portal authentication:***

1 Configure the RADIUS portal server:

   a Configure the user information and user group information. The user group name must:

   - Be returned to the firewall with an ACCEPT message.
   - Match a group name on the firewall.
   - Have guest privilege on the firewall.

   b Configure the **idle timeout** and **session timeout** attributes if the firewall requires they be returned with the ACCEPT message.

   c Define the welcome URL as a **Vendor Specific Attribute**; SonicWall's vendor code is 8741.

   d If RADIUS accounting is supported, set the interim interval.

2 Navigate to **FIREWALL | Manage | Users > Settings**.

3 Click **Authentication**.

4 Under **User Login Settings**, select **RADIUS + LOCAL Users** from **Authentication method for login**.

5 Click **CONFIGURE RADIUS**. The **RADIUS Configuration** dialog displays.

6 Click **Users**.

7 For **Mechanism for setting user group memberships**:, choose **Use RADIUS Filter-Id attribute on RADIUS server**.

8 Click **OK**.

9 Navigate to **FIREWALL | Manage | Network > Zones**.

10 Click either the **Add** icon or the **Edit** icon for a wireless zone. The **Add**/**Edit Zone** dialog displays.

11 Ensure the **Security Type** is **Wireless**.

12 Follow the steps for configuring a zone for captive portal authentication with RADIUS in *SonicOS 6.5 System Setup*.

## Multiple External (LHM) Web Servers

To provide authentication of IPv4 Traffic and IPv6 Traffic, GMS supports two external Lightweight Hotspot Messaging (LHM) web servers, one for IPv4 and the other for IPv6. Different traffic types redirect to their corresponding LHM servers.

# Advanced Security Features

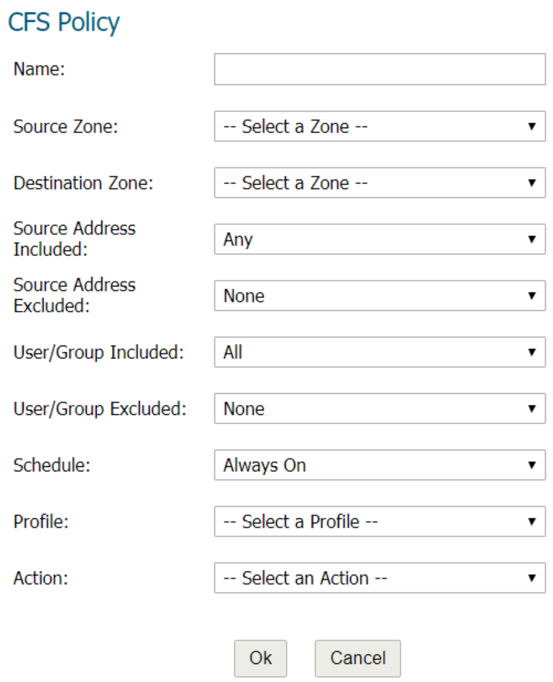
**Topics:**

- CFS Policy Exclusion
- Capture ATP Sender/Receiver Email Information
- Policy-based HTTPS CFS
- DNS Security
- Client Anti Virus Enforcement and Exclusion

## CFS Policy Exclusion

The concept of exclusion has been extended to CFS policies. With this feature, Address Objects and Users can be both included and excluded in CFS policies, making the CFS policy more flexible to meet your requirements. You can configure some Address Objects with large ranges while excluding some small ranges or addresses within the large range in one CFS policy. For example, you can block all employees from visiting external websites, while excluding the president from this restriction. Before this, you had to configure two policies: one for the president with all allowed categories and one for the employees with blocked categories.

On the **FIREWALL | Manage | Firewall > Content Filter Policies** page, the **Add CFS Policy** and **Edit CFS Policies** dialogs now have options for including and/or excluding Source Address Objects and/or User and Groups.



CFS Policy

| | |
|---|---|
| Name: | |
| Source Zone: | -- Select a Zone -- |
| Destination Zone: | -- Select a Zone -- |
| Source Address Included: | Any |
| Source Address Excluded: | None |
| User/Group Included: | All |
| User/Group Excluded: | None |
| Schedule: | Always On |
| Profile: | -- Select a Profile -- |
| Action: | -- Select an Action -- |

# Capture ATP Sender/Receiver Email Information

In **FIREWALL | Manage | Capture ATP > Settings**, this feature provides additional Capture Advanced Threat Protection (ATP) capability to:

- Allow GMS Gateway Anti-Virus (GAV) service to parse sender and receiver information of email traffic.
- Log sender and receiver information of email traffic that is being forwarded to GAV Cloud Server for threat analysis.

GAV now parses:

- SMP sender/receiver information from:
  - RCPT TO and MAIL FROM fields
  - To, CC, BCC, and From MIME header fields
- POP3 and IMAP sender/receiver information from:
  - To, CC, BCC, and From MIME header fields

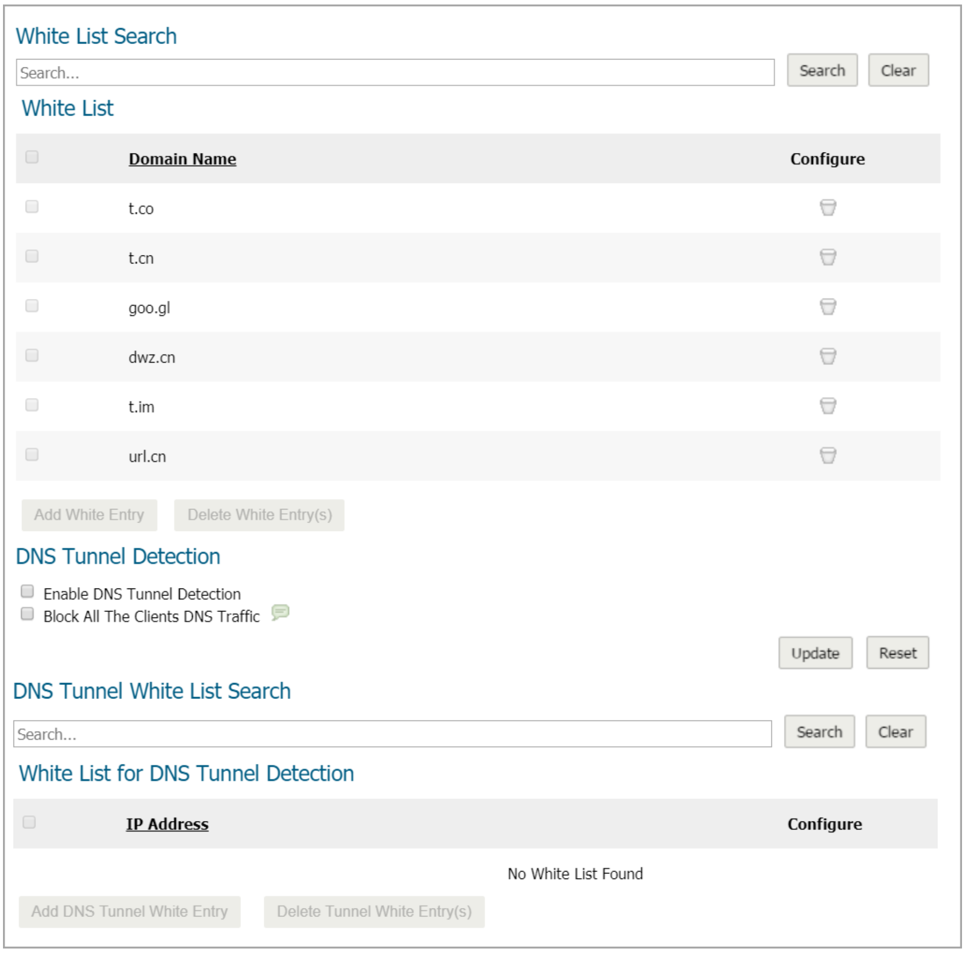
# Policy-based HTTPS CFS

In GMS, this feature allows you to do regular HTTPS filtering for some clients, but bypass regular HTTPS filtering for other clients based on policies you configure.

# DNS Security

GMS detects DNS tunneling, which is a method to bypass security controls and exfiltrate data from a targeted organization. A DNS tunnel can be used as a full, remote-control channel for a compromised internal host. Exfiltrated data includes Operating System (OS) commands, file transfers, or even a full IP tunnel.

Enable and control DNS security through two new options on the **FIREWALL | Manage | Network > DNS Security** page. You can view detected suspicious activity by a client, and you can create a white list of IP addresses.



White List Search

Search...

