

SonicWall® Global Management System 9.2

Getting Started Guide



Contents

Part 1. Introducing GMS

Introduction to GMS	5
---------------------------	---

Part 2. Installing GMS

Before You Begin	7
System Requirements	7
Installation Quick Start	8
Record Configuration Information	8
Installing the GMS OVA File	9
Setting Up the Network Configuration	16
Configuring the System	18
Performing Basic Tasks and Manual Host Configuration	21
Power the Virtual Appliance On	21
Configure Host Settings on the Console	22
Configure Host Settings on the Appliance Management Interface	23
Viewing the Settings Summary	24
Editing The Virtual Machine Settings	25
Setting the Install Mode	26
Single Server Deployment	26
Distributed Deployment	30
Registering GMS	42
GMS Registration	42
Adding Devices	45
Basic Mode	45
Advanced Mode	46

Part 3. Using GMS

Using the GMS Management Interface	50
Centralized Management and Monitoring	51
Distributed Intelligent Platform Monitoring	53
Navigating the GMS Management Interface	55
CONSOLE View	59
Understanding GMS Icons	59
HOME View	61
HOME View (Flow Based)	61
Live Monitor	65

HOME View (Syslog Based)	66
MANAGE View	67
SETUP	67
SYSTEM	68
SECURITY	68
REPORTS View	69
REPORTS View (Flow Based)	69
REPORTS View (Syslog Based)	71
ANALYTICS View	73
Status	73
CONSOLE View	78
Control Center	80
ZeroTouch	86
Connectwise	86
Reports	87
SonicWall Support	92
About This Document	93

Introducing GMS

- Introduction to GMS

Introduction to GMS

SonicWall® Global Management System (GMS) is a Web-based application that can configure and manage thousands of SonicWall firewall appliances from a central location.

SonicWall GMS is:

- easy to install
- easy to configure
- easy to license
- easy to add devices to
- easy to monitor and manage your GMS instances using the Control Center and the Intelligent Platform Monitor (IPM)

GMS can be used as a Management Console in an Enterprise network containing a single SonicWall appliance, and it 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. This dramatically lowers the cost of managing a secure distributed network. GMS does this by enabling 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 also includes Analytics for flow-based reporting. Analytics is a powerful management tool that provides intelligence-driven analytics with real-time visualization, monitoring, and alerting of correlated security data. It is a valuable module that can be taken out and sold on its own as a different product. Historically, the GMS analytics reporting has been based on incoming and outgoing syslog traffic from the appliances to the server. However, the new module allows the GMS analytics reporting to also be based on flow traffic, as a different packet. The way to capture the traffic selection, of either flow or syslog, is done at the time of installation.

GMS provides monitoring features that enable you to view the current status of SonicWall appliances and non-SonicWall appliances, pending tasks, and log messages. It also provides graphical reporting of firewall, Secure Mobile Access (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, you can add VPN licenses to SonicWall appliances, configure VPN settings, and enable or disable remote-client access for each network.

Installing GMS

- Before You Begin
- Installing the GMS OVA File
- Setting Up the Network Configuration
- Configuring the System
- Setting the Install Mode
- Registering GMS
- Adding Devices

Before You Begin

Review these sections for information before installing your SonicWall GMS Virtual Appliance:

- [System Requirements](#)
- [Installation Quick Start](#)

System Requirements

The SonicWall GMS Virtual Appliance comes with a base license to manage either 5, 10, or 25 nodes. You can purchase additional licenses on MySonicWall. For more information on licensing additional nodes, visit: <https://www.sonicwall.com/en-us/support/contact-support/licensing-assistance>.

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>.

System Requirement	Minimum Requirements
SonicWall GMS Virtual Appliance	<ul style="list-style-type: none"> • ESXi 6.5 • A CPU greater than quad core level • 16 GB RAM (more is recommended for increased performance) • 40, 250 or 950 GB available disk space (depending on number of devices) • thick provisioning <p>NOTE: GMS is not supported as a VMware virtual machine running in a cloud service, such as Amazon Web Services EC2.</p>
Hard Drive	<ul style="list-style-type: none"> • Spindle Speed: 10,000 RPM or higher • Cache: 64 MB or higher • Transfer rate: 600 MBs or higher • Average Latency: 4 microseconds or lower
Browser	<ul style="list-style-type: none"> • Google Chrome 42.0 and higher (recommended browser for dashboard real-time graphics display) • Mozilla Firefox 37.0 and higher • Microsoft Edge 41 or higher • Microsoft Internet Explorer 10.0 and higher <p>NOTE: Internet Explorer version 10.0 in Metro interfaces of Windows 8 is currently not supported.</p> <p>NOTE: When using Internet Explorer, turn off Compatibility Mode when accessing the GMS management interface.</p> <p>NOTE: Internet Explorer is not supported for Angular-based flow reports.</p>
Network	<ul style="list-style-type: none"> • access to the Internet • either: <ul style="list-style-type: none"> • an IP address automatically assigned through DHCP • a static IP address
SonicWall Appliance and Firmware	<ul style="list-style-type: none"> • SonicOS 6.2 and higher

NOTE: SonicWall GMS provides monitoring support for non-SonicWall TCP/IP- and SNMP-enabled devices and applications. See the documentation that came with your device for more information.

Installation Quick Start

Installing GMS requires only these major steps:

1	2	3	4	5	6
Installing the GMS OVA File	Setting Up the Network Configuration	Configuring the System	Setting the Install Mode	Registering GMS (Console Only)	Adding Devices
Install the GMS virtual appliance on your system.	If needed, customize the configuration for GMS to operate in your network environment.	Use the easy-to-use wizard to configure GMS using the default settings.	Set the mode to be used by GMS to monitor your devices: Flow-based, Syslog-based, no reporting.	Register GMS using its serial number and your MySonicWall account.	Add the devices you want to monitor and maintain using GMS using either Basic or Advanced Mode.

Record Configuration Information

If you install GMS using a static IP address, record the following configuration information from your system for your reference before proceeding with your installation. You might not be prompted for this if you are installing using a DHCP-generated IP address.

Information Needed	Description	Your Configuration Information
SMTP Server Address	The Host IP or Name of your Simple Mail Transfer Protocol (SMTP) server. For example, mail.emailprovider.com.	
SMTP Server Password	The Password for your SMTP.	
HTTPS Web Server Port	The number of your secure (SSL) Web server port if customized. The default port is 443.	
GMS Administrator Email 1	The email address of a GMS administrator who receives email notifications from GMS.	
GMS Administrator Email 2	The email address of an additional GMS administrator who receives email notifications from GMS. This field is optional.	
Sender Email Address	The email address from which the email notifications are sent by GMS.	

Installing the GMS OVA File

Before installing the SonicWall Global Management System, please read [Before You Begin](#) for the system requirements and other useful information.

To install GMS

You can install GMS by deploying the OVA file to your VMware ESXi server. Each OVA file contains the software components needed. Deploy the OVA file by using the vSphere or vCenter client, which are available with ESXi.

NOTE: VMware ESXi elements must already be in place and the administrator must be familiar with the basics of deploying a virtual appliance on the ESXi server.

TIP: [Step 15](#) has some important information about selecting your networks. Even if you do not need all these step-by-step instructions, be sure to follow the instructions in [Step 15](#) to avoid connectivity issues after the deployment.

To perform a fresh install of GMS on VMware ESXi:

- 1 Download the GMS OVA file from MySonicWall to a computer with vSphere / vCenter access.
- 2 Access vSphere or vCenter and log into your ESXi server.
- 3 Navigate to the location where you want to install the virtual machine, and select the folder.
- 4 To begin the import process, click **Actions** and select **Deploy OVF Template**.
- 5 In the **Select an OVF template** screen, select **Local file**:
 - **Local file** – Click **Choose Files** and navigate to the GMS OVA file that you previously downloaded from the provided beta link.

Deploy OVF Template

1 Select an OVF template

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

☐ URL

☒ Local file

No file chosen

- 6 Click **Next**.
- 7 In the **Select a name and folder** screen, type a descriptive name for the GMS appliance into the **Virtual machine name** field and select a location for the virtual machine.
- 8 Click **Next**.

Deploy OVF Template

✓ 1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select a name and folder

Specify a unique name and target location

Virtual machine name:

Select a location for the virtual machine.

▼ vcenter6-pr.svus.sonicwall.com

▼ San Jose

▼ DEV

> CAS

> CFS

> DPISSL

> **GMS**

> HGMS

> SJ-Automation

> SMA

> SonicOS-MH

> Engineering Services

> QA

> Shanghai

CANCEL

BACK

NEXT

- 9 In the **Select a computer resource** screen, click **Next** to accept the default resource for the selected folder, or select a different resource and then click **Next**. Wait while the resource is validated. This is the resource pool where you want to deploy the template.

Deploy OVF Template

✓ 1 Select an OVF template

✓ 2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select a compute resource

Select the destination compute resource for this operation

▼ GMS

> GMS-Cluster-1

▼ GMS-Dev

esx-mil148-dev16-dm.eng.sonicwall.com

gms-esx-04.eng.sonicwall.com

> Cloud GMS 2.0 (8.4) Dev Ref .199

> GMS 8.7 Deployments

> GMS 9.0 Deployments

> GMS 9.1 Deployments

GMS 9.2 Deployments

> GMS/Analyzer 8.5 Deployments

> GMS/Analyzer 8.6 Deployments

> GMS-DEV-2

> esx-sjc-11.eng.sonicwall.com

> gms-esx-01.eng.sonicwall.com

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

SonicWall Global Management System 9.2 Getting Started Guide
Installing the GMS OVA File

11

10 In the **Review details** screen, verify the template details and then click **Next**.

The screenshot shows the 'Deploy OVF Template' window with the 'Review details' step selected in the left sidebar. The main area displays a table with template details and navigation buttons at the bottom.

Review details	
Verify the template details.	
Publisher	No certificate present
Download size	733.7 MB
Size on disk	1.6 GB (thin provisioned)
	40.0 GB (thick provisioned)

CANCEL BACK NEXT

11 In the **License agreements** screen, read the terms for the **SonicWall End User Product Agreement**, click the checkbox next to **I accept all license agreements** and then click **Next**.

The screenshot shows the 'Deploy OVF Template' window with the 'License agreements' step selected in the left sidebar. The main area displays the license agreement text and a checkbox for acceptance.

License agreements

The end-user license agreement must be accepted.

Read and accept the terms for the license agreement.

SonicWall End User Product Agreement

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

This SonicWall End User Product Agreement (the "Agreement") is made between

☒ I accept all license agreements.

CANCEL BACK NEXT

- 12 In the **Select storage** screen, first select a datastore from the table. This is the location where you want to store the virtual machine files.

Deploy OVF Template

✓ 1 Select an OVF template
 ✓ 2 Select a name and folder
 ✓ 3 Select a compute resource
 ✓ 4 Review details
 ✓ 5 License agreements
6 Select storage
 7 Select networks
 8 Ready to complete

Select storage
 Select the storage for the configuration and disk files

☐ Encrypt this virtual machine (No encryption policies available)

Select virtual disk format: **Thick Provision Lazy Zeroed** ▼

VM Storage Policy: ⚠

☒ Disable Storage DRS for this virtual machine

Name	Capacity	Provisioned	Free	Type
DatastoreCluster	5 TB	4.95 TB	54.01 GB	
ESX-MIL148-DEV16-DM-...	923.5 GB	976 MB	922.55 GB	VM
GMS-EQL-01-LUN-2	5 TB	7.28 TB	267.8 GB	VM
GMS-EQL-01-LUN-4	10 TB	17.09 TB	246.96 GB	VM
GMS-EQL-01-LUN-5	10 TB	14.41 TB	1.5 TB	VM
GMS-ESX-04-RAID1-Local1	1.08 TB	2.88 TB	79.56 GB	VM
HGMS-EQL-01-LUN-1	10 TB	16.49 TB	1.11 TB	VM

Compatibility
 ✓ Compatibility checks succeeded.

CANCEL BACK **NEXT**

- 13 In the same screen, select the type of provisioning for the GMS virtual appliance disk from the **Select virtual disk format** drop-down list. SonicWall recommends **Thick Provision**, but any selection works.

- 14 Click **Next**.

GMS 9.2 VM contains only one interface.

NOTE: The GMS configuration should have the option for **MAC address changes** enabled for the vswitch ports connected.

Typically, GMS is deployed between your internal network and a network with internet access. Therefore you map the source **X0** to your LAN network (vswitch port), and map the source **X1** to the WAN network (vswitch port) with connectivity to the internet.

IMPORTANT: **SONICOS_X1** (the default WAN Interface) is set to **DHCP** by default, with **HTTPS management** enabled for GMS, as this configuration eases deployments in virtual/cloud environments.

NOTE: System defaults for the X1 interface:

- X1 – Default WAN – DHCP addressing, with HTTPS and Ping management enabled

NOTE: Configuration settings import from physical firewalls to GMS is not supported.

15 In the **Select networks** screen, choose a destination network for each source network by choosing it from the drop-down menu next to **VM Network**.

Deploy OVF Template

✓ 1 Select an OVF template

✓ 2 Select a name and folder

✓ 3 Select a compute resource

✓ 4 Review details

✓ 5 License agreements

✓ 6 Select storage

7 Select networks

8 Ready to complete

Select networks

Select a destination network for each source network.

Source Network	Destination Network
VM Network	X0
	10.206.23.X
	X0
	X6
	X4
	X3
	X2
	X7
	X5
	vFW-Network

IP Allocation Settings

IP allocation: Stat

IP protocol: IPv4

CANCEL

BACK

NEXT

16 Click **Next**.

- 17 In the **Ready to complete** screen, review the settings and click **Finish** to create the GMS virtual appliance. To change a settings, click **Back** to navigate back through the screens to make a change.

Deploy OVF Template

✓ 1 Select an OVF template

✓ 2 Select a name and folder

✓ 3 Select a compute resource

✓ 4 Review details

✓ 5 License agreements

✓ 6 Select storage

✓ 7 Select networks

8 Ready to complete

Click Finish to start creation.

Provisioning type	Deploy from template
Name	gms92-installation
Template name	sw_gmsvp_vm_eng_9.2.9205.1295.40GB.64bit-pg
Download size	733.7 MB
Size on disk	1.6 GB
Folder	GMS
Resource	GMS 9.2 Deployments
Location	GMS-EQL-01-LUN-5
Storage mapping	1
All disks	Datastore: GMS-EQL-01-LUN-5; Format: Thin Provision
Network mapping	1
VM Network	10.206.23.X
IP allocation settings	
IP protocol	IPv4
IP allocation	Static - Manual

CANCEL

BACK

FINISH

The name of the new GMS virtual appliance appears in the left pane of the vSphere or vCenter window when complete.

The next step is to power on your GMS virtual appliance in the vSphere or vCenter interface.

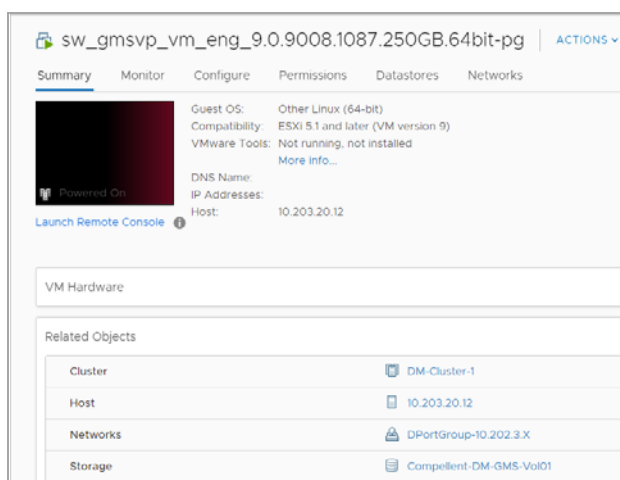
Once your GMS virtual firewall is powered on, the next step is to register it on MySonicWall.

Setting Up the Network Configuration

After installing GMS, you need to configure its network settings.

To set up the network configuration for GMS:

- 1 Launch the remote console.

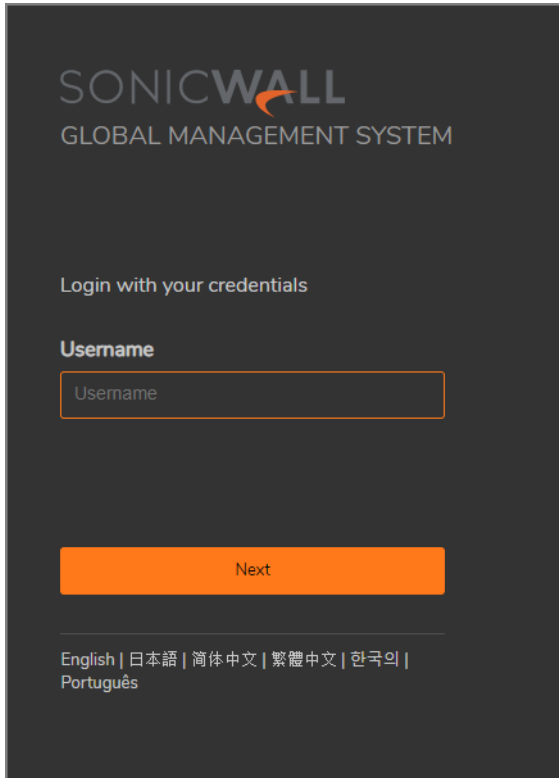


- 2 If your network configuration has a DHCP server, an IP address is automatically assigned to the virtual machine



NOTE: If a DHCP server is not present, you need to use the command-line interface to manually assign an IP address to the virtual machine.