White List

| □ | Domain Name | Configure |
|---|---|---|
| □ | t.co | 🗑 |
| □ | t.cn | 🗑 |
| □ | goo.gl | 🗑 |
| □ | dwz.cn | 🗑 |
| □ | t.im | 🗑 |
| □ | url.cn | 🗑 |

DNS Tunnel Detection

□ Enable DNS Tunnel Detection

□ Block All The Clients DNS Traffic

DNS Tunnel White List Search

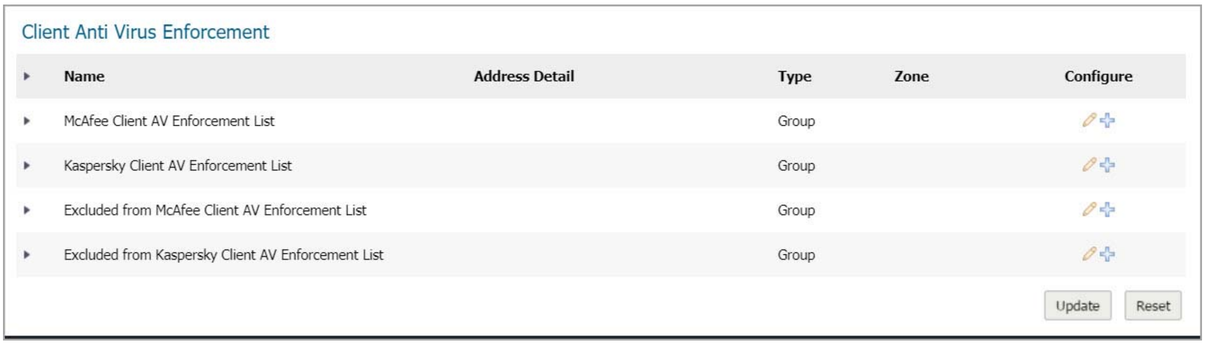
Search...

White List for DNS Tunnel Detection

| □ | IP Address | Configure |
|---|---|---|
| | No White List Found | |

# Client Anti Virus Enforcement and Exclusion

The Client Anti Virus Enforcement list provides the options to exclude address objects from the Client AV Enforcement list.



Client Anti Virus Enforcement

| ▸ | Name | Address Detail | Type | Zone | Configure |
|---|---|---|---|---|---|
| ▸ | McAfee Client AV Enforcement List | | Group | | ✎ ✚ |
| ▸ | Kaspersky Client AV Enforcement List | | Group | | ✎ ✚ |
| ▸ | Excluded from McAfee Client AV Enforcement List | | Group | | ✎ ✚ |
| ▸ | Excluded from Kaspersky Client AV Enforcement List | | Group | | ✎ ✚ |

The **Client Anti-Virus Enforcement** table has four entries, all include a Type of Group:

- **McAfee Client AV Enforcement List** or **Kaspersky Client AV Enforcement List**, depending on which you use)
- **Excluded from McAfee Client AV Enforcement List** or **Excluded from Kaspersky Client AV Enforcement List**

To see the IP addresses associated with each entry, click the **Expand** icon. The **Address Detail**, **Type**, and **Zone** for each entry displays. If you have not configured the enforcement list, clicking the **Expand** icon displays **No Entries**.

To hide the IP addresses, click the **Collapse** icon.

You can edit or add to these two entries, but you cannot delete them.

**Topics:**

- Creating the Client AV Enforcement List
- Excluding Address Objects from the Client AV Enforcement List

## Creating the Client AV Enforcement List

> **NOTE:** Predefined Address Objects, such as interface IPs or the Default Gateway cannot be edited or deleted individually; their **Edit** and **Delete** icons are dimmed. You remove a predefined Address Object from the **Client AV Enforcement List** through editing the List itself. You can, however, edit or delete any Address Object you have defined.

Configure the client AV enforcement list with the IP address of the address objects that are to have Client AV enforced.

You can define ranges of IP addresses to receive Anti-Virus enforcement by creating an Address Object

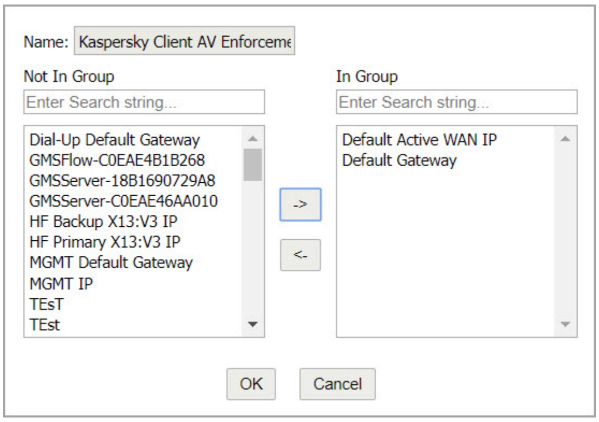
containing a range of IP addresses. Any computer requiring enforcement needs a static IP address within the specified range of IP addresses. Up to 64 IP address ranges can be entered for enforcement.

### *To edit a client AV enforcement list from the existing Address Objects:*

1 Navigate to the **FIREWALL | Manage | Security Services > Client AV Enforcement** page.

2 Scroll to the **Client Anti-Virus Enforcement** section.

3 Click the **Edit** icon for the **Client AV Enforcement List** you would like to modify. The **Edit Address Object Group** dialog displays.



Name: Kaspersky Client AV Enforceme

Not In Group

Dial-Up Default Gateway
GMSFlow-C0EAE4B1B268
GMSServer-18B1690729A8
GMSServer-C0EAE46AA010
HF Backup X13:V3 IP
HF Primary X13:V3 IP
MGMT Default Gateway
MGMT IP
TEsT
TEst

In Group

Default Active WAN IP
Default Gateway

4 Select the IP address(es) to have **Client AV enforcement** from the list on the left.

5 Click the **Right Arrow** button to move the entries to the list on the right.

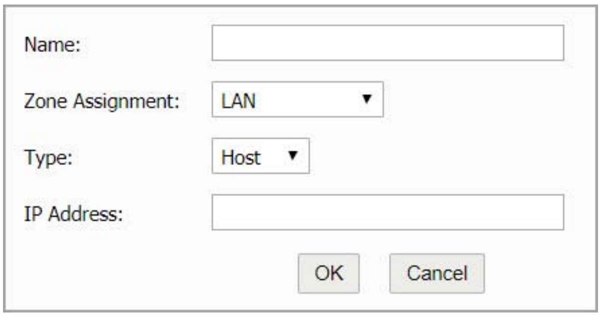
6 When finished adding Address Objects, click **OK**.

### *To add an Address Object to the Client AV Enforcement List:*

1 Navigate to the **FIREWALL | Manage | Security Services > Client AV Enforcement** page.

2 Scroll to the client **Anti-Virus Enforcement** section.

3 Click the **Add** icon for the appropriate **Client AV Enforcement List**. The **Add Address Object** dialog displays.


Name:

Zone Assignment: LAN

Type: Host

IP Address:

4 Enter a friendly name in the **Name** field.

5 Select the zone from the **Zone Assignment** drop-down menu.

6 Select a type (Host or Range) from the **Type** drop-down menu.

7 Enter the IP address of the Address Object in the **IP Address** field.

8 Click **OK**.

# Excluding Address Objects from the Client AV Enforcement List

SonicWall Client Anti-Virus currently supports Windows platforms. To access the Internet, computers with other operating systems must be exempt from Anti-Virus policies.

△ **CAUTION: To ensure full network protection from virus attacks, it is recommended that only servers and unsupported machines be excluded from protection and that third-party anti-virus software is installed on each machine before excluding that machine from Anti-Virus enforcement.**

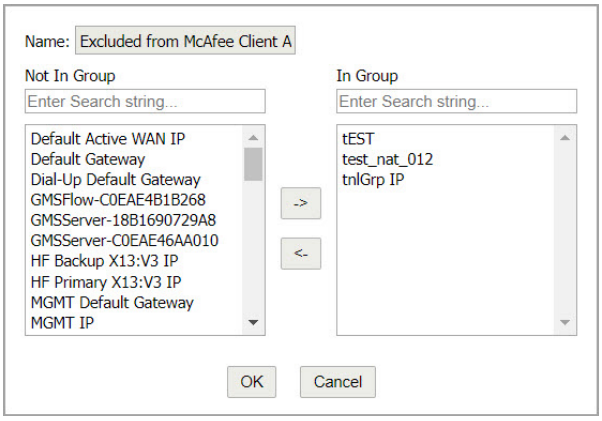
ⓘ **NOTE:** Predefined Address Objects, such as interface IPs or the Default Gateway cannot be edited or deleted individually; their **Edit** and **Delete** icons are dimmed. You remove a predefined Address Object from the **Excluded from Client AV Enforcement List** through editing the List itself. You can, however, edit or delete any Address Object you have defined.

### *To define excluded Address Objects:*

1 Navigate to the **FIREWALL | Manage | Security Services > Client AV Enforcement** page.

2 Scroll to the **Client Anti-Virus Enforcement** section.

3 Click the **Edit** icon for the **Excluded from McAfee/Kasperski Client AV Enforcement List**. The **Edit Address Object Group** displays.



Name: Excluded from McAfee Client A

Not In Group

Enter Search string...

Default Active WAN IP<br>
Default Gateway<br>
Dial-Up Default Gateway<br>
GMSFlow-C0EAE4B1B268<br>
GMSServer-18B1690729A8<br>
GMSServer-C0EAE46AA010<br>
HF Backup X13:V3 IP<br>
HF Primary X13:V3 IP<br>
MGMT Default Gateway<br>
MGMT IP

In Group

Enter Search string...

tEST<br>
test_nat_012<br>
tnlGrp IP

4 Select the Address Object(s) to be excluded from the list on the left.

5 Click the **Right Arrow** to move the objects to the list on the right.

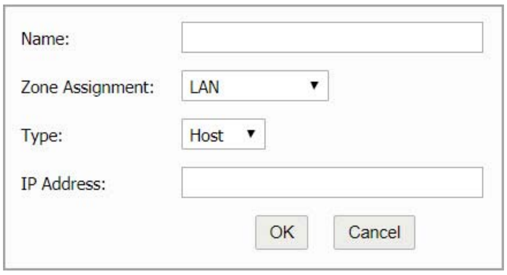
6 When finished excluding Address Objects, click **OK**.

### *To add an Address Object to the Excluded Client AV Enforcement List:*

1 Navigate to the **FIREWALL | Manage | Security Services > Client AV Enforcement** page.

2 Scroll to the **Client Anti-Virus Enforcement** section.

3 Click the **Add** icon for the **Excluded from McAfee/Kasperski Client AV Enforcement List**. The **Add Address Object** dialog displays.



Name:

Zone Assignment: LAN

Type: Host

IP Address:

4 Enter a friendly name in the **Name** field.

5 Select the zone from the **Zone Assignment** drop-down menu.

6 Select the type from the **Type** drop-down menu.

7 Enter the IP address of the Address Object in the **IP Address** field.

8 Click **OK**.

# GMS API Enhancements

GMS provides API enhancements in security, performance, and versioning. Four thousand additional API commands include enhancements for:

- IPSec VPN
- Action Objects
- IPv6
- SSL-VPN
- User / group Objects
- Bandwidth Objects
- App Rules
- DPI-SSL Policies
- Capture
- Email Objects
- CFS Policies
- Wireless
- Match Objects
- CFS Objects
- DPI Policies
- SonicWave

GMS uses Swagger for API implementation. To display the Swagger API specifications online, click the link, **HTTPS://SONICOS-API.SONICWALL.COM**, on the GMS management interface.

# External Storage of Trace Logs

During a normal operation of a firewall, all the State and Critical Logs (A.K.A. Trace Logs) are stored in system memory. During a warm restart, these Trace Logs are copied into flash memory and then cleared from system memory to allow the latter to become ready to store new logs. Thus, flash memory acts as a persistent storage for Trace Logs. As flash memory is limited in its capacity, the quota allocated for Trace Logs is also limited: a maximum of eight log files, each of 128 KB x Number of Cores, can be stored in flash memory at a time. When the Trace Logs reach their quota limit, they are either:

- Wrapped around (currently for state logs) in system memory.
- Discarded (currently for critical logs).

On a warm restart, the system memory log is copied to a new or already existing log file (in case the number limit is reached). This process continues on each warm restart. On a cold restart, however, the system memory Trace Log is discarded.

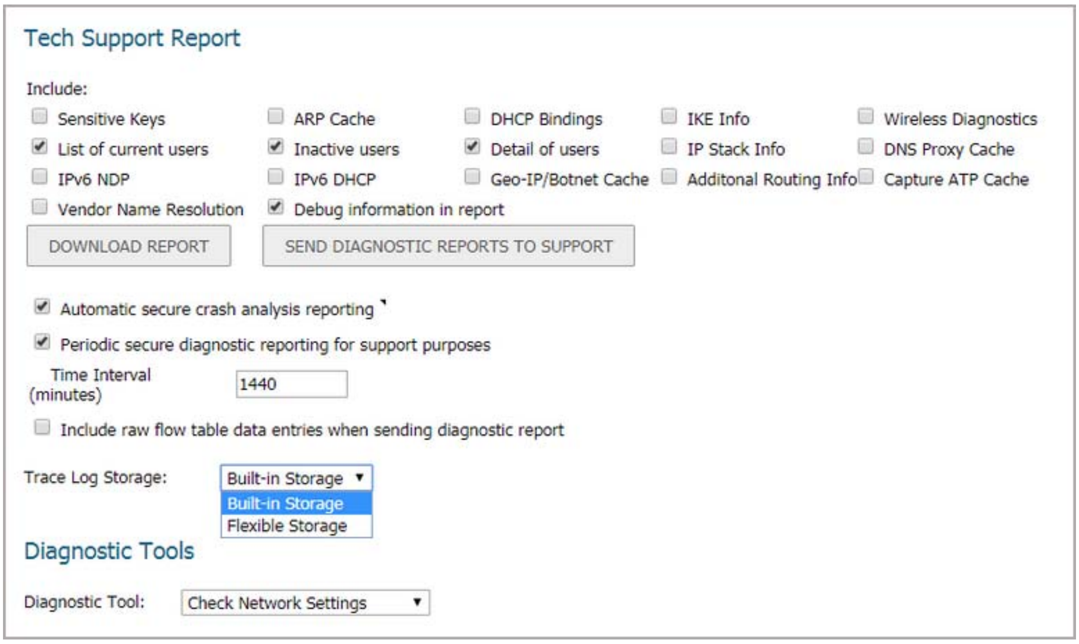
GMS allows Trace Logs to be stored into an external storage device that is present on the firewall and fully functional. As external storage devices have much higher capacities than flash memory, more and/or larger-sized Trace Logs can be stored in them. Also, instead of discarding Trace Logs when the Trace Logs space in system memory becomes full, they are saved in external storage the same way as during a warm restart.

The number of files that can be stored in:

- Flash memory is eight log files of 128KB x Number of CPU Cores each.
- An external drive is 10 times the number supported in flash memory; that is, 10 x 128 Kb x Number of CPU Cores x eight files (one for each last warm restart).

***To select an external storage device:***

1 Navigate to **FIREWALL | Manage | Diagnostics > Network**. Scroll down to Tech Support Report.



Tech Support Report

Include:

□ Sensitive Keys □ ARP Cache □ DHCP Bindings □ IKE Info □ Wireless Diagnostics
☑ List of current users ☑ Inactive users ☑ Detail of users □ IP Stack Info □ DNS Proxy Cache
□ IPv6 NDP □ IPv6 DHCP □ Geo-IP/Botnet Cache □ Additonal Routing Info □ Capture ATP Cache
□ Vendor Name Resolution ☑ Debug information in report

DOWNLOAD REPORT SEND DIAGNOSTIC REPORTS TO SUPPORT

☑ Automatic secure crash analysis reporting

☑ Periodic secure diagnostic reporting for support purposes

Time Interval (minutes): 1440

□ Include raw flow table data entries when sending diagnostic report

Trace Log Storage: Built-in Storage ▾

Diagnostic Tools

Diagnostic Tool: Check Network Settings ▾

2 Scroll to **Trace Log Storage**.

3 Select **Flexible Storage** as the type of external storage device.

4 Click **Update**. The firewall uses this device immediately.

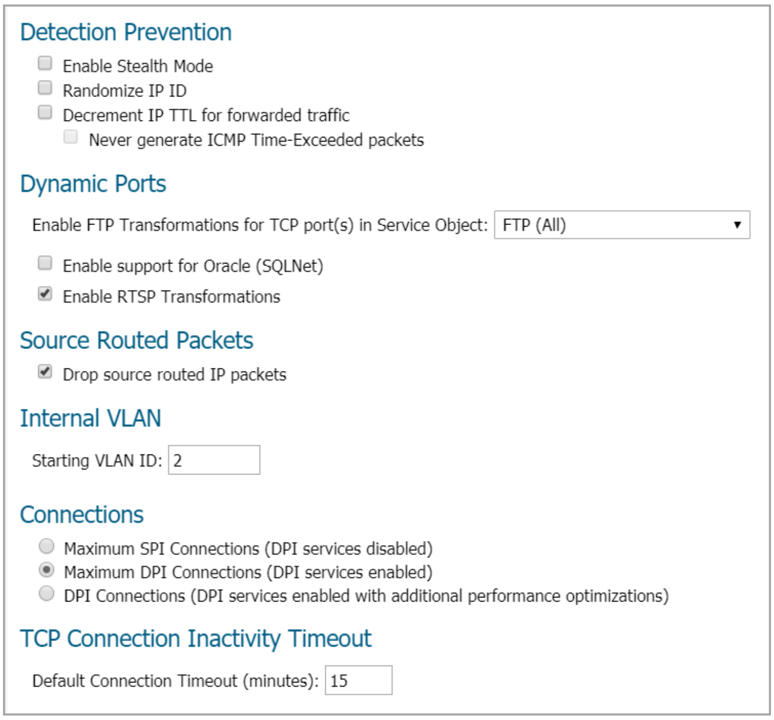
# OpenSSL Support

GMS supports OpenSSL 1.0.2.

# Configurable Internal VLANs

GMS supports a configurable starting VLAN on TZ300-TZ600 series, NSA series, NSA series, and SuperMassive 9000 series firewalls.