- 3 Open a web browser and enter the IP address of the GMS installation in this format: `https://<IP address>`.
- 4 Log in the GMS console using the default administration account:
 - Username: `admin`
 - Password: `password`



The image shows the login interface of the SonicWall Global Management System. It features a dark gray background with the SonicWall logo and the text 'GLOBAL MANAGEMENT SYSTEM' at the top. Below this, the instruction 'Login with your credentials' is displayed. A 'Username' label is positioned above a text input field that contains the placeholder text 'Username'. An orange 'Next' button is located below the input field. At the bottom, a horizontal line separates the login fields from a list of language options: English | 日本語 | 简体中文 | 繁體中文 | 한국의 | Português.

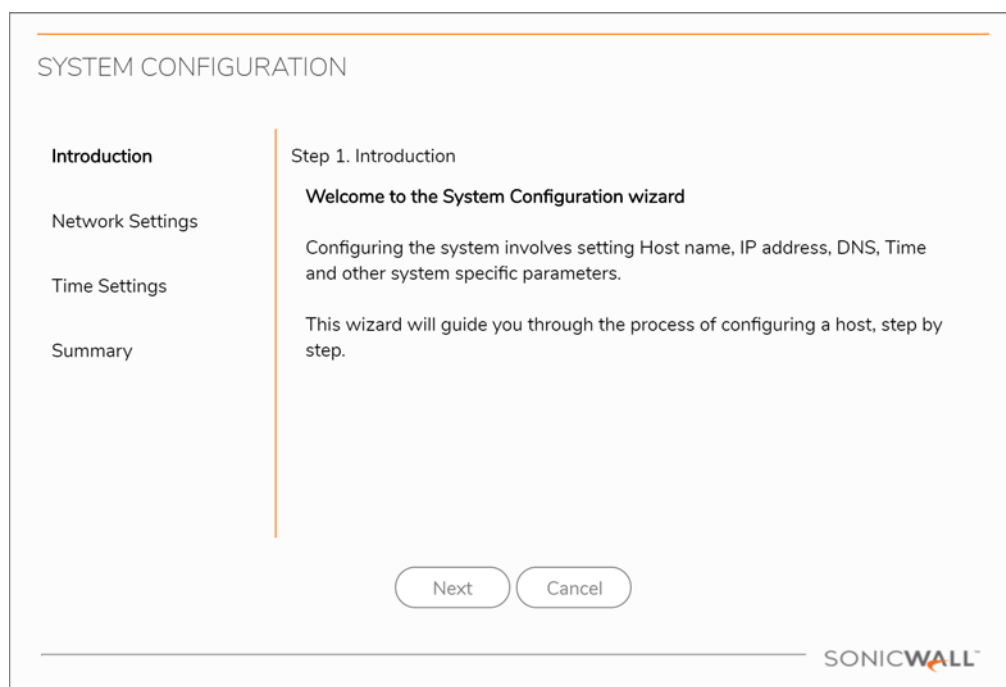
Configuring the System

This section guides you through the configuration of the IP address, gateway address, preferred time setting, and the domain for your GMS installation.

To configure the GMS system:

- 1 If you are not already logged in to GMS, log in using the default administration account.

The first page of the System Configuration tool displays.



- 2 Click **Next** to proceed with the configuration.
- 3 When configuring with DHCP, you can update the values for the host Name, Domain, and the DNS servers to those required for your network environment. The Host IP address/Subnet mask and the Default

gateway are automatically populated by the DHCP server. You can opt to select the “Static” radio button to configure a static Host IP address / Subnet mask and the Default gateway address. Click **Next**.

SYSTEM CONFIGURATION

Introduction

Network Settings

Time Settings

Summary

Step 2. Network Settings

Select IP type: ☒ DHCP ☐ Static

▼ IPv4 Network Settings

Name e.g.: hostname

Domain e.g.: domain.com

Host IP address/ Subnet mask /

Default gateway

DNS server 1

DNS server 2

SONICWALL™

NOTE: By default, the **Select IP type** is **DHCP**. The **Host IP address/ Subnet mask** is automatically assigned. The customer does not need to configure the **Host IP address/ Subnet Mask** and **Default gateway**. The fields appear grayed out. If the customer switches to **Static**, the fields are enabled.

- If necessary, update the **Time**, **Date**, and **TimeZone** for your GMS installation and click **Next**. By default the time zone is **UTC**.

SYSTEM CONFIGURATION

Introduction

Network Settings

Time Settings

Summary

Step 3. Time Settings

Time (hh:mm:ss) 21 : 20 : 09

Date July 09 2019

TimeZone (UTC) Coordinated Universal Time

☒ Set time automatically using NTP

To continue, click Next.

Back

Next

Cancel

SONICWALL™

- 5 Verify the settings your system provides. If you need to change any of the configuration settings that you entered on previous pages, click **Back**.

SYSTEM CONFIGURATION

Introduction

Network Settings

Time Settings

Summary

Step 4. Summary

Network Settings

Hostname gms

Domain example.com

IP address 10.206.23.115

Default gateway 10.206.23.1

Subnet mask 255.255.255.0

DNS server 1 10.50.129.148

DNS server 2 10.50.129.149

Time Settings

Time

TimeZone (GMT-08:00) Pacific Time (US & Canada); Tijuana

Click "Apply" and proceed to complete the setup process.

Back

Apply

Cancel

SONICWALL™

- If no changes are required, click **Cancel** to continue with setting up GMS without restarting the virtual machine.
- If you need to change any settings from their default values, click **Apply** to accept your configuration settings. If you need to change any of the configuration settings that you entered on previous pages, click **Back**.

SonicWall Global Management System 9.2 Getting Started Guide
Configuring the System

20

The virtual machine reboots after you apply your configuration settings. If it does, you need to enter your username and password again to continue.

NOTE: If the DHCP server has been configured correctly, the values for the DNS-related fields are filled in automatically.

Performing Basic Tasks and Manual Host Configuration

This section describes how to manually power on and configure basic settings on the GMS Virtual Appliance, including virtual hardware settings and networking settings when no DHCP server is available.

The following tasks are required to configure your GMS Virtual Appliance before registering it:

- 1 [Power the Virtual Appliance On](#) on page 21
- 2 [Configure Host Settings on the Console](#) on page 22
- 3 [Configure Host Settings on the Appliance Management Interface](#) on page 23

This chapter also contains information on:

- [Viewing the Settings Summary](#) on page 24
- [Editing The Virtual Machine Settings](#) on page 25

Power the Virtual Appliance On

There are multiple ways to power the GMS Virtual Appliance on (or off).

To power the virtual appliance on (or off), complete one of the following steps:

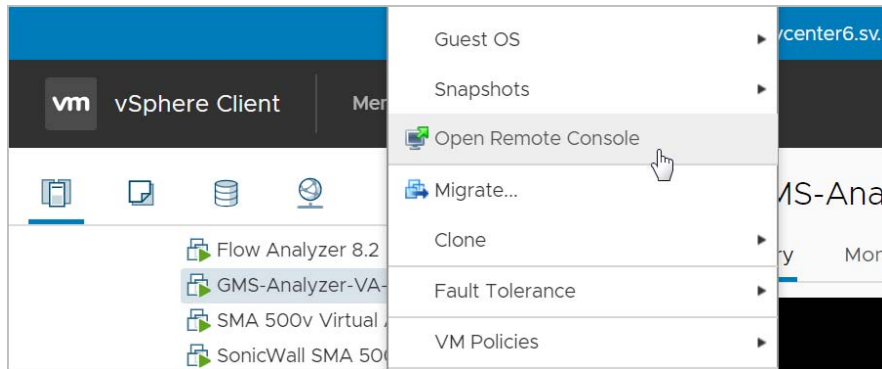
- Right-click the SGMS Virtual Appliance in the left pane and navigate to **Power > Power On** (or **Power > Power Off**) in the right-click menu.
- Select the GMS Virtual Appliance in the left pane and then click **Power on the virtual machine** (or **Shut down the virtual machine**) on the Getting Started tab in the right pane.
- Select the GMS Virtual Appliance in the left pane and then click **Power On** (or **Shut down guest**) on the Summary tab in the right pane.

Configure Host Settings on the Console

NOTE: This feature is only applicable when a DHCP Server is not available to grant an IP address to the deployed virtual machine, or when you wish to configure a Static IP.

After powering on the GMS Virtual Appliance, complete the following steps to open the console and configure the IP address and default route settings:

- 1 In vSphere, right-click the GMS Virtual Appliance in the left pane.



- 2 Select **Open Remote Console** in the right-click menu.
- 3 When the console window opens, click inside the window, type `snwcli` at the **login:** prompt.
- 4 Press **Enter**. Your mouse pointer disappears when you click in the console window. To release it, press **Ctrl+Alt**.
- 5 The console might display warning messages that can be ignored, and then displays a second **Login:** prompt. Type `admin` at the **Login:** prompt.
- 6 Press **Enter**.
- 7 Enter `password` at the **Password:** prompt.
- 8 Press **Enter**. The `SNWLCLI>` prompt is displayed.
- 9 Configure the local IP address for the virtual appliance by entering the following command, substituting your IP address and subnet mask for the values shown here:

```
interface eth0 10.208.112.175 255.255.255.0
```

You can also configure IPv6 address at this step by using the interface command. Or, use the /appliance (System) interface **Network > Settings** screen to do the IPv6 configuration.

- 10 Configure the default route for the virtual appliance by typing the following command, substituting your gateway IP address for the value shown here:

```
route --add default --destination 10.208.112.1
```

You can test connectivity by pinging another server or your main gateway, for example:

```
ping 10.208.111.1
```

```
ping 10.0.0.1
```

Press **Ctrl+c** to stop pinging.

- 11 Enter `exit` to exit the CLI.
- 12 Close the console window by clicking the **X**.

Configure Host Settings on the Appliance Management Interface

After configuring the IP address and default route settings on the GMS Virtual Appliance console, the next steps are to configure the host name, network, and time settings in the appliance management interface.

The **Host Configuration Tool** is a wizard that takes you through several basic steps to get your GMS Virtual Appliance configured for your network.

NOTE: This wizard can be skipped if no changes are required or when an IP has already been dynamically assigned.

The wizard starts automatically after you log in for the first time. You can cancel the wizard at this time, which leaves the default configuration on the virtual appliance and prevents the wizard from automatically starting again.

NOTE: If you log out of the appliance management interface without actually cancelling the wizard, it starts automatically on your next login.

You can manually start the wizard at any time by clicking **Wizards** at the top-right corner of the page.

To complete host configuration for the virtual appliance, complete the following steps:

- 1 Launch a browser and enter the URL of the virtual appliance, such as:
`https://10.208.112.175`
- 2 On the appliance interface login page, enter the default credentials:
User—*admin*
Password—*password*
- 3 Click **Submit** to log in.
- 4 The login page re-displays with the default login credentials pre-populated.
- 5 Click **Submit**.
- 6 The **Host Configuration Tool** wizard starts automatically. In the **Introduction** screen, click **Next**.
- 7 In the **Network Settings** screen, configure the following network settings for the GMS Virtual Appliance.
 - **Name** – A descriptive name for this virtual appliance
 - **Domain** – In the form of “sonicwall.com”; this domain is not used for authentication
 - **Host IP Address** – The static IP address for the eth0 interface of the virtual appliance
 - **Subnet Mask** – In the form of 255.255.255.0
 - **Default Gateway** – The IP address of the network gateway – this is the default gateway and is required for networking purposes.
 - **DNS Server 1** – The IP address of the primary DNS server
 - **DNS Server 2 (Optional)** – The IP address of the secondary DNS server
- 8 Click **Next**:
- 9 In the **Time Settings** screen, select values for the following system settings on the virtual appliance:
 - **Time (hh:mm:ss)** – Hours, minutes, and seconds of current time; this field is disabled if the NTP option is selected
 - **Date** – Month, day, and year of current date; this field is disabled if the NTP option is selected

- **TimeZone** – Select from the drop-down list
- **Set time automatically using NTP** – Select this checkbox to use an NTP server to set the virtual appliance time; a default NTP server is pre-configured

10 Click **Next**:

11 In the **Summary** screen, verify the settings.

12 Click **Back** to make changes on a previous screen, or click **Apply** to accept the settings.

A dialog warns you that the virtual appliance is rebooting.

13 Click **OK**.

14 Wait for the settings to be applied, possibly for a few minutes. The screen displays a progress bar until it finishes, and then displays the status.

i **NOTE:** If you modified the DNS settings, the services on the appliance restart when changes are applied, causing a momentary connectivity loss to the Web server. Your browser is redirected to the appliance management interface login page.
If you modified the Time settings, the virtual appliance reboots. Use your browser to reconnect to the appliance management interface.

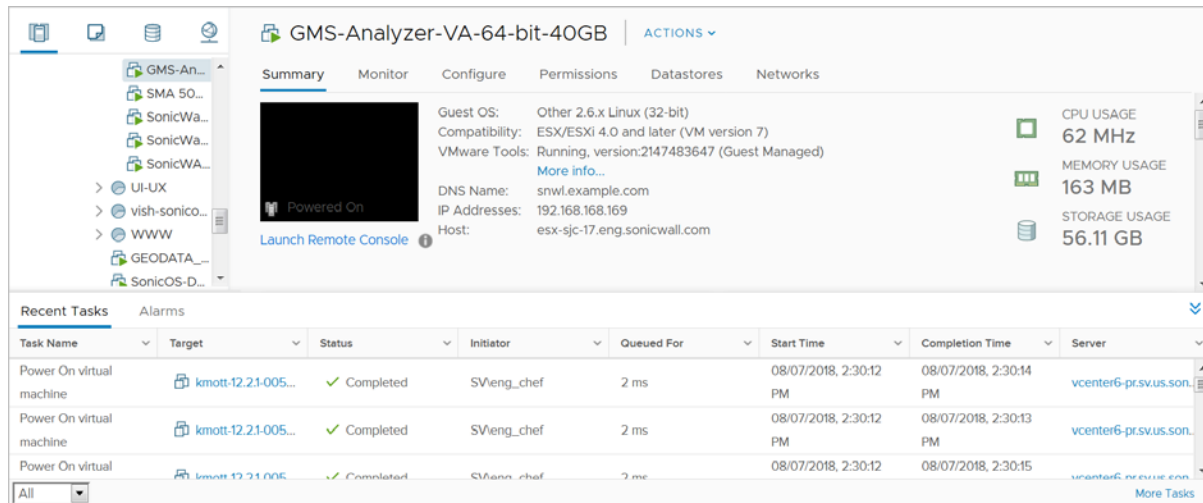
Viewing the Settings Summary

When the GMS Virtual Appliance is selected in the left pane, the **Summary** tab of the vSphere interface displays pertinent information such as memory, powered on/off state, hard disk storage usage, network subnet settings, and other settings.

i **NOTE:** This page might incorrectly indicate that VMware Tools are not installed.

A short list of commands are also provided on this page, including **Power On** and **Edit Settings**.

When using vSphere with vCenter Server, the **Migrate** and **Clone** commands are also available in the **Actions** drop-down.

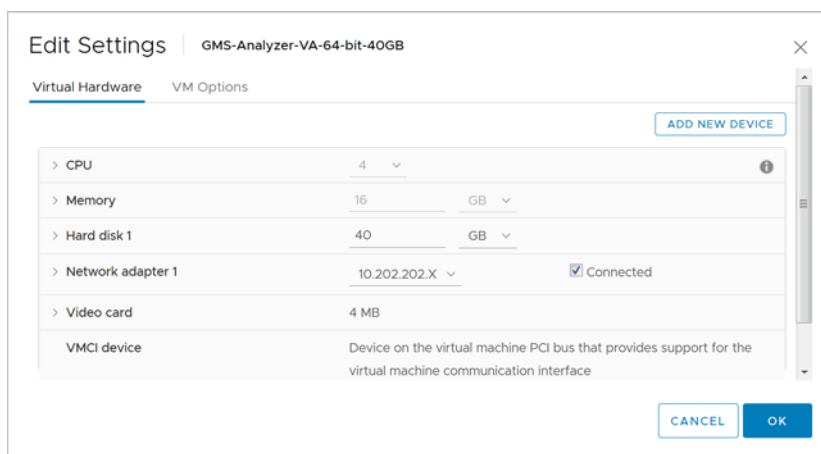


Editing The Virtual Machine Settings

You can use the vSphere client to edit settings for the GMS Virtual Appliance, including memory, CPUs, descriptive name, datastore, and resource allocation.

To edit virtual machine settings:

- 1 In the vSphere client, right-click the GMS Virtual Appliance in the left navigation pane and select **Edit Settings**.



- 2 In the **Virtual Hardware** window, see the settings for CPU, memory, hard disk, and other hardware. Click the row in the table to access the editable settings in the right pane.
- 3 Click the **VM Options** tab to view and edit the GMS Virtual Appliance name, location (datastore), guest power management (for standby), and other settings.
- 4 When finished, click **OK**.

Setting the Install Mode

The Install Mode wizard allows you to configure between a Single Server deployment and a Distributed deployment.

You must decide the type of deployment your application is going to make before the installation procedure begins. You should know whether this deployment is going to be for a single server (all-in-one) or a multi-server (with consoles and agents) deployment. The steps that follow show the Wizard sequence and where each screen leads.

If your installation mode is for a single server (all-in-one), it cannot expand. Due to a paradigm shift in 9.2, you cannot expand in this installation mode. Based on your selection, some of the steps jump. For example, if you choose the single-server installation mode, it directly jumps to the reporting module.

GMS is made for two modules: reporting and management. You can choose either flow-based reporting or syslog-based reporting or no reporting with just management.

Decide which of the two installation options best match your requirements.

Topics:

- [Single Server Deployment](#) on page 26
- [Distributed Deployment](#) on page 30

Single Server Deployment

To set the Install mode for a Single Server deployment:

- 1 If you are not already logged into GMS, log in using the default administration account.
The first page of the Install Mode Selection Tool displays.