An I**nternal VLAN** section has been added to **FIREWALL | Manage | Firewall Settings > Advanced**:



Detection Prevention

- □ Enable Stealth Mode
- □ Randomize IP ID
- □ Decrement IP TTL for forwarded traffic
  - □ Never generate ICMP Time-Exceeded packets

Dynamic Ports

Enable FTP Transformations for TCP port(s) in Service Object: FTP (All)

- □ Enable support for Oracle (SQLNet)
- ☑ Enable RTSP Transformations

Source Routed Packets

- ☑ Drop source routed IP packets

Internal VLAN

Starting VLAN ID: 2

Connections

- ○ Maximum SPI Connections (DPI services disabled)
- ● Maximum DPI Connections (DPI services enabled)
- ○ DPI Connections (DPI services enabled with additional performance optimizations)

TCP Connection Inactivity Timeout

Default Connection Timeout (minutes): 15

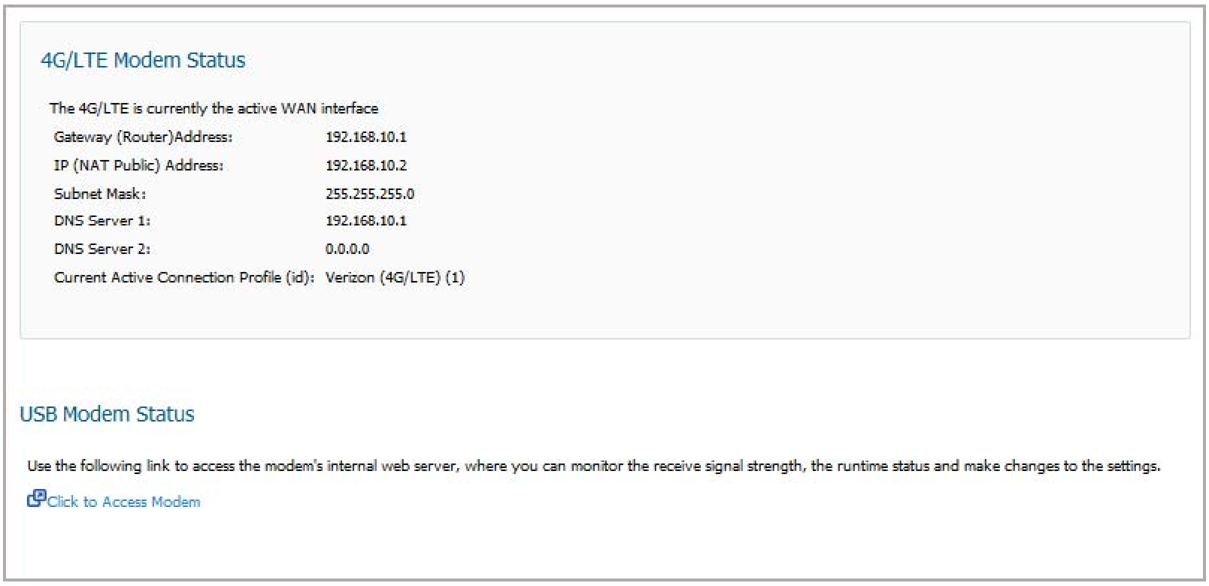
The default VLAN ID is **2**.

For the configured internal VLAN to take effect, you must restart the firewall. When you configure the internal VLAN, a **RESTART** button appears on the **FIREWALL | Manage | Firewall Settings > Advanced** page.

# 4G/LTE USB Modem Support

Newer 4G/LTE USB modems provide status information, such as signal strength, through an internal web server instead of the AT command used by older modems. To support these newer modems, GMS acts as a proxy server for a modem's internal web server.

Access the modem's internal web server through the **FIREWALL | Manage | Access Points > Station Status** page of the GMS management interface:



4G/LTE Modem Status

The 4G/LTE is currently the active WAN interface

| | |
|---|---|
| Gateway (Router)Address: | 192.168.10.1 |
| IP (NAT Public) Address: | 192.168.10.2 |
| Subnet Mask: | 255.255.255.0 |
| DNS Server 1: | 192.168.10.1 |
| DNS Server 2: | 0.0.0.0 |
| Current Active Connection Profile (id): | Verizon (4G/LTE) (1) |

USB Modem Status

Use the following link to access the modem's internal web server, where you can monitor the receive signal strength, the runtime status and make changes to the settings.

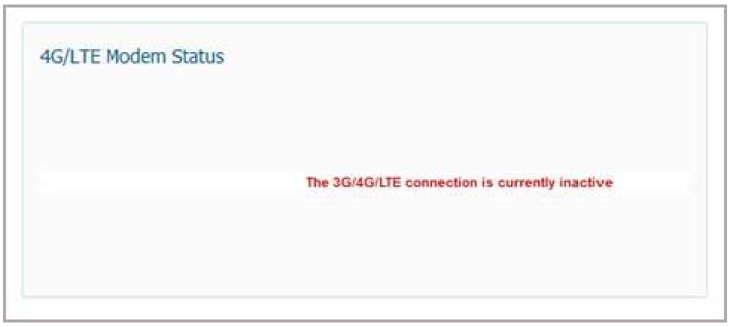
Click to Access Modem

**NOTE:** Unlike with older model modems, the receive signal strength is not displayed. Use the `Click to Access Modem` link to view the receive signal strength.

***To access the modem's internal web server:***

1. Navigate to the **MONITOR | Current Status > 3G/4G/Modem Status page**.
2. Scroll to the **USB Modem Status** section.
3. Click the **Click to Access Modem** link. The proxy page displays in a new management interface page you can view as a separate browser window. From the proxy page, you can view such data as received signal strength and view or change modem settings.

   **TIP:** If an IP address is not displayed because the connection is inactive, the **Click To Access Modem** link does not work.

   4G/LTE Modem Status

   The 3G/4G/LTE connection is currently inactive

# IPv6 Addressing Mode for H.323 ALG

GMS fully supports IPv6 addressing mode for H.232 ALG (application layer gateway) that connects IPv6 and IPv4 networks. When users make H.323 phone calls in IPV6 mode, the calls actually traverse through the firewall, with the message correctly transformed to hide the private address information that should not be revealed. Navigate to the **FIREWALL | Manage | VoIP > Settings** page to configure details.

# Enhancements to Reports

**Topics:**

- Display Appflow Statistical Data Since Last Reset
- Language and Style Selection for SFR Reports

# Display Appflow Statistical Data Since Last Reset

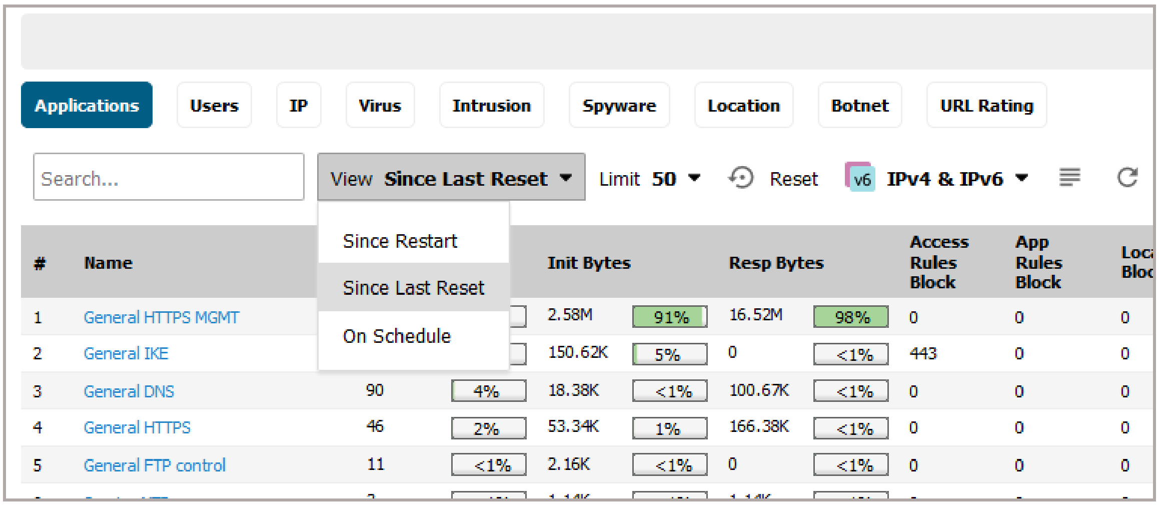
GMS provides a way to display and send both Appflow and Capture Threat Assessment reports after a manual reset.

**Topics:**

- Appflow Reports
- Capture Threat Assessment

## Appflow Reports

On the FIREWALL | Manage | AppFlow > Appflow Reports page, you can now display the statistical data since last reset as well as since restart and on a schedule:



View **Since Last Reset**   Limit **50**   **IPv4 & IPv6**

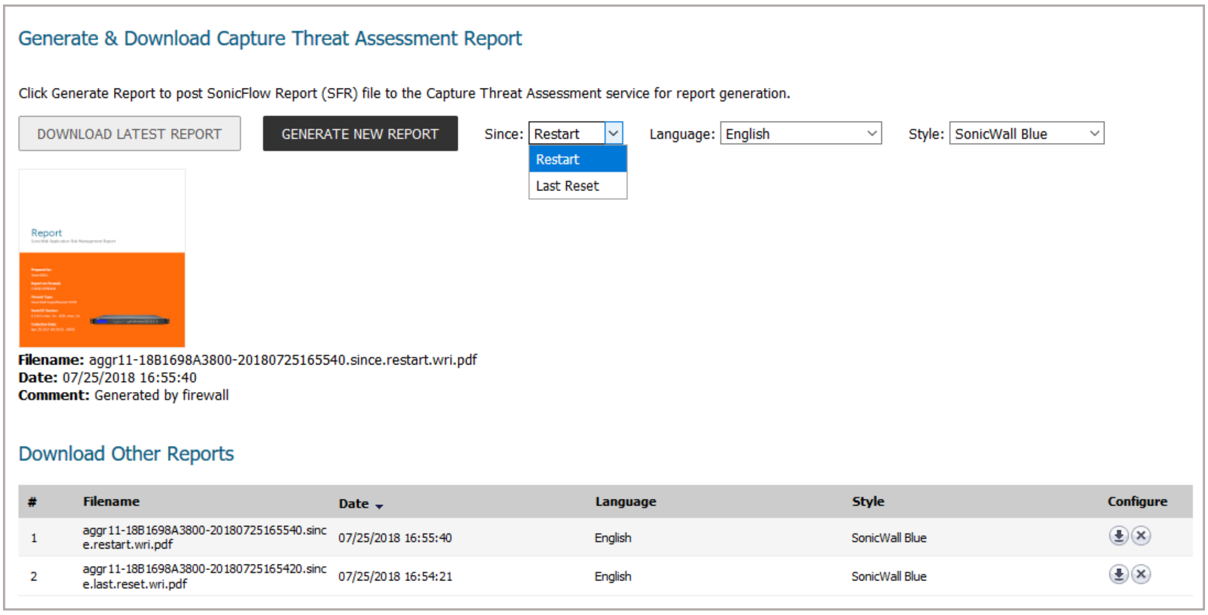
| # | Name | | | Init Bytes | | Resp Bytes | | Access Rules Block | App Rules Block | Loc Bloc |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | General HTTPS MGMT | | | 2.58M | 91% | 16.52M | 98% | 0 | 0 | 0 |
| 2 | General IKE | | | 150.62K | 5% | 0 | <1% | 443 | 0 | 0 |
| 3 | General DNS | 90 | 4% | 18.38K | <1% | 100.67K | <1% | 0 | 0 | 0 |
| 4 | General HTTPS | 46 | 2% | 53.34K | 1% | 166.38K | <1% | 0 | 0 | 0 |
| 5 | General FTP control | 11 | <1% | 2.16K | <1% | 0 | <1% | 0 | 0 | 0 |

When you select **Since Last Reset** from **View**, a **Reset** icon displays between the **Limit** and **IPv4/IPv6** options. You can manually reset the statistics by clicking the icon.

Your view selection also is reflected in the reports you generate manually.

## Capture Threat Assessment

On the **FIREWALL | Manage | Capture ATP > Capture Threat Assessment** page, you can specify either **Restart** or **Last Reset** from **Since**. The **Last Reset** choice for the Capture Threat Assessment report depends on the setting on the **FIREWALL | Manage | AppFlow > Appflow Reports** page.



Generate & Download Capture Threat Assessment Report

Click Generate Report to post SonicFlow Report (SFR) file to the Capture Threat Assessment service for report generation.

Since: Restart

Language: English

Style: SonicWall Blue

**Filename:** aggr11-18B1698A3800-20180725165540.since.restart.wri.pdf
**Date:** 07/25/2018 16:55:40
**Comment:** Generated by firewall

Download Other Reports

| # | Filename | Date | Language | Style | Configure |
|---|---|---|---|---|---|
| 1 | aggr11-18B1698A3800-20180725165540.since.restart.wri.pdf | 07/25/2018 16:55:40 | English | SonicWall Blue | ⬇ ✕ |
| 2 | aggr11-18B1698A3800-20180725165420.since.last.reset.wri.pdf | 07/25/2018 16:54:21 | English | SonicWall Blue | ⬇ ✕ |

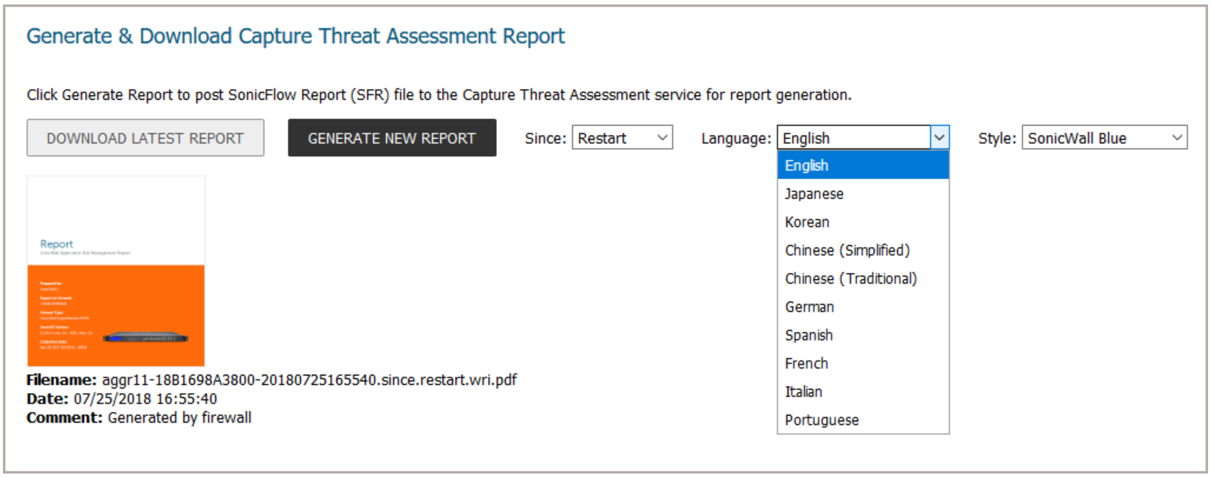
# Language and Style Selection for SFR Reports

**Topics:**

- Language Selection
- Style Selection
- Language and Style of Reports

## Language Selection

A new option, **Language**, on the **FIREWALL | Manage | Capture ATP > Capture Threat Assessment** page allows you to select the language for your SFR report:



Generate & Download Capture Threat Assessment Report

Click Generate Report to post SonicFlow Report (SFR) file to the Capture Threat Assessment service for report generation.

Since: Restart

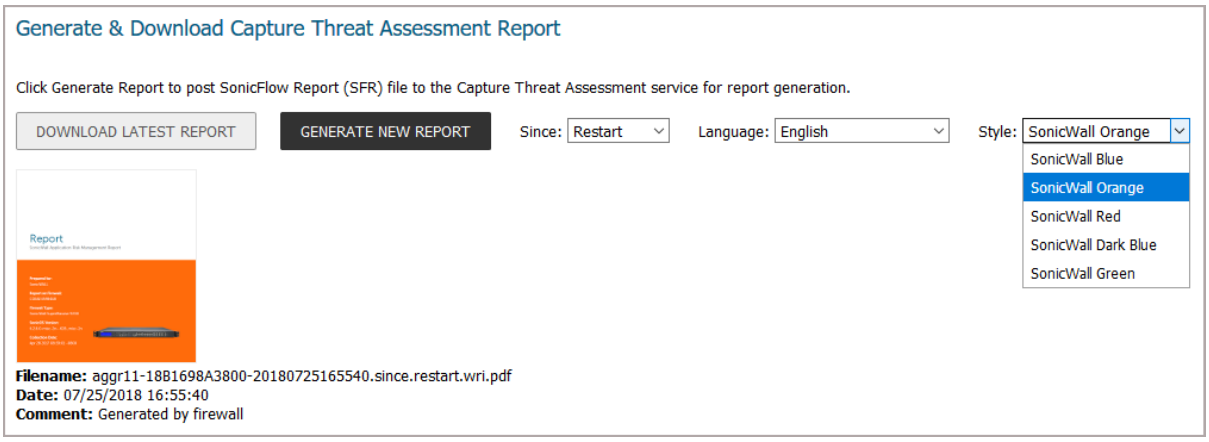
Language: English

Style: SonicWall Blue

**Filename:** aggr11-18B1698A3800-20180725165540.since.restart.wri.pdf
**Date:** 07/25/2018 16:55:40
**Comment:** Generated by firewall

## Style Selection

A new option, **Style**, on the **FIREWALL | Manage | Capture ATP > Capture Threat Assessment** page allows you to select the color for your SFR report:



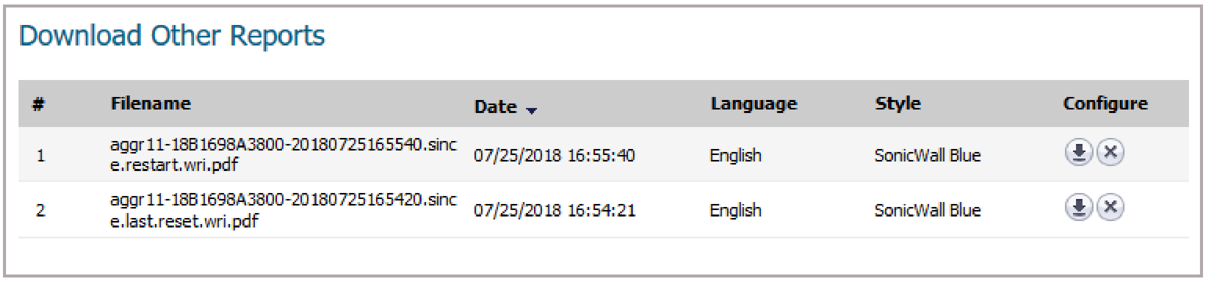
Generate & Download Capture Threat Assessment Report

Click Generate Report to post SonicFlow Report (SFR) file to the Capture Threat Assessment service for report generation.

**Filename:** aggr11-18B1698A3800-20180725165540.since.restart.wri.pdf
**Date:** 07/25/2018 16:55:40
**Comment:** Generated by firewall

## Language and Style of Reports

The **Download Other Reports** section of the **FIREWALL | Manage | Capture ATP > Capture Threat Assessment** page displays the language and style of each of the reports listed.



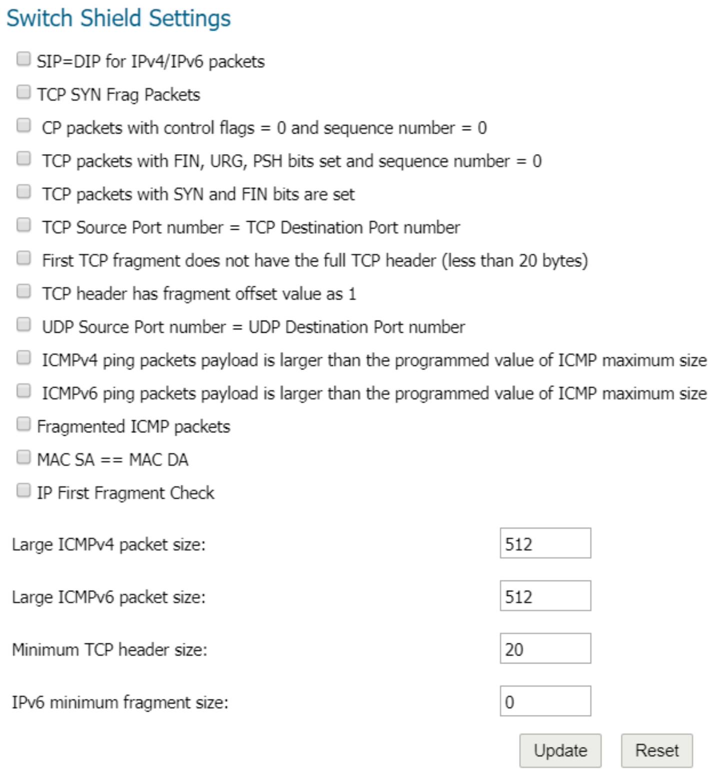
Download Other Reports

| # | Filename | Date | Language | Style | Configure |
|---|---|---|---|---|---|
| 1 | aggr11-18B1698A3800-20180725165540.since.restart.wri.pdf | 07/25/2018 16:55:40 | English | SonicWall Blue | |
| 2 | aggr11-18B1698A3800-20180725165420.since.last.reset.wri.pdf | 07/25/2018 16:54:21 | English | SonicWall Blue | |

# Switch Shield Support (DDOS Protection using Switch Capabilities)

> **NOTE:** This feature is supported on NSA 3600 through NSA 6600, NSA series, and SuperMassive series platforms. For the NSA 6600 and other platforms that do not have ports connected through the Broadcom switch (directly connected ports), this feature applies only to ports that are connected through the Broadcom switch (indirectly connected ports).

This feature provides protection from a Denial of Service attacks that make the firewall too busy to provide service. A new management interface page, **FIREWALL | Manage | Switching > Switch Shield**, has been added to GMS:



Switch Shield Settings

- □ SIP=DIP for IPv4/IPv6 packets
- □ TCP SYN Frag Packets
- □ CP packets with control flags = 0 and sequence number = 0
- □ TCP packets with FIN, URG, PSH bits set and sequence number = 0
- □ TCP packets with SYN and FIN bits are set
- □ TCP Source Port number = TCP Destination Port number
- □ First TCP fragment does not have the full TCP header (less than 20 bytes)
- □ TCP header has fragment offset value as 1
- □ UDP Source Port number = UDP Destination Port number
- □ ICMPv4 ping packets payload is larger than the programmed value of ICMP maximum size
- □ ICMPv6 ping packets payload is larger than the programmed value of ICMP maximum size
- □ Fragmented ICMP packets
- □ MAC SA == MAC DA
- □ IP First Fragment Check

| | |
|---|---|
| Large ICMPv4 packet size: | 512 |
| Large ICMPv6 packet size: | 512 |
| Minimum TCP header size: | 20 |
| IPv6 minimum fragment size: | 0 |

***To enable Switch Shield protection:***

1. Navigate to **FIREWALL | Manage | Switching > Switch Shield**.
2. Select the Switch Shield options to be enabled. To protect against:
   - IP packets in which the source IP equals the destination IP, select **SIP = DIP for IPv4/IPv6 packets**
   - TCP Syn fragmented packets, select **TCP Syn Frag Packets**
   - TCP packets without control flags or sequence, select **TCP packets with control flags = 0 and sequence number = 0**
   - TCP packets with FIN, URG, and PSH bits enabled and the sequence number equal to 0, select **TCP packets with FIN, URG, and PSH bits set and sequence number = 0**
   - TCP packets with SYN and FIN bits enabled, select **TCP packets with SYN and FIN bits are set**
   - TCP packets with the source port equal to the destination port, select **TCP Source Port = TCP Destination Port**
   - TCP packets with a partial (< 20 bytes) header, select **First TCP fragment does not have the full TCP header (less than 20 bytes**)

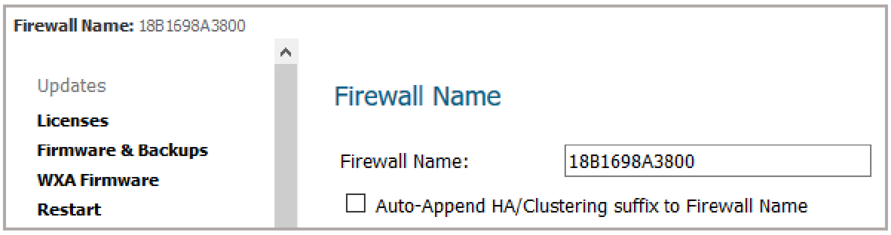
- TCP header offset equal to 1, select **TCP header has fragment offset value as 1**
- UDP packets with the source Port equal to the destination port, select **UDP Source Port number = UDP Destination Port number**
- Fragmented ICMP packets, select **Fragmented ICMP packets**
- Packets in which the source MAC address equals the destination MAC address, enable **MAC SA == MAC DA**
- IPv4 first fragment, select **IP first Fragment Check**
- Oversized or big ICMP packets, specify the maximum packet size in the:
  - **Large ICMPv4 packet size** field
  - **Large ICMPv6 packet size** field
- Invalid TCP headers, specify the minimum header size in the **Minimum TCP header size** field
- Small IPv6 fragments, enter the minimum fragment size in the **IPv6 minimum fragment size** field

3 Click **Update**.

# Pin Friendly Name of Firewall

By default, the firewall name is generated by the firewall itself and consists of a string of alphanumeric characters. In GMS, you can change that to a more meaningful, “friendly,” name on the **FIREWALL | Manage | System > Management** page. This friendly name is pinned to the management interface pages instead of the firewall-generated one.

Firewall-generated name



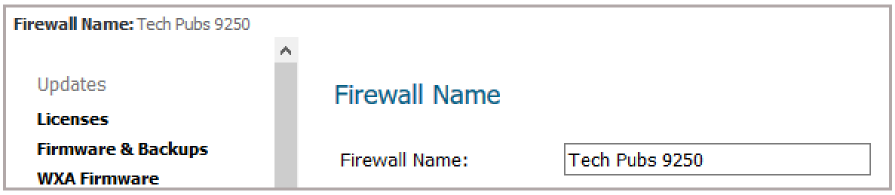
Firewall Name: 18B1698A3800

Firewall Name

Firewall Name: 18B1698A3800

□ Auto-Append HA/Clustering suffix to Firewall Name

Friendly name



Firewall Name: Tech Pubs 9250

Firewall Name

Firewall Name: Tech Pubs 9250

ⓘ **TIP:** Record the firewall-generated name along with its friendly name.

# Resolved Issues

The following is a list of issues addressed in this release.

### Backend Communication

| Resolved Issue | Issue ID |
|---|---|
| Synchronizing GMS with MySonicWall isn't working. | 199349 |

### Database

| Resolved Issue | Issue ID |
|---|---|
| Vulnerabilities were reported during a PCI Audit scan of MySQL. | 192283 |

### Diagnostics

| Resolved Issue | Issue ID |
|---|---|
| TSR fails to download as expected. | 207801 |

### Console Panel

| Resolved Issue | Issue ID |
|---|---|
| Secure Access: Guest users with View Only access attempt to unlock locked users, but the user interface returns an “Update Failed: Invalid Input” error message. | 207363 |
| Selecting multiple change orders does not generate a Compliance report and there are no console logs being displayed. | 202850 |
| When logging in to GMS from other accounts, the “Add user Type” option does not function as expected. | 199219 |

### Firewall Configuration

| Resolved Issue | Issue ID |
|---|---|
| Enabling BWM checkboxes on an access rule in GMS 8.5 does not enable it on the firewall as expected. | 211332 |
| The “Add Route Policy” dialog box loads continuously and eventually crashes the web-page. | 203460 |

### GMS

| Resolved Issue | Issue ID |
|---|---|
| GMS uploads signature data to only one TZ in a group and fails to upload to all other TZs in the group. | 213430 |
| Unable to delete MAC address objects created at the Group level. | 209063 |
| Numerous services do not connect to the database as expected after rebooting. | 209021 |
| GMS 8.4 vulnerabilities reported as CVE-2017-3454, CVE-2017-3455, CVE-2017-3600, and CVE-2017-3633. | 203321 |

### Inheritance

| Resolved Issue | Issue ID |
|---|---|
| Reverse inheritance fails for the Wire mode from unit to group as well as for the units managed under it. | 193340 |
| Content Filtering 4.0 policy inheritance tasks do not function as expected. Required dependent objects are not applied. | 191691 |