INSTALL MODE SELECTION

Introduction

Install mode

Distributed mode

Database

Role configuration

Reporting type

Summary

Step 1. Introduction

Welcome to the Install Mode Selection tool

In order to use the application installed on this system, it is necessary to select the install mode for this appliance. Mode selection is an important step in the setup operation. Choosing the mode allows role configuration to be completed either automatically with default settings or manually with custom configuration. This wizard will guide you through the process of selecting an installation mode, step by step.

Next

Cancel

SONICWALL™

- Click **Next**. The **Install mode** page of the Install Mode Selection Tool displays.

INSTALL MODE SELECTION

Introduction

Install mode

Distributed mode

Database

Role configuration

Reporting type

Summary

Step 2. Install mode

Please choose the type of install this is.

☒ **Is this a Single Server deployment?**

This mode will automatically choose the AIO (All In One)/Default install mode. In this express install operation, no inputs are required from the user. It is configured as a standalone single server "All In One" appliance.

☐ **Is this installation part of a distributed deployment?**

This mode will allow the user to choose the role for this server in this deployment. The installation will then continue as a Custom install.

Back

Next

Cancel

SONICWALL™

SonicWall Global Management System 9.2 Getting Started Guide
Setting the Install Mode

27

- 3 If you are installing for a single server deployment, choose **Is this a Single Server deployment?** and click **Next**.

Installation roles (in the configuration files) also vary for these installation modes. These apply to the Primary server in the deployment.

i NOTE: Once you select a single-server deployment, that is the only instance you have. You cannot add more deployments in this mode. To add more, you need to choose the distributed deployment mode by clicking the second radio button.

- 4 Select the **Reporting type** you want to use for this deployment.
 - **Flow based** - this mode includes management plus flow-based (IPFIX) reporting and analytics
 - **Syslog based** - this mode includes management plus syslog-based reporting
 - **None** - this mode provides management only of the GMS with no reporting
- 5 Click **Next**. The **Summary** page of the Install Mode Selection tool displays.

INSTALL MODE SELECTION

Introduction

Install mode

Distributed mode

Database

Role configuration

Reporting type

Summary

Step 7. Summary

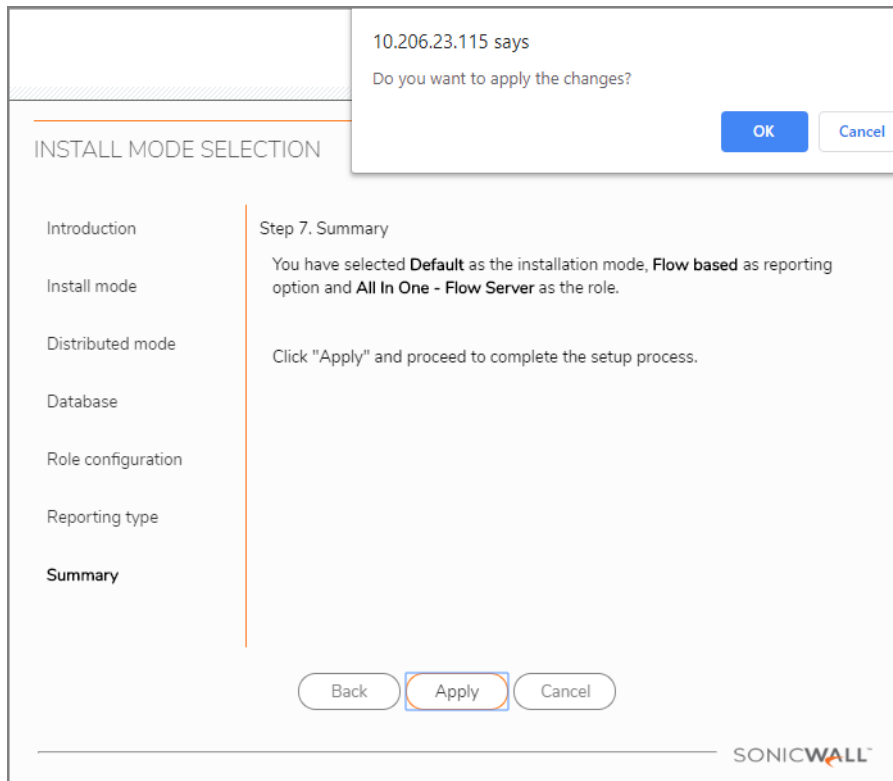
You have selected **Default** as the installation mode, **Flow based** as reporting option and **All In One - Flow Server** as the role.

Click "Apply" and proceed to complete the setup process.

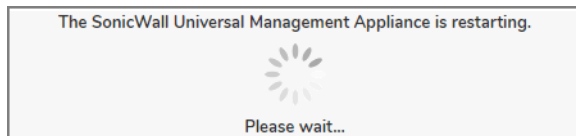
Back Apply Cancel

SONICWALL

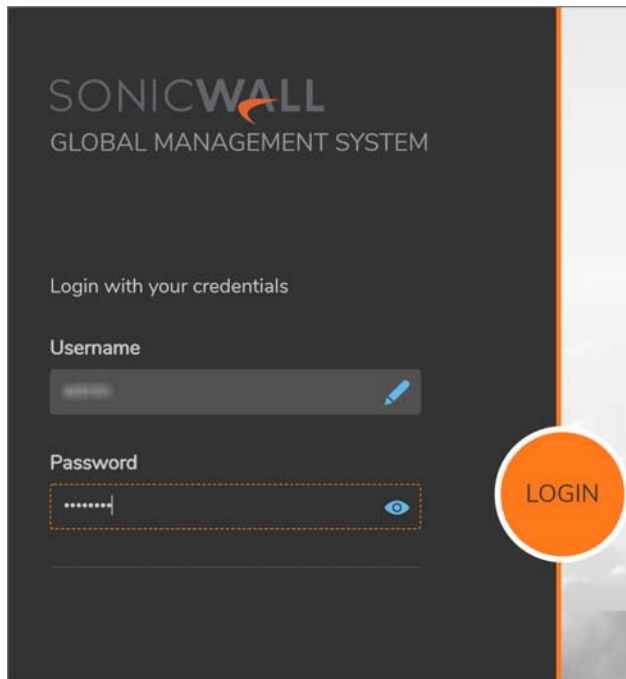
- Click **Apply**. A small popup window displays at the top asking, **Do you want to apply the changes?** Click **OK**.



- Click **Apply** again..
NOTE: The configuration of the GMS may take up to 15 minutes to complete.
- Click **OK**. The system reboots to complete the installation process.



- Log into GMS again using the default administration account.



Distributed Deployment

GMS 9.2 supports Ease of Installation for a distributed setup. GMS simplifies the installation process even when multiple servers (instances) are required for a larger deployment. The selection screen for this type of deployment is applicable to Distributed Mode only. After you have chosen a distributed installation during the Install Mode process, these options appear.

In any Distributed deployment, you must deploy a console first. The console has to be deployed as the first instance of the virtual machine. The rest is agent and you need the Console ID and the Console Administrator's password to pair it properly.

To set the Install mode for a Distributed deployment:

- 1 If you are not already logged into GMS, log in using the default administration account.

The first page of the Install Mode Selection tool displays.

INSTALL MODE SELECTION

Introduction

Install mode

Distributed mode

Database

Role configuration

Reporting type

Summary

Step 1. Introduction

Welcome to the Install Mode Selection tool

In order to use the application installed on this system, it is necessary to select the install mode for this appliance. Mode selection is an important step in the setup operation. Choosing the mode allows role configuration to be completed either automatically with default settings or manually with custom configuration. This wizard will guide you through the process of selecting an installation mode, step by step.

Next

Cancel

SONICWALL™

- 2 Click **Next**. The **Install mode** page of the Install Mode Selection Tool displays.

INSTALL MODE SELECTION

Introduction

Install mode

Distributed mode

Database

Role configuration

Reporting type

Summary

Step 2. Install mode

Please choose the type of install this is.

☐ Is this a Single Server deployment?

This mode will automatically choose the AIO (All In One)/Default install mode. In this express install operation, no inputs are required from the user. It is configured as a standalone single server "All In One" appliance.

☒ Is this installation part of a distributed deployment?

This mode will allow the user to choose the role for this server in this deployment. The installation will then continue as a Custom install.

Back Next Cancel

SONICWALL™

- 3 When you are installing for multiple servers as a distributed deployment, choose **Is this installation part of a distributed deployment?** and click **Next**.
- 4 Choose the type of Installation, a **Console** or an **Agent**.

INSTALL MODE SELECTION

Introduction

Install mode

Distributed mode

Database

Role configuration

Reporting type

Summary

Step 3. Distributed mode

Please choose the type of install.

☐ Is this a Console?

The Console role is used in a multi-server GMS deployment. In this role, the server is configured to run all GMS Services.

☒ Is this an Agent?

Please provide the location of the Primary Console and the password to use to authenticate the connection. Primary Console is the host that will provide Database, License and other information to configure this agent.

Host IP or Name: 10.206.23.172

Password:

Back Next Cancel

SONICWALL™

Console Installation

- 1 The Primary server's installation is as a **Console**. The Database should also be configured here. Either the embedded **MYSQL** can be used locally, or a remote **SQL SERVER** can also be connected. The database configuration page appears in the next step, which is available only for this selected mode. This is the screen for a **MYSQL** database type. The data fields are auto-populated.

MySQL Database

Introduction

Install mode

Distributed mode

Database

Role configuration

Reporting type

Summary

Step 4. Database

Enter the database parameters for the selected role: Console

Database Type:

MYSQL

Database Host:

MYSQL

Database Port:

SQL SERVER

Database User:

Database Password:

.....

Confirm Database Password:

.....

Database Driver:

org.mariadb.jdbc.Driver

Database URL:

jdbc:mysql://localhost:3306

Back

Next

Cancel

SONICWALL™

SQL Server Database

INSTALL MODE SELECTION

Introduction

Install mode

Distributed mode

Database

Role configuration

Reporting type

Summary

Step 4. Database

Enter the database parameters for the selected role: Console

Database Type: SQL SERVER

Database Host:

Database Port: 1433

Database User:

Database Password:

Confirm Database Password:

Database Driver: com.microsoft.sqlserver.jdbc.SQLServerDriver

Database URL: jdbc:sqlserver://:1433

Back Next Cancel

SONICWALL

- 2 Select the **Database Type**: SQL SERVER.
- 3 Enter the **Database Host** name or IP address.
- 4 Enter the **Database Port**. The default is 1433.
- 5 Select the **Database User**.
- 6 Enter the **Database Password**.
- 7 Confirm the **Database Password**.
- 8 The **Database Driver** and **Database URL** should fill automatically.
- 9 Click **Next**. Missing information returns an error message.

INSTALL MODE SELECTION

Introduction

Install mode

Distributed mode

Database

Role configuration

Reporting type

Summary

Step 4. Database

Enter the database parameters for the selected role: Console

Database Type:

SQL SERVER

Database Host:

Database Port:

1433

Database User:

Database Password:

.....

Confirm Database Password:

.....

Database Driver:

com.microsoft.sqlserver.jdbc.SQLServerDriver

Database URL:

jdbc:sqlserver://10.206.23.86:1433

Back

Next

Cancel

SONICWALL™

10 Select the **Reporting type** you want to use for this GMS.

INSTALL MODE SELECTION

Introduction

Install mode

Distributed mode

Database

Role configuration

Reporting type

Summary

Step 6. Reporting type

Please select a report type that will be used in report generation for units added to the system.

☒ **Flow based**

Reports are generated using IPFIX packets for units that have reporting licensed and enabled. The Analytics feature will be available with this selection.

☐ **Syslog based**

Reports are generated using Syslog packets for units that have reporting enabled. Live Monitor feature will be available with this selection.

☐ **None**

Management only mode, Reports are disabled.

Back

Next

Cancel

SONICWALL™

- **Flow based** - this mode includes management plus flow-based (IPFIX) reporting and analytics
- **Syslog based** - this mode includes management plus syslog-based reporting
- **None** - this mode provides management only of the GMS with no reporting

11 Click **Next**. The **Summary** page of the Install Mode Selection Tool displays.

INSTALL MODE SELECTION

Introduction

Install mode

Distributed mode

Database

Role configuration

Reporting type

Summary

Step 7. Summary

Following is a summary of the distributed environment settings:

Install mode

Install mode: Custom

Report type: Flow based

Role: Console

Database

Database type: MS_DB

Database Host: [redacted]

Database Port: 1433

Database User: [redacted]

Database Password: [redacted]

Click "Apply" and proceed to complete the setup process.

Back Apply Cancel

SONICWALL

12 Click **Apply**.

For Console registration information, see [Registering GMS](#).

Agent Installation

Use this option for other servers in the deployment, such as a redundant console, agents, flow agents, and so on.

The agent installation queries the web services module to gather all the information needed to complete this server's installation without requiring any further input from you. This also includes all licensing information for the agent to function.

INSTALL MODE SELECTION

Introduction

Install mode

Distributed mode

Database

Role configuration

Reporting type

Summary

Step 3. Distributed mode

Please choose the type of install.

☐ Is this a Console?

The Console role is used in a multi-server GMS deployment. In this role, the server is configured to run all GMS Services.

☒ Is this an Agent?

Please provide the location of the Primary Console and the password to use to authenticate the connection. Primary Console is the host that will provide Database, License and other information to configure this agent.

Host IP or Name:

Password:

Back Next Cancel

SONICWALL

The wizard requests you enter the Host IP/Name of the server that is already setup as a Primary Console. The host being installed then contacts the Primary Console at the specified address to capture additional information to complete the setup. You do not have to re-enter these settings. GMS automatically figures out the details by contacting the Primary Console. See the Web Services interface for additional details.

The database configuration, reporting mode configuration, and the licensing information are collected from the primary server and used during the next steps of the installation. The collection of this information from the primary server happens after the **Next** button is clicked. See [Easy Licensing](#) for more information.

A valid **Host IP address or Name** and **Password** must be specified. In the event of a failure, an error message displays.

Role Configuration

This screen only applies to Agent Installation after you have chosen the distributed installation in the previous step selecting Agent only. A list of the applicable roles for a distributed setup appears. For Flow-based deployments the following roles are available.

INSTALL MODE SELECTION

Introduction

Install mode

Distributed mode

Database

Role configuration

Reporting type

Summary

Step 5. Role configuration

Select one of the following role(s):

☐ Console (Redundant)

Details

☐ Agent

Details

☐ Reports Summarizer

Details

☐ Monitor

Details

☐ Event Manager

Details

☐ Syslog Collector

Details

☐ ZeroTouch Agent

Details

To continue, click Next.

Back

Next

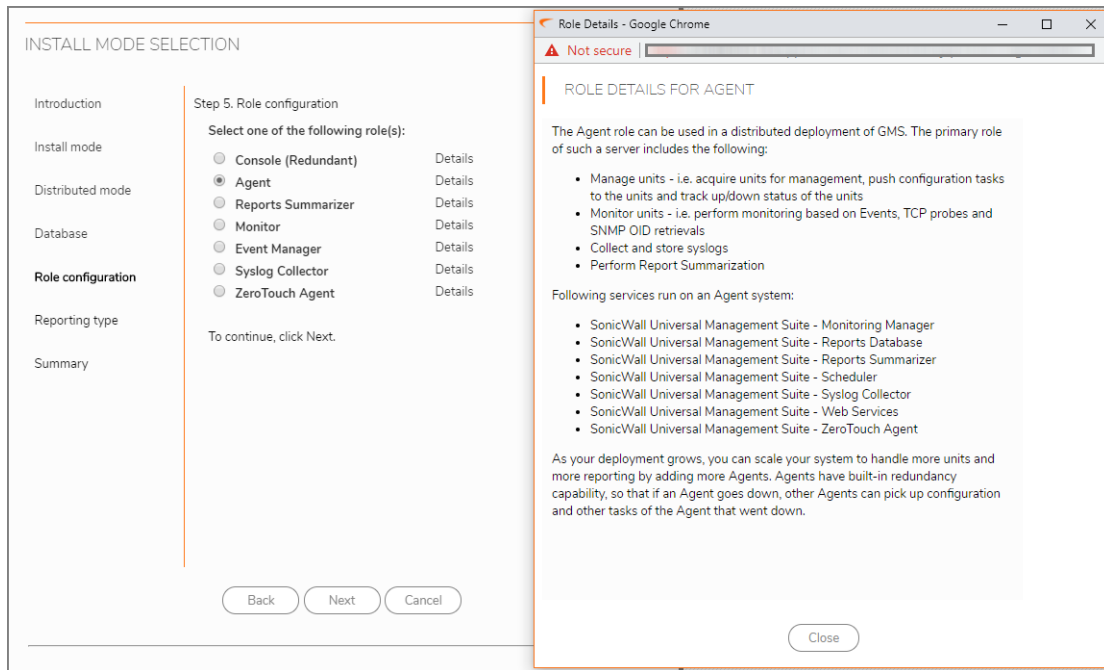
Cancel

SONICWALL™

NOTE: The All-In-One option does not appear as a role in this step.

Click **Details** to see additional content per selection.

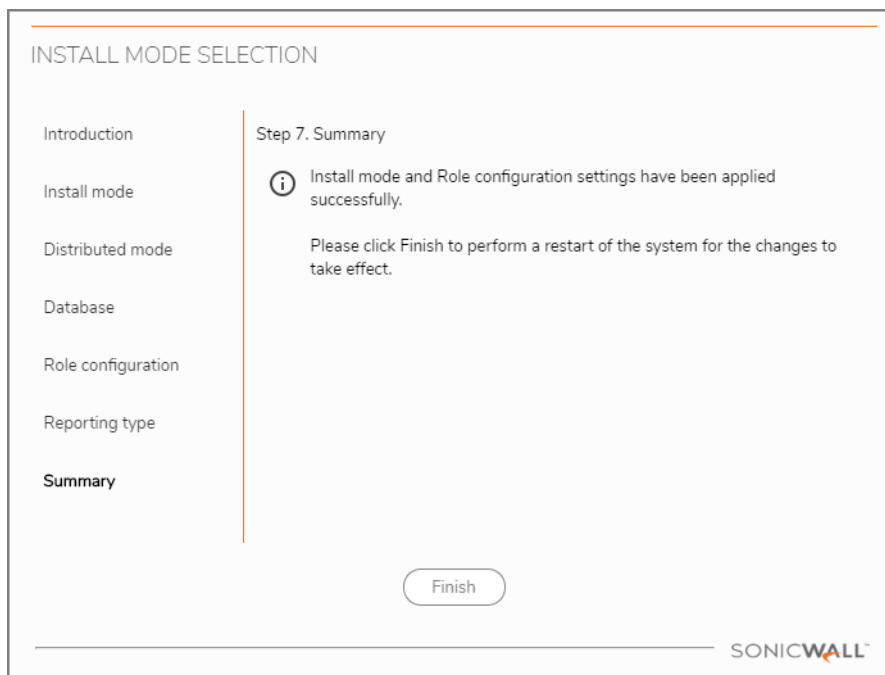
- 1 Select the desired role for this Agent instance.
- 2 Click **Next**.



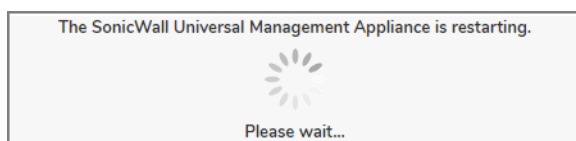
3 Click **Apply**. A status bar displays.

NOTE: The configuration of GMS could take up to 15 minutes to complete.

4 After Install mode and the Role Configuration settings are completed, click **Finish**.



5 The system reboots to complete the installation process.



6 Log into GMS again using the default administration account.

You have completed the configuration of the reporting mode. Next, you need to configure GMS. See [Configuring the System](#) for more information.

Easy Licensing

GMS is designed for Ease of Use, manual registration of one or more distributed instances is not necessary when the Primary server is already registered to a specific account.

The application automatically registers all distributed instances using the same serial numbers and MySonicWall accounts that were used to register the primary server during deployment.

Registering GMS

Registration for GMS agents is handled by the [Easy Licensing](#) feature introduced in GMS 9.2, and is automatically completed during the agent installation process. For a [Console Installation](#) or a [Single Server Deployment](#), you must manually register GMS by logging into MySonicWall and completing the steps that follow.

Topics:

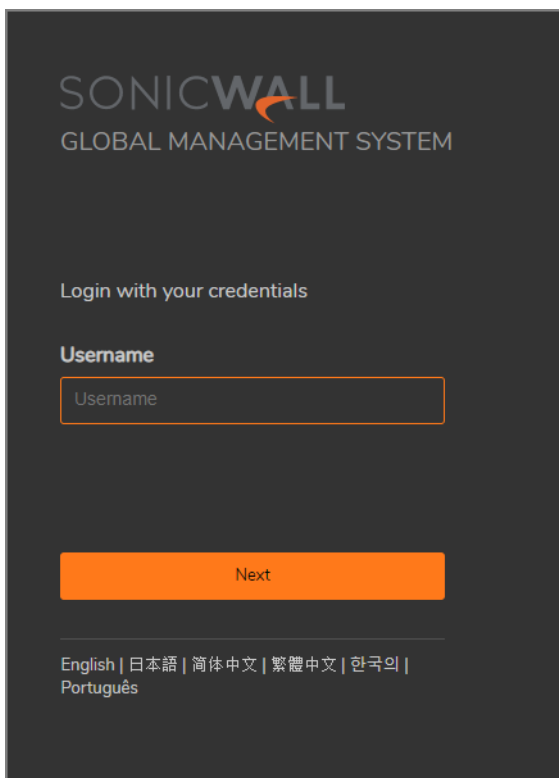
- [GMS Registration](#)

GMS Registration

This section guides you through registering your GMS installation.

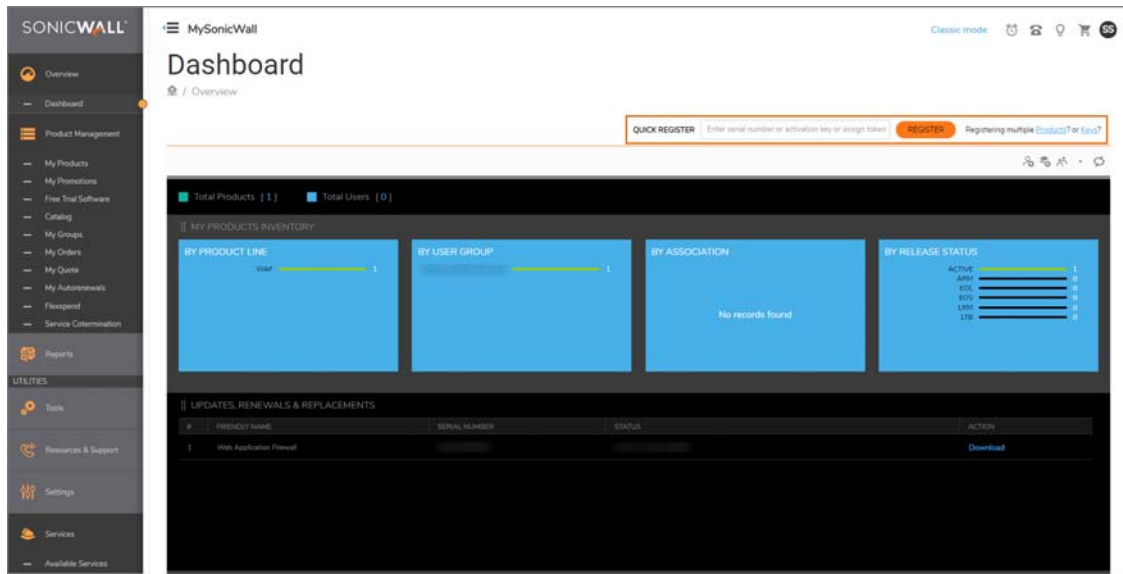
To register GMS (Console Only):

- 1 Enter your MySonicWall **username** or **email address** and **password**.

The image shows a dark-themed login interface for the SonicWall Global Management System. At the top, the SonicWall logo is displayed above the text 'GLOBAL MANAGEMENT SYSTEM'. Below this, the instruction 'Login with your credentials' is shown. A 'Username' label is positioned above a text input field containing the placeholder text 'Username'. An orange 'Next' button is located below the input field. At the bottom, a horizontal line separates the login section from a list of languages: English | 日本語 | 简体中文 | 繁體中文 | 한국의 | Português.

If you do not already have a [MySonicWall](#) account, create one before continuing.

- 2 On the left-hand menu, click **Overview > Dashboard**.
- 3 Enter the serial number or activation key or assign token in the text field next to **QUICK REGISTER**.



- 4 Click **REGISTER**. The **REGISTER A PRODUCT** dialog displays.
- 5 Enter the **Serial number**, **Friendly name**, **Authentication code**, and **Tenant Name** for your product and click **Register** again.

REGISTER A PRODUCT

Enter details below to complete registration of the following product:

Serial number

Friendly name

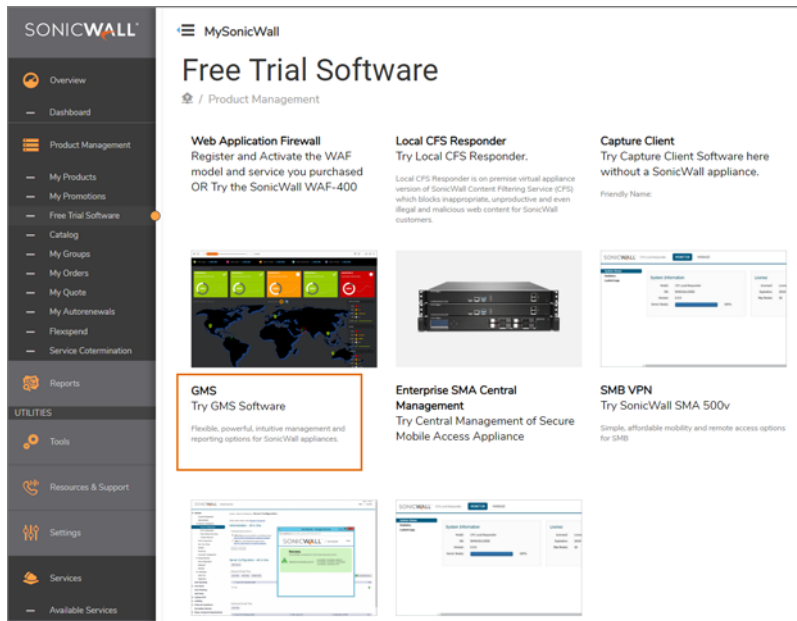
Authentication code

Tenant Name

Cancel

Register

If you do not have a license, you can get a trial license from the **Free Trial Software** page.



- 6 When your GMS is successfully registered, a confirmation message displays.
- 7 Click **Continue**.

Adding Devices

After you complete the installation and configuration of GMS, you can begin adding SonicWall network security appliances and other devices.

GMS supports these modes for adding units:

- [Basic Mode](#)
- [Advanced Mode](#)

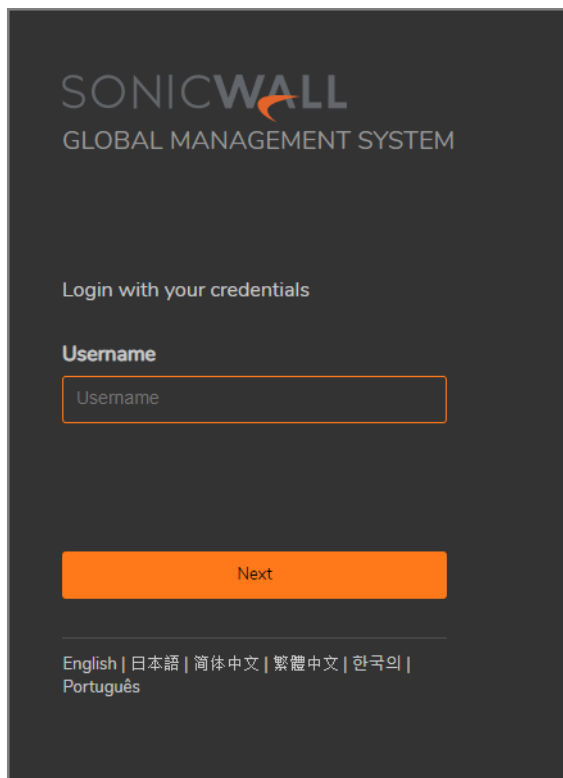
Basic Mode

Basic mode provides a simplified process for adding devices to GMS. When adding a device in Basic mode, GMS does not need to receive a heartbeat from the device as it can reach it directly by its IP address.

NOTE: You do not need to change any settings on the appliance itself to add it to GMS.

To add units to GMS in Basic mode:

- 1 If you are not already logged into GMS, log in using your administration account:



SONICWALL
GLOBAL MANAGEMENT SYSTEM

Login with your credentials

Username

Username

Next

English | 日本語 | 简体中文 | 繁體中文 | 한국의 |
Português

- 2 Click the plus (+) sign at the top left of the GMS management interface. The **Add Unit** dialog box displays.

The screenshot shows the SonicWall Global Management System 9.2 interface. The top navigation bar includes 'HOME', 'MANAGE', 'REPORTS', and 'CONSOLE'. The 'MANAGE' tab is selected, and the 'Add Unit' dialog box is open. The dialog box has three tabs: 'Basic', 'Acquisition Details', and 'Advanced'. The 'Basic' tab is active, showing fields for 'Unit Name', 'Serial Number', 'IP Address', 'Login Name' (admin), 'Password', and 'HTTPS Management Port' (443). The 'Acquisition Details' tab is also visible, showing fields for 'IP Address', 'Login Name', 'Password', and 'HTTPS Management Port'. The 'Advanced' tab is collapsed. At the bottom, there are 'Cancel' and 'OK' buttons. A note states: 'Note: The unit may be rebooted for Flow related changes to take effect.' The Reporting section shows 'Syslog based' selected and 'Disabled' unselected.

- 3 Under **Basic**, enter:
 - **Unit Name** (a user-friendly name for the device)
 - **Serial Number**
- 4 Under **Acquisition Details**, enter:
 - **IP Address**
 - **Login Name** (The default login name is admin.)
 - **Password**
 - **HTTPS Management Port** (The default port is 443.)

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

- 5 If GMS was installed with a reporting mode, but you do not want reporting for this device, select **Disabled** or **Syslog based** for **Reporting**.

Advanced Mode

Advanced mode provides a more customized process for adding devices to GMS.

To add units to GMS in Advanced mode:

- 1 Under **Advanced**, click the double-down arrow icon on the right to expand your choices.

- 2 Enter the basic information about the device you are adding to GMS:
 - Unit Name (a user-friendly name for the device)
 - Serial Number
 - IP Address
 - Login Name (The default login name is admin.)
 - Password
 - HTTPS Management Port: (The default port is 443.)
- 3 If GMS was installed with a reporting mode, but you do not want reporting for this device, select **Disabled for Reporting**.
- 4 Select **Syslog Based** for your reporting mode if you do not want **Flow based** reporting.
- 5 Click the double-down arrows to the right of the **Advanced** heading. Additional installation options become visible.
- 6 For **Managed Address**, select the radio button for **Determine automatically**, **Specify manually**, and check the box next to **Make manual address sticky**.
- 7 For **Management Mode**, select the radio button for **Using Existing Tunnel** or LAN, **Using Management Tunnel**, or **Ussing SSL**.
- 8 For **Default Port**, choose either the default port 443, or click on the up or down arrow to change the number.
- 9 For **Agent IP Address**, the designated numerical label is shown by default.
- 10 For **Standby Agent IP**, none is shown by default.
- 11 For **Sandwich**, none is shown by default.

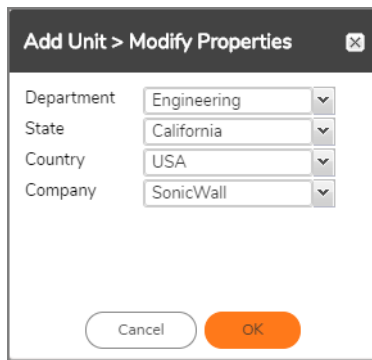
The screenshot shows the 'Advanced' configuration window for adding a device to GMS. The window is titled 'Advanced' and contains several sections:

- Managed Address:** Two radio buttons are present: 'Determine automatically' (unselected) and 'Specify manually' (selected). Below the radio buttons is a text input field. A checkbox labeled 'Make manual address sticky' is checked.
- Management Mode:** Three radio buttons are present: 'Using Existing Tunnel or LAN' (unselected), 'Using Management Tunnel' (unselected), and 'Using SSL' (selected).
- Management Port:** A dropdown menu showing '443'.
- Agent IP Address:** A dropdown menu showing '10.206.23.126'.
- Standby Agent IP:** A dropdown menu showing 'None'.
- Sandwich:** A dropdown menu showing 'None'.

At the bottom of the window, there are four buttons: 'Cancel', 'OK' (highlighted in orange), 'Properties', and 'Assign Privileges'.

- 12 Click **OK**. GMS begins the acquisition process for the device..

13 Click the **Properties** button to assign specific properties to the device:



Add Unit > Modify Properties [X]

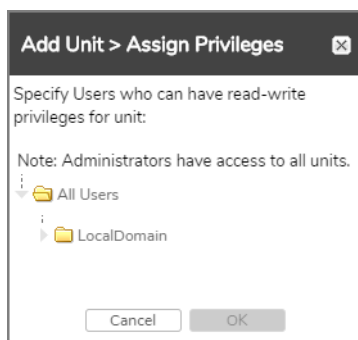
Department: Engineering ▼
State: California ▼
Country: USA ▼
Company: SonicWall ▼

Cancel OK

- Department
- State
- Country
- Company

14 Click **OK**. GMS begins the acquisition process for the device.

15 Click the **Assign Privileges** button to specify users who can have read-write privileges for the unit.



Add Unit > Assign Privileges [X]

Specify Users who can have read-write privileges for unit:

Note: Administrators have access to all units.

- └─ All Users
- └─ LocalDomain

Cancel OK

16 When you have finished setting the options for the device, click **OK**. GMS begins the acquisition process for the device.

i | **NOTE:** Administrators have access to all units.

17 When the device has been successfully acquired, you can begin managing it through GMS.

After you are done adding devices, you can begin monitoring and managing them using GMS. See [Using the GMS Management Interface](#) for more information.