### Installation/Upgrade

| Resolved Issue | Issue ID |
|---|---|
| The ability to directly upgrade a lower version of GMS to a higher version without upgrading all releases and service packs in between. | 206869 |

### Policies Panel

| Resolved Issue | Issue ID |
|---|---|
| Pushing signature updates to the firewalls from GMS does not function as expected. | 211094 |
| Guest Account passwords are being masked when auto-generated. | 209496 |
| Reverse Inheritance of a “SonicPoint Wave2 Profile” does not update the “Service Provider” and “Plan Type” options in the 3G/4G/LTE WWAN Connection profile settings. | 207854 |
| Modifying the Default CFS policy creates duplicate CFS policies at the Group level. | 207819 |
| Because some L2TP interfaces cannot be added to GMS, two text boxes are missing: Gateway IP and Subnet Mask. | 207366 |
| Deleting an Address Object group at the Group/Global level does not delete the actual group. Instead, it deletes the contents of that group and then creates an empty Address Object group. | 207357 |
| When authentication is set to “WPA2-PSK” or “WPA2-EAP,” inheritance of a Virtual Access Points profile fails at the Unit level. | 206256 |
| When authentication is set to “WPA2-PSK” or “WPA2-AUTO-PSK,” the Inheritance of a SonicPoint profile fails at the unit level. | 206214 |
| Editing the “Capture Client Enforcement List” in Group UTMs creates a new “SentinelOne Client AV Enforcement List.” | 206152 |
| Test connectivity for password authentication shows no data in GMS, but the authentication is successful in the UTM. | 206074 |
| Test connectivity on the Test TACACS Settings page does not function correctly from the GMS side but is successful in the UTM. | 206070 |
| Unable to add a Sonicpoint Wave2 Profile because the **OK** button is non-responsive at the Unit level/Group level. | 206018 |
| Virtual Access Points fails at the unit level with “Virtual Access Point/Group/NAME: WPA passphrase is not valid” or “WPA Radius Server 1 secret is not valid” error messages. | 205953 |
| When editing a WAN interface and selecting the WAN assignment as DHCP on the Advanced tab, two necessary checkboxes are missing from the GMS screen. | 205927 |
| GMS does not show a second TACACS+ profile when it has been added. | 205848 |
| Data mismatch of SonicPoint profiles between GMS and the UTM. | 205723 |
| The **FIREWALL \| Manage \| Network > Default NAT policy** (any interface-to-any interface) is not visible at the group level. | 205684 |

### Policies Panel (Continued)

| Resolved Issue | Issue ID |
|---|---|
| Adding a LAN or VLAN Interface in GlobalView does not list Wire Mode in the IP Assignment drop-down menu. | 203593 |
| Deleting the VLAN entries from the group level, deletes them at the group level, but the VLAN remains “as is” on the unit level. | 196600 |

### Reporting

| Resolved Issue | Issue ID |
|---|---|
| The GMS overwrite option for custom reports overwrites the default report ID in error. | 207971 |
| The Botnet pie chart view does not show data on the Dashboard as expected. | 207849 |
| Optimizer crashes the Reports database after upgrading to GMS 8.4.1 on Windows. | 207060 |

### User Interface

| Resolved Issue | Issue ID |
|---|---|
| TCP connections do not close as expected after the user logs out. | 208322 |

### Workflow

| Resolved Issue | Issue ID |
|---|---|
| Permissions are not set as expected after a new firewall has been added and “Assign Privileges” and “All Users” are selected. | 198607 |

# Known Issues

The following is a list of issues known to exist at the time of the GMS 8.7 release.

### Appliance

| Known Issue | Issue ID |
|---|---|
| The Auto Export Tool fails to download backup files after upgrading to GMS 8.6. | 211521 |

### Console Panel

| Known Issue | Issue ID |
|---|---|
| The View Change Order page does not show a scroll bar as expected which makes checking an item tedious. | 212014 |
| Action Objects are not deleted as expected when the name includes Unicode characters. | 211914 |
| GMS Summarization functions very slowly when the debug LOG level is set at 5. | 211054 |
| The ConnectWise Asset synchronization does not automatically occur after GMS has been uninstalled. | 210631 |

### Net Monitor

| Known Issue | Issue ID |
|---|---|
| Net monitor does not function as expected for Edge browsers because Java plug-in support does not exist. | 214607 |

### Policies Panel

| Known Issue | Issue ID |
|---|---|
| FQDN objects are not listed as expected under **Performance Probes > Probe Target**. | 215032 |
| SD-WAN groups: Adding more than 10 SD-WAN groups should be possible. | 214852 |
| Group and Global Inheritance filters do not appear as expected in their respective Performance Probe sections. | 214697 |
| Forward inheritance does not function as expected in SD-WAN Route policies. | 214601 |
| Reverse Inheritance for **FIREWALL \| Manage \| Network > Route Policies** does not function as expected. | 214461 |
| The **High Availability Communication Encryption** checkbox does not function as expected. | 214144 |
| Adding an SD-WAN Route Policy at the group level fails to push the policy to the unit. | 214079 |
| Wifisec settings for WLAN are unavailable in GMS. | 211994 |
| Forward inheritance for zones does not always function as expected. | 210992 |
| Monthly data deletion does not function as expected resulting in a Reports Database II failure. | 203834 |

### Reports Panel

| Known Issue | Issue ID |
|---|---|
| After a license has expired, subscription alerts do not function as expected. | 211664 |
| GMS Reports show an ID (number) instead of a Name because there are missing signatures in the database tables. | 197774 |

# Platform Compatibility

The SonicWall Global Management System 8.7 release can be hosted in two deployment scenarios as follows:

- Microsoft Windows Server Software
- VMware ESXi Virtual Appliance

Deployment Considerations:

- Before selecting a platform to use for your GMS deployment, use the Capacity Planning Tool at https://www.SonicWall.com/en-us/products/firewalls/management-and-reporting/global-management-system. This helps you set up the correct GMS system for your deployment.

△ CAUTION: **SonicWall recommends that you take steps to minimize abrupt shutdowns of the server hosting GMS, as this can cause corruption of the Reporting database, potentially leading to loss of data for the current month. A possible solution includes using an Uninterrupted Power Supply (UPS).**

Before installing GMS 8.7, ensure that your system meets the minimum hardware and software requirements described in the following sections:

- Supported Platforms
- Unsupported Platforms
- Hardware Requirements
- Hard Drive HDD Specifications
- GMS Virtual Appliance Supported Platforms
- Virtual Appliance Deployment Requirements
- Browser Requirements

- Microsoft SQL Server Requirements
- Java Support
- SonicWall Appliances Supported for GMS Management
- Non-SonicWall Appliance Support

# Supported Platforms

The SonicWall Global Management System supports the following Microsoft Windows operating systems:

- Windows Server 2016 Standard (English and Japanese language versions)
- Windows Server 2012 Standard 64-bit
- Windows Server 2012 R2 Standard 64-bit (English and Japanese language versions)
- Windows Server 2012 R2 Datacenter

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

> **TIP:** For best performance and scalability, it is recommended to use a 64-bit Windows operating system. Bundled databases run in 64-bit mode on 64-bit Windows operating systems. All listed operating systems are supported in both virtualized and non-virtualized environments. In a Hyper-V virtualized environment, Windows Server is a guest operating system running on Hyper-V. GMS is then installed on the Windows Server virtual machine that is layered over Hyper-V.

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

# Unsupported Platforms

The following platforms have been dropped from support:

- CDP management and reporting
- UMA EM5000 as part of the GMS deployment
- Windows 32-bit as part of the GMS deployment
- Firewalls with firmware older than SonicOS 5.0
- Gen4 or older Firewalls

# Hardware Requirements

To determine the hardware requirements for your deployment, use the Capacity Planning Tool at https://www.SonicWall.com/en-us/products/firewalls/management-and-reporting/global-management-system.

> **NOTE:** A Windows 64-bit operating system with at least 16GB of RAM is highly recommended for better performance of reporting modules. For more information, read the “Capacity Planning and Performance Tuning” appendix in the *SonicWall Global Management System Administration Guide*.

# Hard Drive HDD Specifications

The following hard drive HDD specifications are required when using GMS Software on a Windows Server or a GMS Virtual Appliance:

**Hardware Requirements**

| Requirement | Details |
|---|---|
| Spindle Speed | 10,000 RPM or higher |
| Cache | 64 MB or higher |
| Transfer rate | 600 MBs or higher |
| Average latency | 4 microseconds or lower |

# GMS Virtual Appliance Supported Platforms

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

- ESXi 6.5, 6.0 and 5.5

# Virtual Appliance Deployment Requirements

Consider the following before deploying the GMS Virtual Appliance:

- GMS management is not supported on Apple MacOS.
- All modules are 64-bit.
- Using the Flow Server Agent role requires a minimum of:
  - Quad Core
  - 16GB of memory
  - 300GB available disk space

To determine the hardware requirements for your deployment, use the Capacity Planning Tool at https://www.SonicWall.com/en-us/products/firewalls/management-and-reporting/global-management-system.

The performance of GMS Virtual Appliance depends on the underlying hardware. It is highly recommended to dedicate all the resources that are allocated to the Virtual Appliance, especially the hard-disk (datastore). In environments with high volumes of syslogs or AppFlow (IPFIX), you will need to dedicate local datastores to the GMS Virtual Appliance.