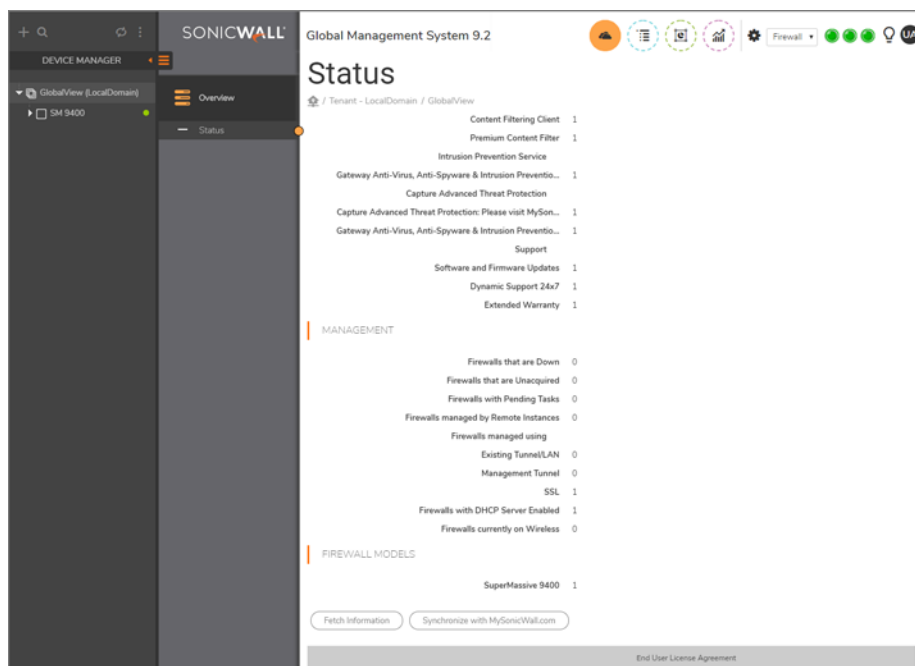
Using GMS

- Using the GMS Management Interface
- HOME View
- MANAGE View
- REPORTS View
- ANALYTICS View

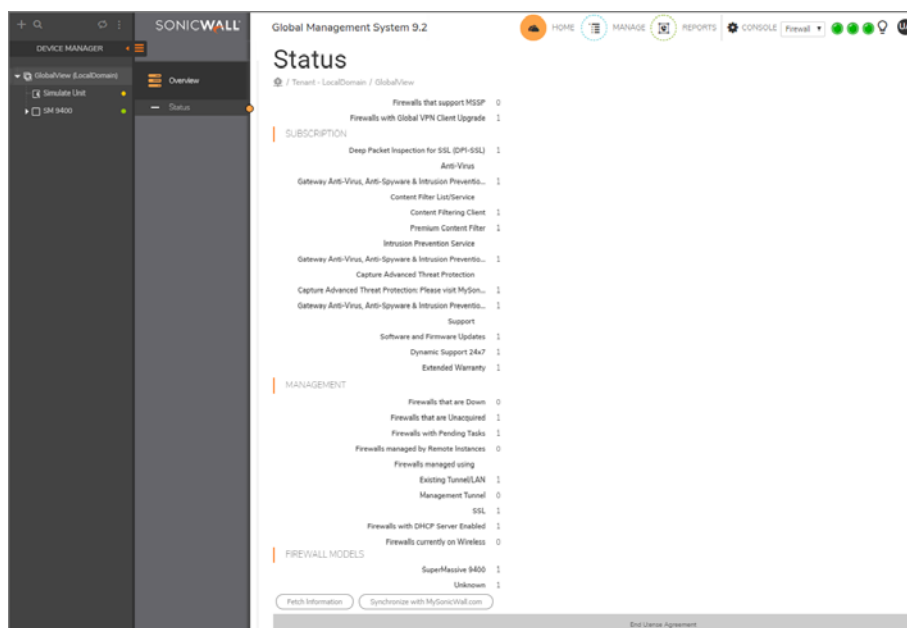
Using the GMS Management Interface

This chapter introduces the SonicWall® GMS user interface navigation and management views.

Under **Flow Based reporting**, the GMS view offers **ANALYTICS** in the top navigation.



Under **Syslog Based reporting**, the GMS view excludes **ANALYTICS** in the top navigation.




Topics:

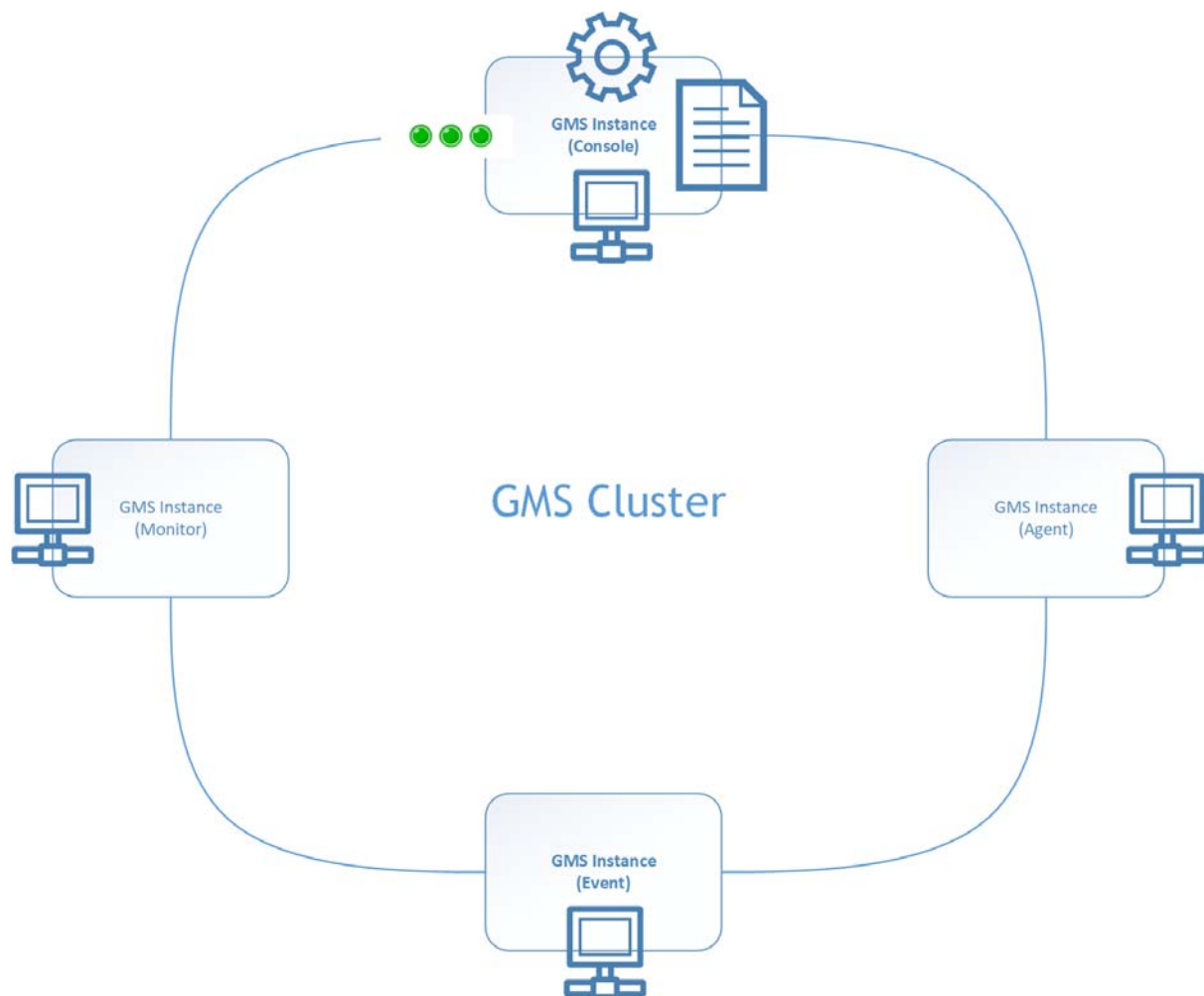
- [Centralized Management and Monitoring](#)
- [Distributed Intelligent Platform Monitoring](#)
- [Navigating the GMS Management Interface](#)
- [CONSOLE View](#)
- [Understanding GMS Icons](#)

Centralized Management and Monitoring


To enhance scalability and availability, GMS systems can now be deployed in a distributed setup. Multiple GMS instances with specific role configurations can be deployed to scale accurately. Previously, each GMS instance provided a UMH interface to configure or maintain the GMS instances. Centralized Management and Monitoring now improves on that ability.

To maintain good system health and still achieve system-wide control, the new Centralized Management and Monitoring feature empowers you to perform system-wide operations and monitor your system's health within a single-user interface.

 **NOTE:** The Centralized Management & Monitoring feature is only available on a SonicLinux-based GMS virtual machine.



The Centralized Management and Monitoring feature relies on an underlying clustering architecture that interconnects all GMS instances (deployment) to form a GMS cluster. GMS maintains the membership of a cluster, meaning it can detect when a node (a GMS instance) has joined or left the cluster. So indirectly, it detects the up/down state of a GMS instance. Each icon on top of the Console instance represents the new functionality that Centralized Management and Monitoring can provide.

The  represents the new Distributed IPM feature as described in the [Distributed Intelligent Platform Monitoring](#) section that follows.

The Gear icon, next to **CONSOLE**,  represents the applications configuration panel. By clicking it, you land on the **View Log page** where you can access **SEARCH CRITERIA** and **SEARCH RESULTS**.

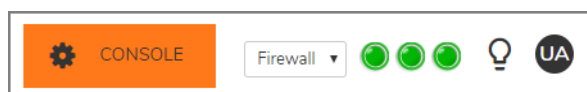
Distributed Intelligent Platform Monitoring

Topics:

- [Centralized Management](#)
- [Distributed LED State](#)
- [Enhanced Informative Tooltip Display](#)

GMS provides Distributed Intelligent Platform Monitoring (DIPM), a set of real-time monitoring tools that extends intelligent platform monitoring (IPM) to a clustering environment for improved central management. It can also provide you with an historical view of system resource usage. IPM automatically adapts to the available resources.

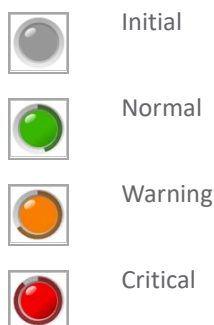
The status indicators are visible in the upper right section of the GMS management interface.



From left, the green status indicators display the current status of:

- CPU/Processor usage
- Memory/RAM usage
- Storage/Disk usage

The possible visible states of these indicators are:



The threshold values for each of these states can be set from the **Threshold Settings** section of the **IPM > Settings** page for each appliance.

Centralized Management

The following figure provides a high-level overview of the new feature. DIPM is based on existing clustering framework. The GMS console and agents join the same cluster to establish the communication channels. The collected clustering information is stored in the *SGMS DB* database. Each agent includes an IPM monitor (SAR) that runs in the background to collect and store specific information into a file-based database (represented by a journal icon in the figure). The GMS console sends requests to its associated agents to gain the data used in Settings, Real-time Monitor, and the Historical View. The agent, on the other side, pushes the real-time data back to the console to reflect the LED status.

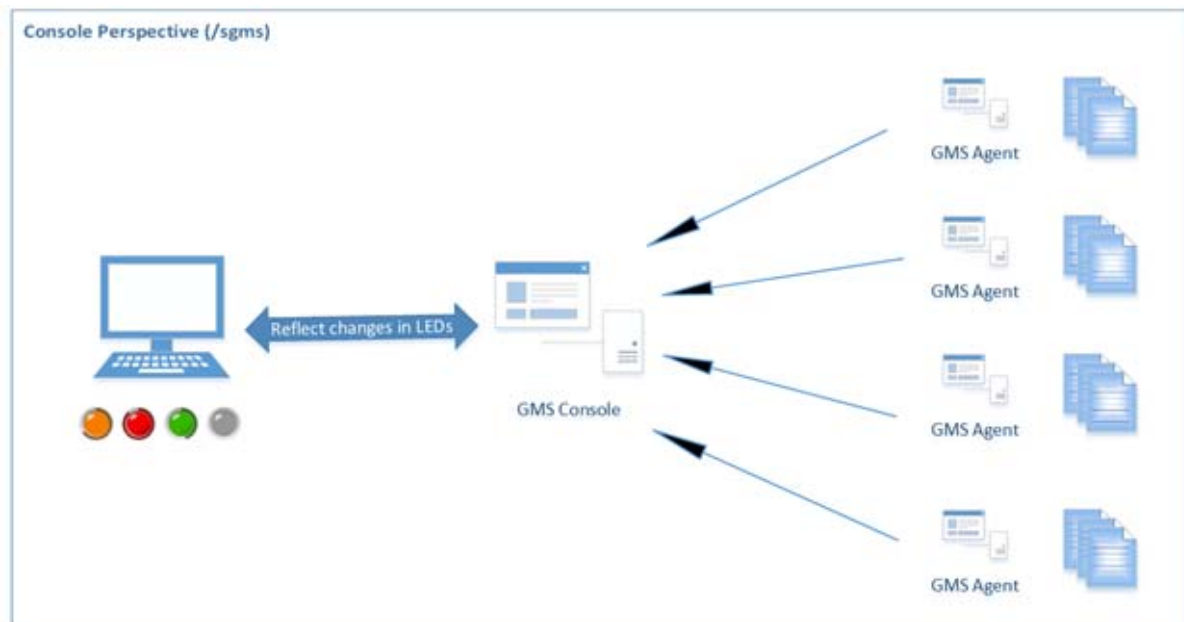
Distributed LED State

LED status involves two differing communication perspectives (Agent and Console) as shown in the following figures.

Agent Perspective



Console Perspective



The functionality of the agent perspective LEDs (/appliance) has not changed. The local IPM monitor pushes the latest metrics to the IPM Manager on the GMS agent and, if a client or browser connects to it, the data is used to reflect the LED status.

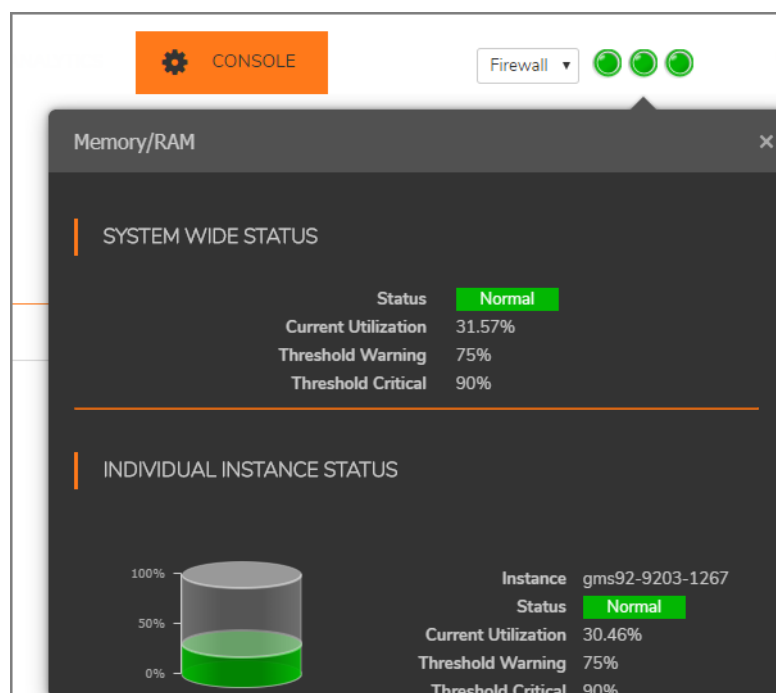
The highest severity from all the data is shown only in the outer ring of the LED. The LED status changes depending on the average of all of the agent's data over a period of 15 minutes.

The communication channel between the client or browser and the web server is bi-directional, making the push from web server to client possible.

Enhanced Informative Tooltip Display

In the figure that follows, the top section shows the overall memory utilization (as an average) as well as the threshold settings. The individual agent instances display current usage in a grid-based fashion that automatically reflect the latest updated values. An informative tooltip showing the LEDs on the console has

been enhanced to display valuable information in a distributed fashion as well. This figure provides a general impression of how the tooltip might appear.



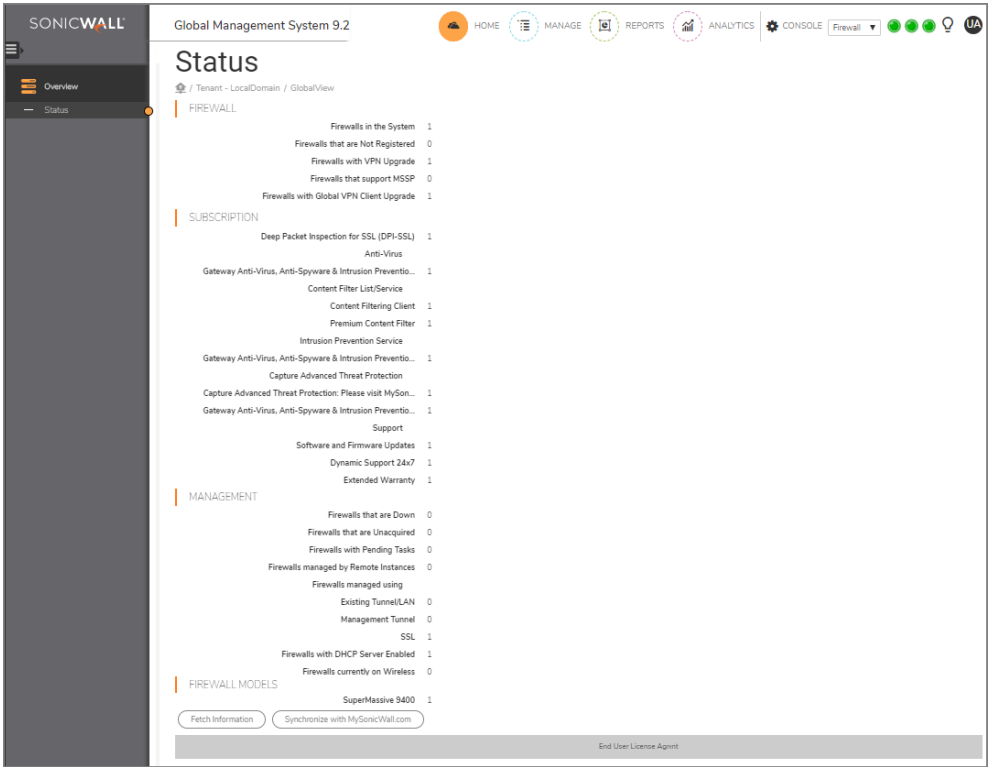
Navigating the GMS Management Interface

The SonicWall® GMS management user interface, whether in the **Flow Based** and **Syslog Based** views, is similar so the content for both is covered in this document. Differences are noted where applicable.

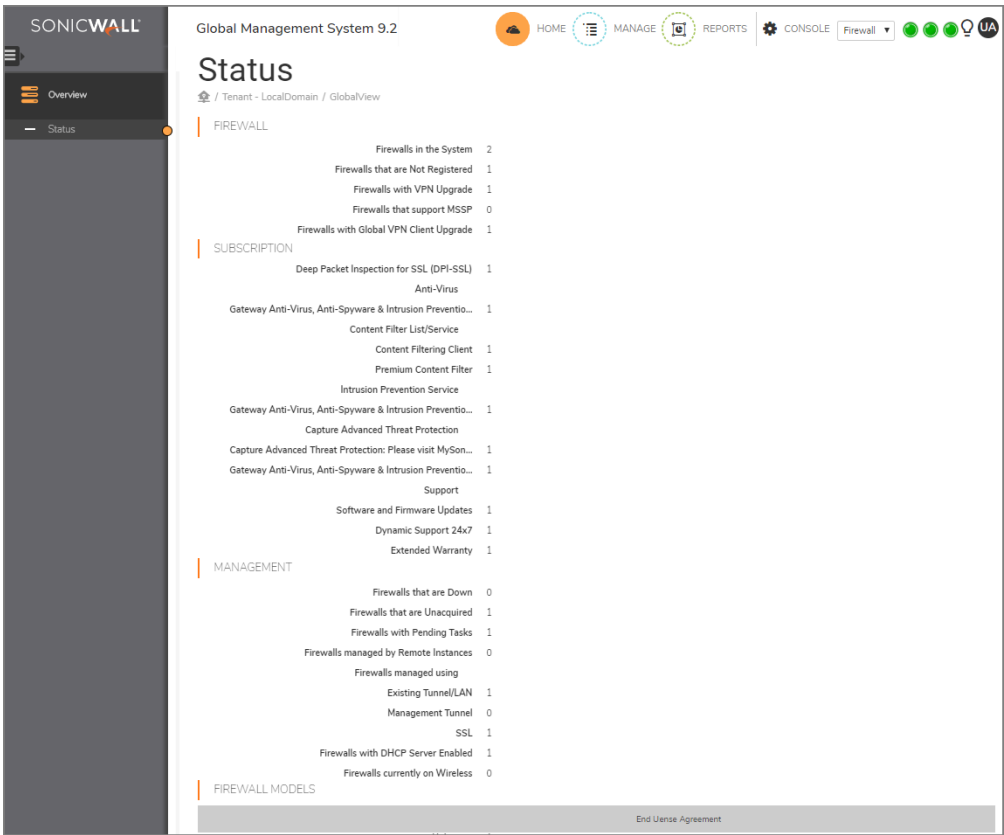
When you first open GMS, the interface shows three work areas:

- 1 **DEVICE MANAGER:** You can group the devices in your security infrastructure using the pre-defined views. Under each view you see a summary of the devices that are being managed in your security infrastructure. The views include GlobalView, Firmware View, and ModelView.
- 2 **Command Menu:** The commands are grouped under similar functions. Click on the command to expand it and see the options. For example, Status, IPM, Service Management, Log Management, and Firmware Upgrade are grouped under **Control Center**.
- 3 **Work space:** This is where all the data is displayed. You can monitor your status, see reports, set schedules, drill down for data and so forth.

Flow GMS Management UI



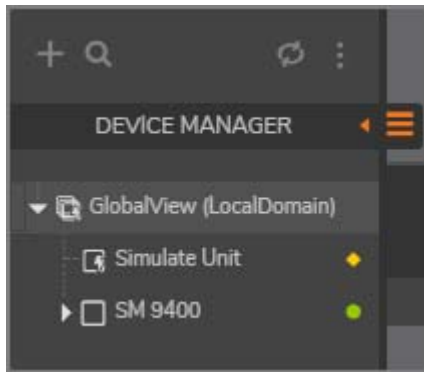
Syslog GMS Management UI



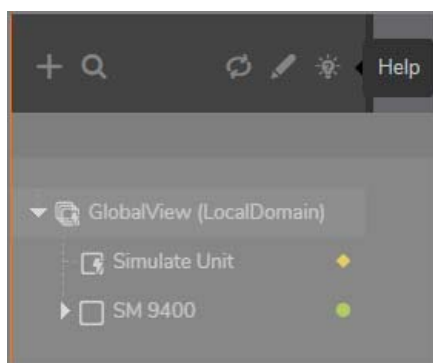
Device Manager

In the Device Manager, you can group the devices in your security infrastructure using the pre-defined views. Under each view you see a summary of all of the devices that are being managed in your security infrastructure. The appliances are listed in alphabetic order. You can change the views, and additional views include GlobalView, FirmwareView, and ModelView. In the latter two, the devices are grouped by firmware version and model number, respectively.

Above DEVICE MANAGER, there are some icons that when selected facilitate your work in this space.



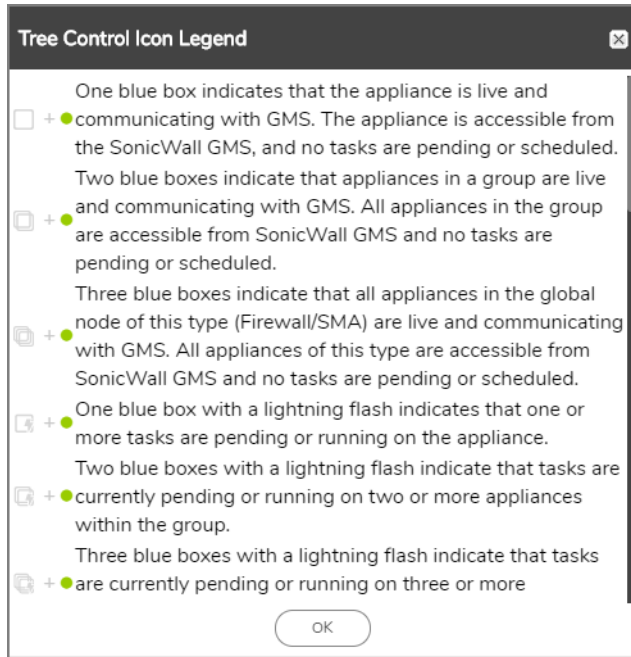
- 1 Click on the **Add Firewall (+)** icon to add a unit.
- 2 Click on the **Search icon** to look for a unit (firewall).
- 3 Click on the **Reload Device Manager icon** to refresh the Device Manager.
- 4 Click on the **vertical ellipsis icon** to expand your icon set.



- 5 Click the **edit icon** to **Modify a Unit**

A screenshot of the 'Modify Unit' dialog box. It contains the following fields and options: 'Unit Name' (text input), 'Domain' (dropdown menu), 'Serial Number' (text input), 'Managed Address' (radio buttons for 'Determine automatically' and 'Specify manually'), 'Login Name' (text input, set to 'admin'), 'Password' (text input), 'Management Mode' (radio buttons for 'Using Existing Firmware L40', 'Using Management Server', and 'Using M3'), 'Management Port' (text input, set to '443'), 'Agent IP Address' (text input, set to '10.255.2.1.1.0'), 'Standby Agent IP' (text input, set to '10.255.2.1.1.0'), and 'Reporting' (radio buttons for 'Syslog based' and 'Disabled'). At the bottom, there are buttons for 'Properties', 'Assign Privileges', 'Cancel', and 'OK'.

- 6 Click on the help icon to access the **Tree Control Icon Legend**.
- 7 The status of the device is indicated by small colored symbols next to the device name. Different symbols have different meaning.



The GMS Management Interface contains these major views:

- [HOME View](#)
- [MANAGE View](#)
- [REPORTS View](#)
- [ANALYTICS View](#)
- [CONSOLE View](#)

NOTE: The GMS Management Interface for syslog-based reporting excludes the **ANALYTICS** view.

HOME View

The **HOME** view takes you to the starting point for GMS for either flow- or syslog-based reporting. For more information about using the **HOME** view, see [HOME View](#).

MANAGE View

The **MANAGE** view is used to configure your SonicWall appliances. From the screens on this view, you can apply settings to all SonicWall appliances being managed by the GMS, all SonicWall appliances within a group, or individual SonicWall appliances.

For more information about using the **MANAGE** view, see [MANAGE View](#).

REPORTS View

The **REPORTS** view is used to view and schedule reports about critical network events and activities, such as security threats, inappropriate Web use, and bandwidth levels.

For more information about using the **REPORTS** view, see [REPORTS View](#).


ANALYTICS View

NOTE: The **ANALYTICS** view is only available if you installed GMS with the **Reporting Mode** set to **Flow based**. See for [Setting the Install Mode](#) more information.

The **ANALYTICS** view provides you with access to detailed information about the activities handled by your devices.

For more information about using the **ANALYTICS** view, see [ANALYTICS View](#).

CONSOLE View

To access the **CONSOLE** settings for GMS, click the **gear icon**  located in the top right section of the GMS management interface. To return to the **Appliance** view, click the gear icon again.







The **CONSOLE** represents the applications configuration panel. It gives you access to the **View Log** page where you can access the **SEARCH CRITERIA** and **SEARCH RESULTS** sections.

For more information about using the **CONSOLE** view, see [CONSOLE View](#).

Understanding GMS Icons

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

Status Icon Descriptions

Status Icon	Description
	One blue box indicates that the appliance is live and communicating with GMS. The appliance is accessible from the SonicWall GMS, and no tasks are pending or scheduled.
	Two blue boxes indicate that appliances in a group are live and communicating with GMS. All appliances in the group are accessible from SonicWall GMS and no tasks are pending or scheduled.
	Three blue boxes indicate that all appliances in the global node of this type (Firewall/SMA) are live and communicating with GMS. All appliances of this type are accessible from SonicWall GMS and no tasks are pending or scheduled.
	One blue box with a lightning flash indicates that one or more tasks are pending or running on the appliance.
	Two blue boxes with a lightning flash indicate that tasks are currently pending or running on two or more appliances within the group.
	Three blue boxes with a lightning flash indicate that tasks are currently pending or running on three or more appliances within the group.

Status Icon Descriptions (Continued)

	One blue box with a clock indicates that one or more tasks are scheduled on the appliance.
	Two blue boxes with a clock indicate that tasks are currently scheduled to execute at a future time on two or more appliances within the group.
	Three blue boxes with a clock indicate that tasks are currently scheduled to execute at a future time on three or more appliances within the group.
	One yellow box indicates that the appliance has been added to SonicWall GMS management (provisioned), but not yet acquired.
	Two yellow boxes indicate that two or more appliances in the group have been added to SonicWall GMS management, but not acquired.
	Three yellow boxes indicate that one or more of the appliances of this type (Firewall/SMA) have been added to SonicWall GMS management, but not acquired.
	One yellow box with a lightning flash indicates that one or more tasks are pending on the provisioned appliance.
	Two yellow boxes with a lightning flash indicates that tasks are pending on two or more provisioned appliances within the group.
	Three yellow boxes with a lightning flash indicates that tasks are pending on three or more provisioned appliances within the group.
	A green circle with the number 1 in the middle indicates that the unit is in an HA pair and is currently the Primary unit.
	A yellow circle with the number 2 in the middle indicates that the unit is in an HA pair and is currently on backup.
	One red box indicates that the appliance is no longer sending heartbeats to SonicWall GMS.
	Two red boxes indicate that two or more appliances in the group are no longer sending heartbeats to SonicWall GMS.
	Three red boxes indicate that three or more of the global group of appliances of this type (Firewall/SMA) are no longer sending heartbeats to SonicWall GMS.
	One red box with a lightning flash indicates that the appliance is no longer sending heartbeats to SonicWall GMS and has one or more tasks pending.
	Two red boxes with a lightning flash indicate that two or more appliance in the group are no longer sending heartbeats to SonicWall GMS and have one or more tasks pending.
	Three red boxes with a lightning flash indicates that the appliances are no longer sending heartbeats to SonicWall GMS and have three or more tasks pending.
	A box with a dot in the top-left corner indicates that the appliance is being managed by GMS using a static IP address.
	This icon indicates a fail over to a secondary Ethernet port.
	This icon indicates the a modem is connected using a dialup.
	This icon indicates the wireless is connected using WWAN.
	This icon indicates the unit's Task Pending status is "Immediate."
	This icon indicates the unit's Task Pending status is "Scheduled."
	Use this icon to switch between views.

HOME View

What you see on the **HOME** view depends on the **Reporting Type** you set when you install GMS. (See [Setting the Install Mode](#) for more information.)

Topics:

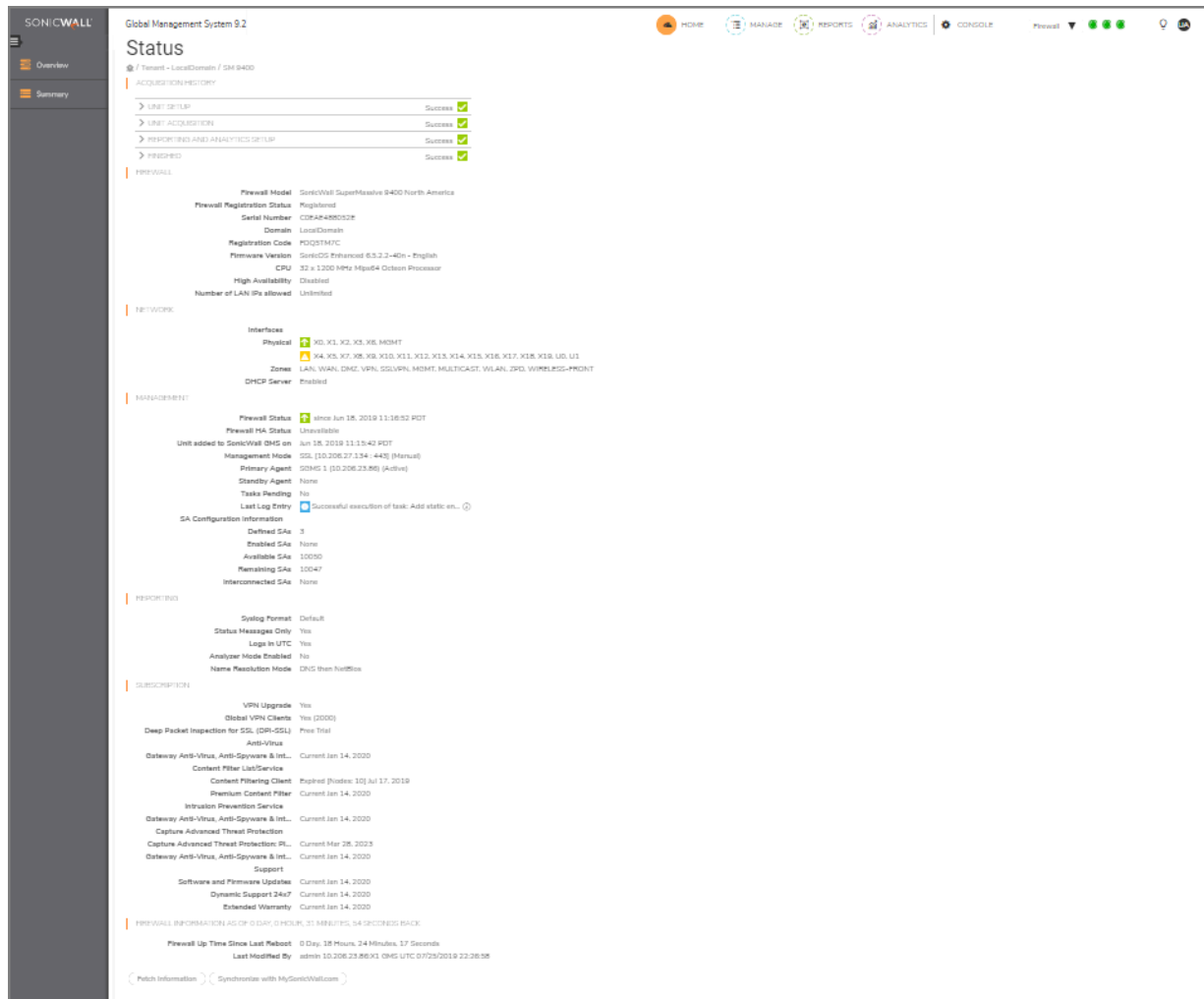
- [HOME View \(Flow Based\)](#)
- [HOME View \(Syslog Based\)](#)

HOME View (Flow Based)

The **HOME** view is the default view you see when you log in to GMS. From it you can access the **Status** page, which shows the system status, along with any applicable statistics and licensing information.

The following sections and buttons are shown:

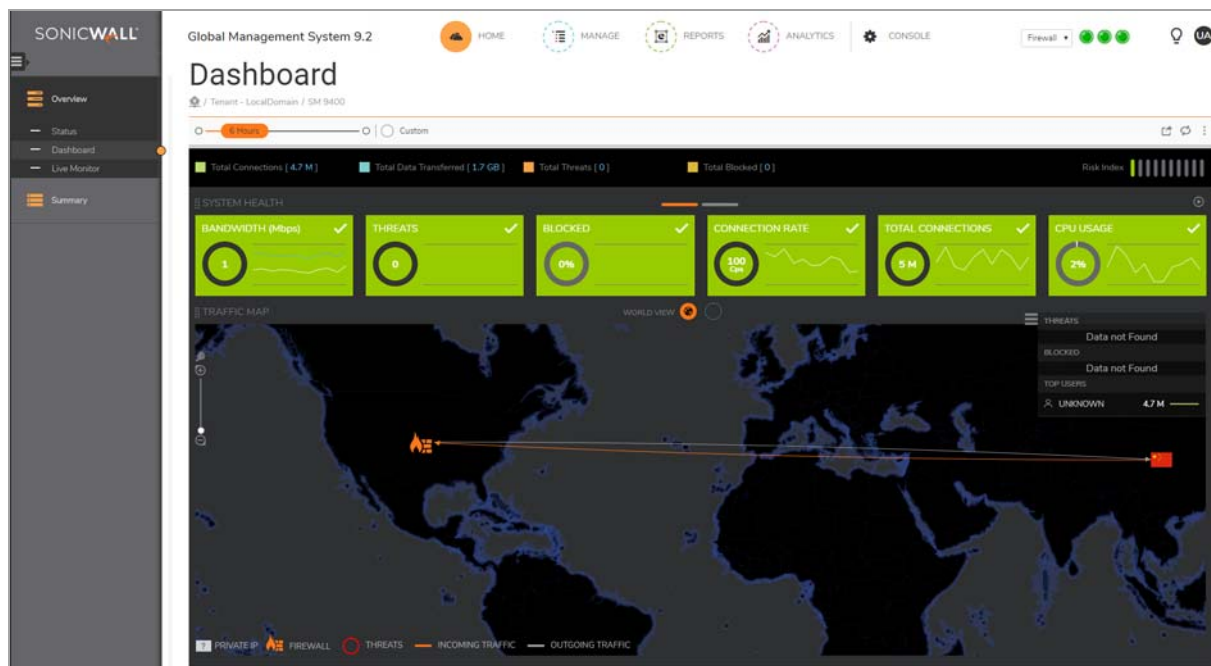
- Acquisition History
- Firewall
- Network
- Management
- Reporting
- Subscription
- Firewall Information
- Fetch Information
- Synchronize with MySonicWall.com
- End User License Agreement



Think of the **HOME** view as the starting point for most tasks:

- The **Overview** commands provide the device **Status**, **Dashboard**, and **Live Monitor**.
- The **Summary** commands provide data reports for each of the 14 parameters featured.