Read the “Capacity Planning and Performance Tuning” appendix in the *SonicWall Global Management System Administration Guide*.

# Browser Requirements

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

This release supports the following Web browsers:

- Chrome 42.0 or higher (recommended browser for dashboard real-time graphics display)
- Firefox 37.0 or higher

- Microsoft Edge 41 or higher
- Safari 11 or higher (MAC only)

Mobile device browsers are not recommended for SonicWall Global Management System system administration.

ⓘ **NOTE:** If using Chrome version 42 and newer to access GMS 7.2 and older, you will need to enable NPAPI support in Chrome, which by default has been disabled starting with version 42.

# Microsoft SQL Server Requirements

The following SQL Server versions are supported:

- SQL Server 2014
- SQL Server 2012

ⓘ **NOTE:** For SQL Server deployments in countries in which English is not the default language, set the default language to English in the Login Properties of the GMS database user in the SQL Server configuration.

ⓘ **NOTE:** A database user with “DB Creator” privileges must be provided to GMS during the Role Configuration process of any GMS Server.

# Java Support

ⓘ **NOTE:** Java is required only when you are using Net Monitor.

Download and install the latest version of the Java 8 plug-in on any system that accesses the GMS management interface. This can be downloaded from:

www.java.com

or

http://www.oracle.com/technetwork/java/javase/downloads/index.html

# SonicWall Appliances Supported for GMS Management

ⓘ **NOTE:** GMS 8.7 does not support legacy SonicWall appliances, including:

- Firewall appliances running firmware earlier than SonicOS 5.0
- CSM Series
- CDP Series

SonicWall Global Management System 8.7 supports the following SonicWall appliances and firmware versions:

**Component Requirements**

| SonicWall Platforms | SonicWall Firmware Version |
|---|---|
| **Network Security Appliance** | |
| SuperMassive 10000 Series | SonicOS 6.0 or newer<br>**NOTE**: Only partial policy management and reporting support is currently available. The following SuperMassive specific features are not supported for centralized policy management in GMS:<br>• Multi-blade Comprehensive Anti-Spam Service (CASS)<br>• High Availability/Clustering<br>• Support for Management Interface<br>• Flow Reporting Configurations<br>• Multi-blade VPN<br>• Advanced Switching<br>• Restart: SonicOS versus Chassis<br>Contact your SonicWall Sales representative through https://www.SonicWall.com/en-us/support for more information. |
| SuperMassive 9000 Series | SonicOS 6.1 or newer |
| NSA Series | SonicOS 5.0 or newer |
| TZ Series and TZ Wireless | SonicOS 5.0 or newer |
| SonicWall SOHO | SonicOS 5.9.1.3 or newer 5.9 versions |
| SonicWall SOHO Wireless | SonicOS 6.2.6 or newer 6.x versions |
| **Email Security/Anti-Spam** | |
| Email Security Series | Email Security 7.2 or newer (management only) |
| **Secure Mobile Access** | |
| SMA 6200/7200 | SMA 10.7.2 or newer |
| SRA/SSL-VPN Series | SSL-VPN 2.0 or newer (management)<br>SSL-VPN 2.1 or newer (management and reporting) |
| E-Class SRA Series | E-Class SRA 9.0 or newer |

**Notes**:

- GMS 8.7 supports SonicWall firewall App Control policy management and App Control reporting support. Refer to the SonicOS documentation for information on the supported SonicOS firmware versions.
- Appliances running firmware newer than this GMS release can still be managed and reports can still be generated. However, the new features in the firmware will be supported in an upcoming release of GMS.

# Non-SonicWall Appliance Support

SonicWall Global Management System provides monitoring support for non-SonicWall TCP/IP and SNMP-enabled devices and applications.

# Upgrading to GMS 8.7

GMS can be configured for a single server or in a distributed environment on multiple servers. GMS 8.7 can be installed fresh, or as an upgrade from GMS 8.4 and higher under the following conditions:

> ⓘ **IMPORTANT:** The following is critical for a successful upgrade to GMS 8.7:
>
> You **MUST** first install **Hotfix 215547: 8.7 upgrade - Database fails when the virtual appliance is restarted** before upgrading to GMS 8.7.

Consider the following before upgrading:

- Hotfix 215547 is critical for a successful upgrade to 8.7.
- Hotfix 215547 is required when upgrading directly from GMS 8.4, 8.5, and 8.6.
- GMS 8.7 does not support the Analyzer platform.
- You must disable the User Account Control (UAC) feature on Windows before running the GMS installer. In addition, disable Windows Firewall or your personal firewall before running this installer.
- For appliances under management using a GMS Management Tunnel or Existing Tunnel, make sure that HTTPS management is allowed from the GMS servers. This is because GMS 8.7 logs into the appliances using HTTPS only.
- The scheduled reports created in GMS 8.0 continue to work properly after upgrading to 8.7. However, the Legacy reports created in GMS 6.0 or earlier versions are not migrated. For more information on viewing legacy reports, refer to the *SonicWall Global Management System Administration Guide*.
- When performing a fresh installation of GMS on Windows, the installer prompts for an IPv6 address of the server if it detects an IPv6 network.

In a distributed environment, shut down all GMS servers except the one that is running the database. GMS servers with the **SonicWall Universal Management Suite — Database** service should be upgraded first, and then you can upgrade the other servers. You must upgrade all GMS servers in your deployment to the same version of GMS. You cannot have some servers running version 8.7 and others running older versions.

> ⓘ **NOTE:** DO NOT start/stop the **SonicWall Universal Management Suite—Database** service manually, before or after upgrading to 8.7. After the upgrade, the **SonicWall Universal Management Suite—Database** service will be down until the MySQL upgrade process has completed as well. Login to the /appliance UI to track the progress.

# Upgrading Procedure

***To upgrade to GMS 8.7, complete the following steps:***

1. Navigate to https://www.MySonicWall.com.
2. Download the GMS 8.7 software.
3. After the files have downloaded, double-click the first file and follow the onscreen instructions. The Installer detects any previous installations of GMS. Click **Install** to proceed with the installation.
4. If you see a Windows Security Alert for Java, click **Unblock**. The installer displays a progress bar as the files are installed. Wait a few minutes for the installer to finish installing.

5 After the files are installed, whether or not the system has a Personal Firewall such as Windows Firewall enabled, a dialog is displayed notifying you to either disable the firewall or manually open the syslog and SNMP ports, and to ensure that these ports are open on your network gateway or firewall if you plan to use HTTPS Management mode for Managing remote appliances (instead of GMS Management Tunnel or Existing Tunnel Modes). Click **OK**. Be sure to adjust the settings as recommended.

6 After the installer has completed, reboot the system to complete the installation.

## Prerequisites for Deploying a GMS 8.7 Virtual Appliance on VMware ESXi

SonicWall recommends using versions of ESXi 6.5 or higher. With ESXi 6.5, to protect an ESXi host against unauthorized intrusion and misuse, VMware imposes constraints on several parameters, settings, and activities. For increased security, SHA-256 with the PKCS#1 RSA encryption signature algorithm is used for the default certificates in both:

- SonicWall GMS 8.7 Virtual Appliance firmware
- VMware ESXi 6.5

## Installing GMS 8.7 on VMware ESXi

GMS 8.7 can be installed on ESXi version 5.5 or newer using the vCenter client corresponding supported versions 5.5 or newer. GMS can also be deployed from the ESXi host client. Use the vCenter client corresponding to the supported ESXi version 5.5 and above and deploy GMS from the ESXi host client. Refer to earlier GMS guides on how to install or upgrade older versions of GMS.

## Upgrading a GMS Virtual Appliance

This section provides procedures for upgrading an existing SonicWall GMS 8.6 virtual appliance or newer installation to GMS 8.7 virtual appliance.

> ⓘ **IMPORTANT:** The following is critical for a successful upgrade to GMS 8.7:
>
> You **MUST** first install **Hotfix 215547: 8.7 upgrade - Database fails when the virtual appliance is restarted** before upgrading to GMS 8.7.

***To upgrade a GMS Virtual Appliance, complete the following:***

1 Download the GMS 8.7 file from www.MySonicWall.com to your workstation software: **sw_gmsvp_all_eng_8.7.*xxxx.yyyy*.<*file format*>**: where ***xxxx*** is the major build number and ***yyyy*** is the minor build number.

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

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

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

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

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

# Product Licensing

All instances of SonicWall Global Management System Software must be registered and licensed before use. This requirement applies to both single server deployments or distributed deployments on multiple servers, to fresh or upgraded installations, and to software installations on Windows servers or VMware Virtual Appliances. SonicWall Global Management System registration is done using the `/appliance` Universal Management Host (UMH) system interface. When installing Universal Management Suite on a server or host, a Web server is installed to provide the `/appliance` UMH system interface. The system interface is available by default after restarting the system at: https://localhost/. To complete registration, the system must have access to the Internet and you must have a MySonicWall account. The SonicWall License Manager, available on the **System > Licenses** page of the UMH system interface, allows you to log in and enter your registration information at https://MySonicWall.com.

# 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.

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 reserve 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.

To view the SonicWall End User Product Agreement, go to: https://www.SonicWall.com/legal/eupa. Select the language based on your geographic location to see the EUPA that applies to your region.

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

Last updated: 3/27/19

232-004604-00 Rev B