NOTE: The commands available in the Overview section vary according to the type of view you selected in the DEVICE MANAGER. When viewing a specific firewall, you can select the Live Monitor option instead. Differences are noted when applicable.



Upon initial login, you see a default Dashboard view. By default, it shows the activity within the last six hours.

The **Dashboard** shows your devices and a representation of the traffic being generated. It allows you to view the devices in a geographical view using a map that you can zoom in and out of. The devices are marked on the map.

The following table describes the components that make up the Dashboard.

Dashboard

Feature	Description
Sliding bar and Custom button	At the top left, use the time-lapse sliding bar and the Custom button to customize the period for which the data is being shown. Use the sliding bar to select predefined periods or define a specific period by using the Custom option.
Export/Download, Refresh, and vertical More options icons	At the top right, use the icons to generate a flow report or download a Capture Threat Assessment, refresh the data, or see other options. The other options include viewing the Page Tips, Go to Schedules (Reports Scheduled Reports > Schedules) or Go to Archives (REPORTS Scheduled Reports > Archives) .
Totals	At the top of the table, totals are provided for your security infrastructure. Includes Total Connections , Total Data Transferred , Total Threats , and Total Blocked .
Risk Index	This bar graph indicates the level of risk your firewall is currently exposed to. The values range from a single green bar to 10 red bars, with red meaning very high risk.

Dashboard

Feature	Description
SYSTEM HEALTH/ TOP ATTACKS	<p>Displays the TOP ATTACKS. Switch between views by clicking on the lines above the tiles. On the SYSTEM HEALTH view the green tiles indicate the status of the options listed. Mouse over each tile to get more data. Click on the title of the tile to drill down for additional information. Depending on the tile you click on, you are routed to Live Reports or a detailed report.</p> <p>The TOP ATTACKS cards always have orange headers. Mouse over the cards to get more details, and click on the tile title to drill down. When you click for more data, you are taken to REPORTS Details > [Tile_name].</p> <p>By clicking the Play/Pause icon in the right corner above the tiles, the view automatically switches between the SYSTEM HEALTH and TOP ATTACKS views. Clicking it again stops the switching.</p>
Threats Menu	<p>At the right of the traffic map, the threats menu shows or hides information. This show/hide block focuses on THREATS, BLOCKED and TOP USERS. By clicking on these headings, you can jump to the detailed report for that topic heading (REPORTS Details > Topic_heading).</p>
TRAFFIC MAP	<p>Displays the TRAFFIC MAP for your infrastructure. Switch between the WORLD VIEW and the GRID VIEW. On the WORLD VIEW, the threats are visually placed on the global map. You can use the roller on your mouse to zoom in or zoom out on a particular threat.</p> <p>The GRID VIEW shows the same traffic in table form, with additional details.</p>
TRAFFIC MAP Legend	<p>Provides PRIVATE IP, FIREWALL, THREATS, INCOMING TRAFFIC, and OUTGOING TRAFFIC information.</p>

Summary

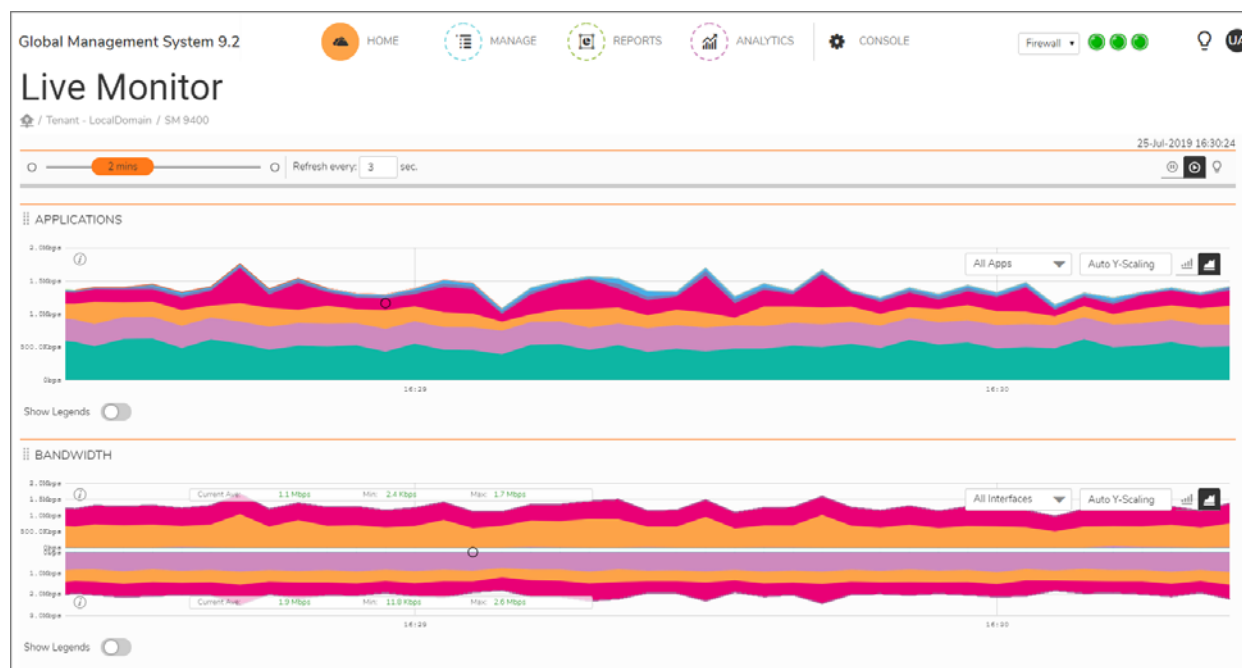
The Summary section provides access to the following reports:

- Applications
- Users
- Viruses
- Intrusions
- Spyware
- Web Categories
- Sources
- Destinations
- Source Locations
- BW Queues
- Botnet
- Blocked
- Threats

Live Monitor

Live Monitor provides a real-time view of the packets forwarded by the firewall and is visible when viewing an individual firewall. (If a group or **GlobalView** is selected in the **Device Manager**, the device options are shown instead.)

The **Live Monitor** is always running, but it does not store the data. After 10 minutes, the data is gone. However, while it is running, a background task is saving the data to a database. All data shown in Live Monitor is saved for historical reasons and you can find it in Live Reports (**REPORTS | Overview > Live Reports**).



Individual charts can be rearranged manually. Show or hide legends by clicking the **Show Legends** button.

The following charts are shown in **Live Reports**:

- **APPLICATIONS** indicates applications that are flowing through the firewall in bits per second.
- **BANDWIDTH** indicates the bandwidth utilization in bits per second.
- **PACKET RATE** shows average packets per second.
- **PACKET SIZE** shows average packets size.
- **CONNECTION RATE** indicates the new connection rate in connections per second.
- **CONNECTION COUNT** shows the total number of active connections.
- **MULTI-CORE MONITOR** shows the CPU utilization per core.

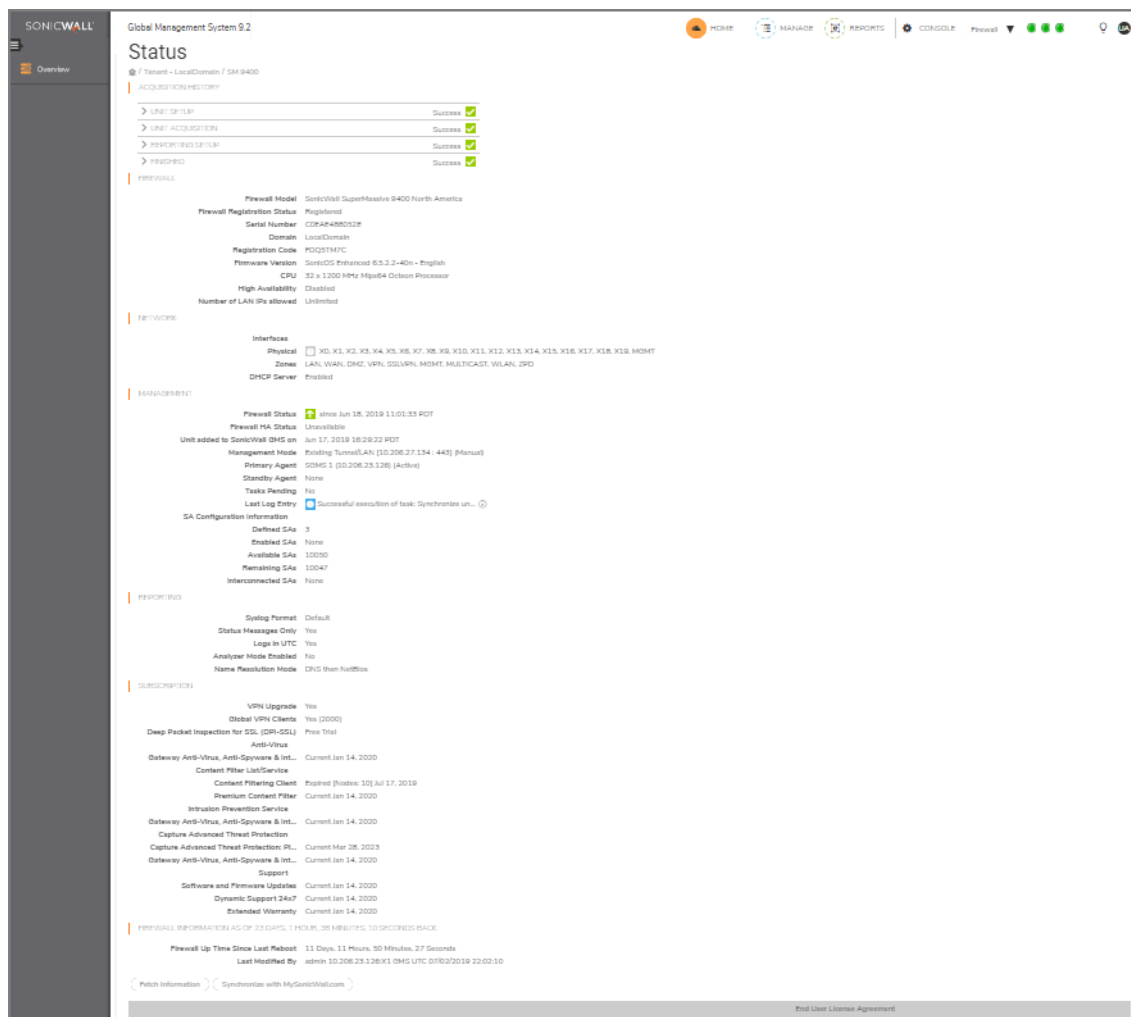
All the charts, except Connection Count, can be filtered to show a subset of the data. Click on the drop-down list in the chart and select the option you want. The chart clears and begins collecting data based on the new parameters.

HOME View (Syslog Based)

The **HOME** view is the default view managing an appliance through GMS. From it you can access the **Status** page, which gives information about the current system and any applicable statistics and licensing information.

The following sections and buttons are shown:

- Acquisition History
- Firewall
- Network
- Management
- Reporting
- Subscription
- Firewall Information
- Fetch Information
- Synchronize with MySonicWall.com
- End User License Agreement



MANAGE View

The **MANAGE** view command menus are the same for **Flow Based** and **Syslog Based**. The menu includes 27 commands that are grouped under **SETUP**, **SYSTEM**, and **SECURITY**. Click on the command of your choice to expand it and see the options expand to the right in the work space.

Topics:

- **SETUP**
- **SYSTEM**
- **SECURITY**

SETUP

The **System SETUP** section allows you to use the following commands:

- **System:** Status, Administrator, Management, SNMP, Certificates, Time, Schedules, Tools, Info, and Settings
- **Network:** interfaces, PortShield Groups, VLAN translation, Failover & LB, Zones, DNS, DNS proxy, DNS Security, Route Policies, NAT Policies, ARP, Neighbor Discovery, MAC-IP Anti-Spoof, IP Helper, Web Proxy, Topology View, and AWS Configuration
- **DHCP:** DHCP over VPN, Settings, Dynamic Ranges, Static Entries, Option Objects, Option Groups, and Trusted Agents
- **Switching:** Rapid Spanning Tree, L2 Discovery, Layer 2 QoS, and Switch Shield
- **3G4GModem:** Settings, Advanced, Connection Profiles
- **Access Points:** SonicPoints, Firmware Management, Station Status, IDS, Advanced IDP, Virtual Access Point, Rf Monitoring, FairNet, and Wi-Fi Multimedia
- **Wireless:** Settings, Security, Advanced, MAC Filter List, IDS, Virtual Access Point
- **Firewall:** Access Rules, App Rules, App Control Advanced, Address Objects, Match Objects, Action Objects, Service Objects, Bandwidth Objects, Email Address Objects, Content Filter Objects, Content Filter Policies, AWS Objects, Dynamic External Objects
- **VoIP:** Settings
- **VPN:** Settings, Summary, Configure, S2TP Server, Monitor
- **SSL VPN:** Server Settings, Portal Settings, Client Settings, Client Routes, and Virtual Office
- **Virtual Assist:** Settings
- **Users:** Status, Settings, Partitions, Multi-RADIUS, RADIUS, LDAP, Multi-LDAP, TACACS+, Local Users, Guest Services, Guest Accounts

SYSTEM

The **SYSTEM** commands allow you to configure:

- **SD-WAN:** SD-WAN Groups, Performance Probes, Performance Class Objects, Path Selection Profiles, SD-WAN Routing
- **Diagnostics:** Network Monitor, Network, Connections Monitor, CPU Monitor, Process Monitor, and Packet Monitor
- **AppFlow:** Flow Reporting, GMSFlow Server, and AppFlow Server
- **Log:** Settings, Categories, Name Resolution, and AWS Logs
- **Register/Upgrades:** Register SonicWalls, Firmware Upgrade, Service Licenses, Search, License Sharing, Used Activation Codes
- **Events:** Alert Settings, Current Alerts

SECURITY

The **SECURITY** section allows you to configure:

- **Firewall Settings:** Advanced, BWM, Flood Protection, Multicast, QoS Mapping, SSL Control, and Cipher Control
- **DPI-SSL:** Client SSL and Server SSL
- **DPI-SSH:** Configure
- **Capture ATP:** Settings and Upload Files
- **Anti-Spam:** Settings and RBL Filter
- **Security Services:** Settings, Content Filter, DPI-SSL Enforcement, Client AV Enforcement, Client CF Enforcement, Gateway Anti-Virus, Intrusion Prevention, Anti-Spyware, Geo-IP Filter, and Botnet Filter
- **Content Filter:** Settings, Custom List, Policies, CFS Exclusion List, CFS IP Address Range, CFS Custom Category, Web Features, N2H2, Websense Enterprise
- **External IDS:** Settings

REPORTS View

The **REPORTS** view features the **Overview** and **Details** command on the left-hand menu. When expanded, **Overview** has the **Status** and **Live Reports** sub-commands; and **Details** shows 14 sub-command reports.

NOTE: The **REPORTS** view is only available if you installed GMS with the **Reporting Type** set to **Flow based** or **Syslog based**. Reporting is not available if you set the **Reporting Type** to **None**. See [Setting the Install Mode](#) for more information.

NOTE: You can only get Scheduled Reports by going to **CONSOLE | Reports > Scheduled Reports**.

Topics:

- [REPORTS View \(Flow Based\)](#)
- [REPORTS View \(Syslog Based\)](#)

REPORTS View (Flow Based)

To expand the **REPORTS** view, click the **three-bar icon** at the top left of the command menu. Then, click on the firewall you want shown under the **DEVICE MANAGER**.

Topics:

- [Status](#)
- [Live Reports](#)
- [Details](#)

Status

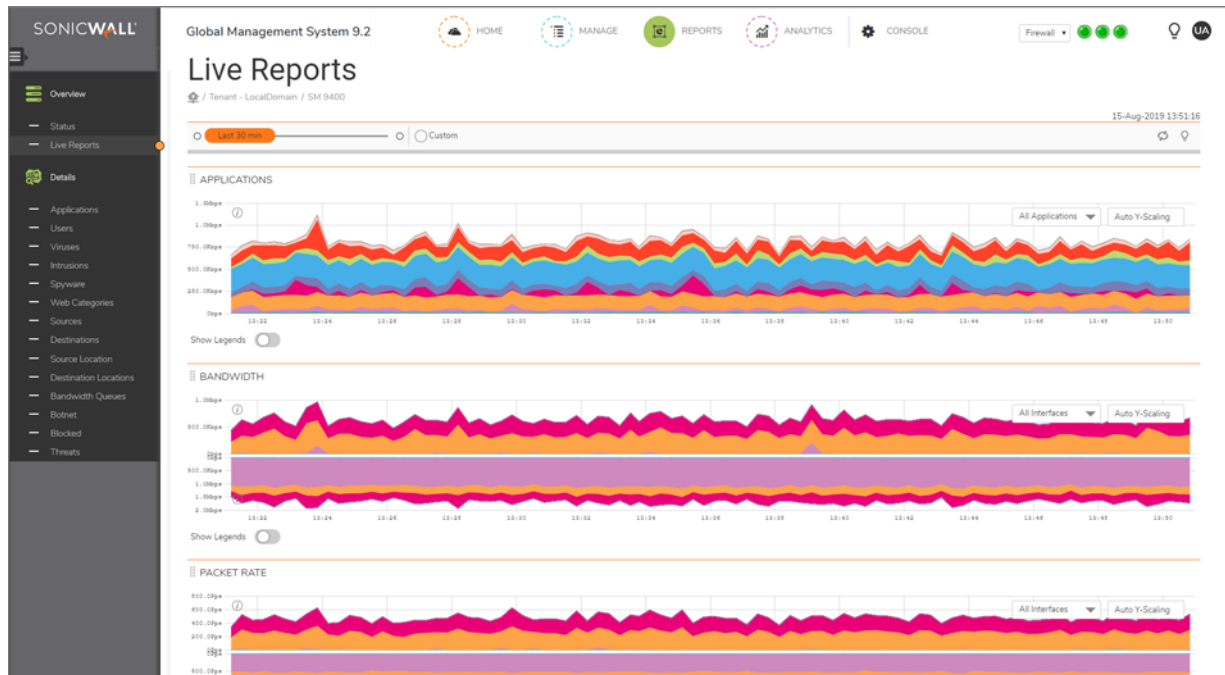
The **Status** page displays the current system status for the firewall, along with any applicable statistics and licensing information:

- Acquisition History
- Unit Setup
- Unit Acquisition
- Reporting and Analytics Setup
- Finished

Live Reports

Live Reports provide a historical view of the real-time monitor charts. You can customize the view for the past 365 days (as per license). You can choose one of the predefined periods with the sliding bar or you can define a custom period by selecting **Custom**. Individual charts can be rearranged manually. Show or hide legends by clicking the Legends button.

The following is an example of a couple of reports. Scroll down to see the others.



The following charts are shown in **Live Reports**:

- **APPLICATIONS** collects the top 25 applications that are traversing through the firewall in bits per second.
- **BANDWIDTH** indicates the incoming bandwidth utilization in bits per second.
- **PACKET RATE** shows average incoming packets per second.
- **PACKET SIZE** collects the incoming packets size, in bytes, for each interface during the collection period.
- **CONNECTION RATE** is plotted by collecting outgoing + incoming connection rate for each interface.
- **CONNECTION COUNT** shows the current number of active connections during each refresh period.
- **MULTI-CORE MONITOR** shows the CPU utilization for each core during each refresh period.

All the charts, except Connection Count, can be filtered to show a subset of the data. Click on the drop-down list in the chart and select the option you want. The chart clears and begins collecting data based on the new parameters.

Details

The following are the reports for **Details**:

- Applications
- Users
- Viruses
- Intrusions
- Spyware
- Web Categories
- Sources
- Destinations
- Source Location
- Destination Locations
- Bandwidth Queues
- Botnet
- Blocked
- Threats

The reports are available with these views:

- Chart
- Table
- Timeline

REPORTS View (Syslog Based)

To open the **REPORTS** view, select the Firewall, Email Security, or SMA view at the top left of the SonicWall GMS user interface and then click **REPORTS**.

These categories are available:

- Data Usage
- Applications
- User Activity
- Web Activity
- Web Filter
- VPN Usage
- Intrusions
- Botnet
- Geo-IP
- Gateway Viruses
- Capture ATP

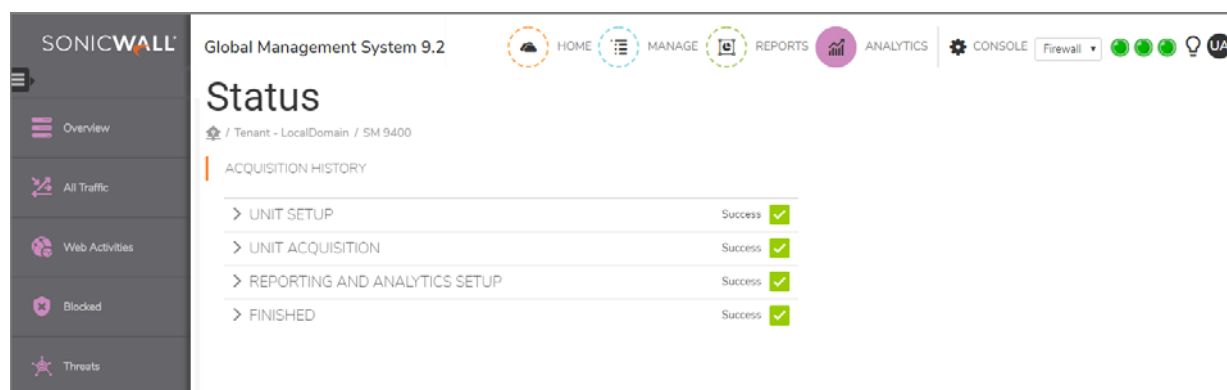
- Spyware
- Attacks
- Authentication
- Up/Down Status
- Custom Reports
- Analyzers
- Configuration
- Events

ANALYTICS View

The **ANALYTICS** view provides access to detailed information about your firewall activities.

NOTE: The **ANALYTICS** view is only available if you installed GMS with the **Reporting Type** set to **Flow based**. It is not shown in Syslog-based installations. See [Setting the Install Mode](#) for more information.

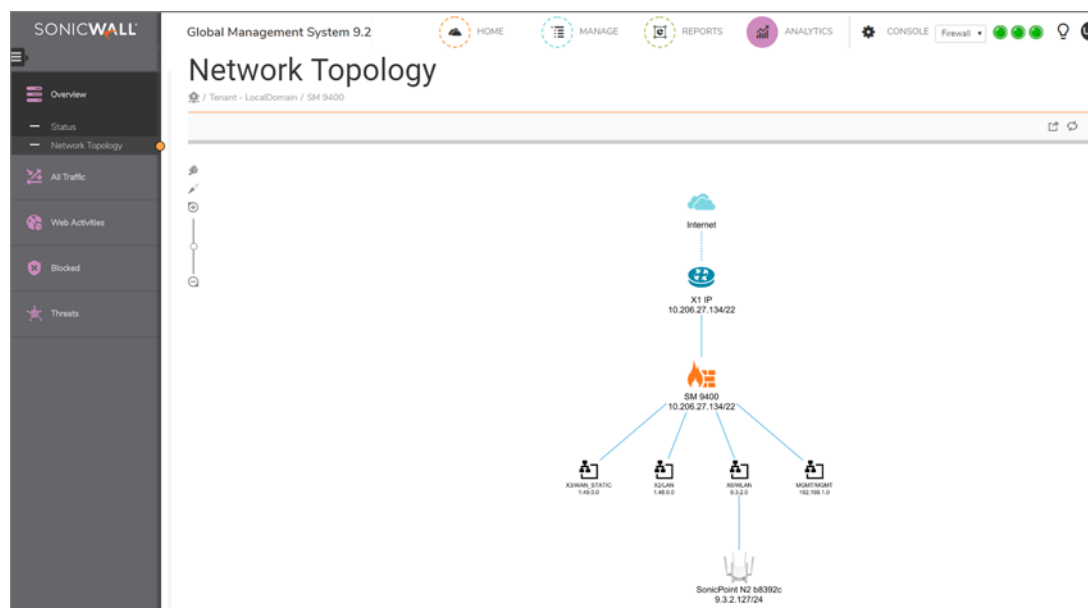
Status



The **Overview > Status** page displays the current system status for the appliance, along with any applicable statistics and licensing information:

- Acquisition History
 - Unit Setup
 - Unit Acquisition
 - Reporting and Analytics Setup
 - Finished

The **Overview > Network Topology** page shows the layout of the connections of your firewall. For example, in the image provided, you see the units connected to your **SuperMassive 9400 Series Next-Generation Firewall**. It shows the four units connected to the appliance's ports and how the SonicPoint N2 b832c is connected to X6/WLAN 9.3.2.0.



All Traffic

The **All Traffic** page displays all of the sessions going through the firewall. The All Traffic sub-commands are **Groups** and **Session Logs**.

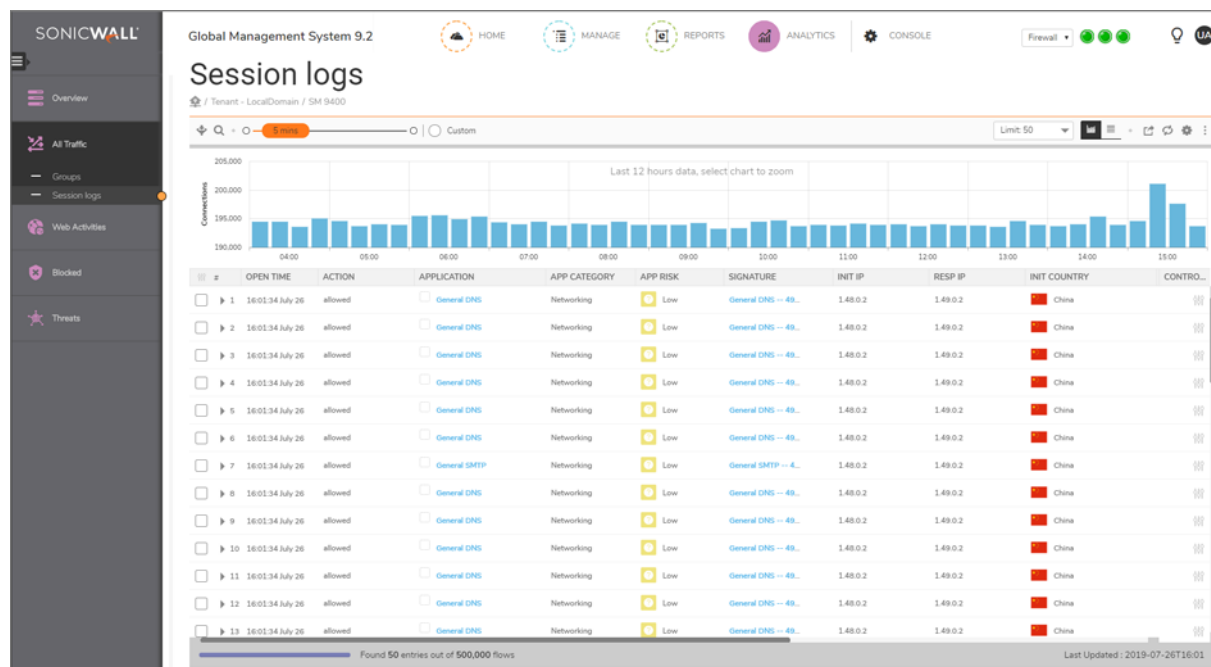
All Traffic > Groups

#	APPLICATIONS	SESSIONS	TOTAL PACKETS	TOTAL BYTES	THREATS	ACTIONS
1	General SMTP	11.5 K	120.5 K	12.8 MB	0	
2	General DNS	71 K	97.2 K	10.4 MB	0	
3	General HTTPS	5.9 K	30.2 K	4.8 MB	0	
4	General HTTP	5 K	23 K	3.2 MB	0	
5	General POP3	764	11.1 K	828 KB	0	
6	General Telnet	402	8.5 K	715 KB	0	
7	General FTP control	40	208	13.5 KB	0	
8	General TCP	20	30	1.6 KB	0	
9	Service RPC Services (IANA)	20	30	1.6 KB	0	
Total 9 items		94.7 K	290.7 K	32.8 MB	0	

100% flows scanned, Grouped 9 entries out of 500,000 / 500,000 flows

Last Updated : 2019-07-26T15:59

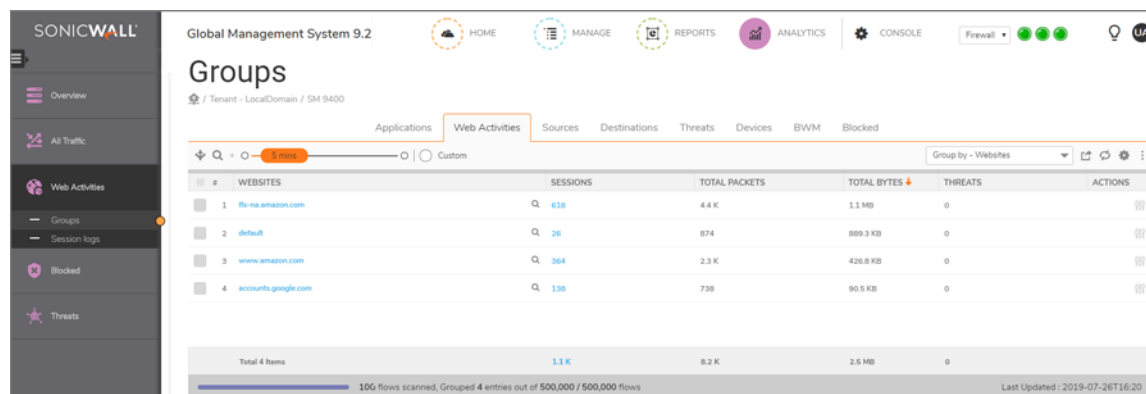
All Traffic > Session Logs



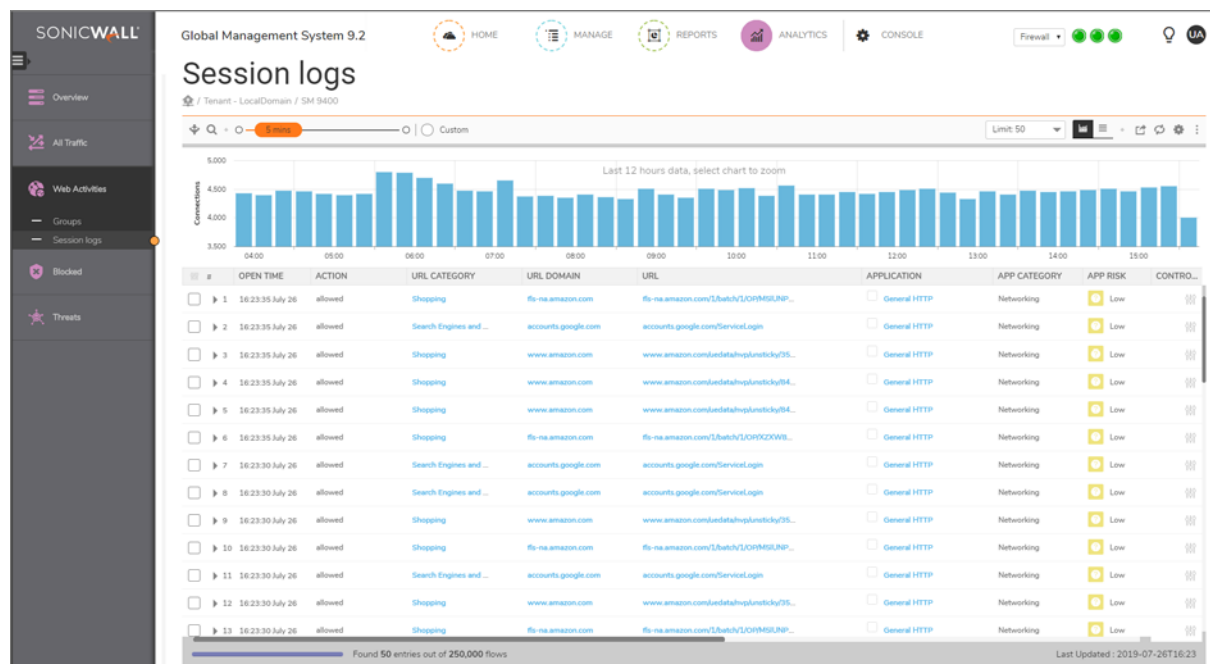
Web Activities

The **Web Activities** page displays all the websites, sessions, total packets, total bytes, threats and actions taken through the firewall. The Web Activities sub-commands are **Groups** and **Session Logs**.

Web Activities > Groups



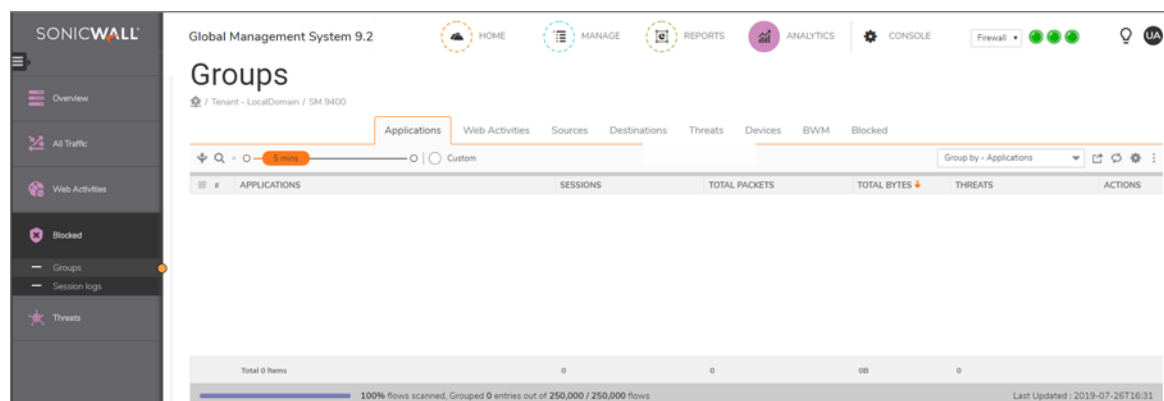
Web Activities > Session logs



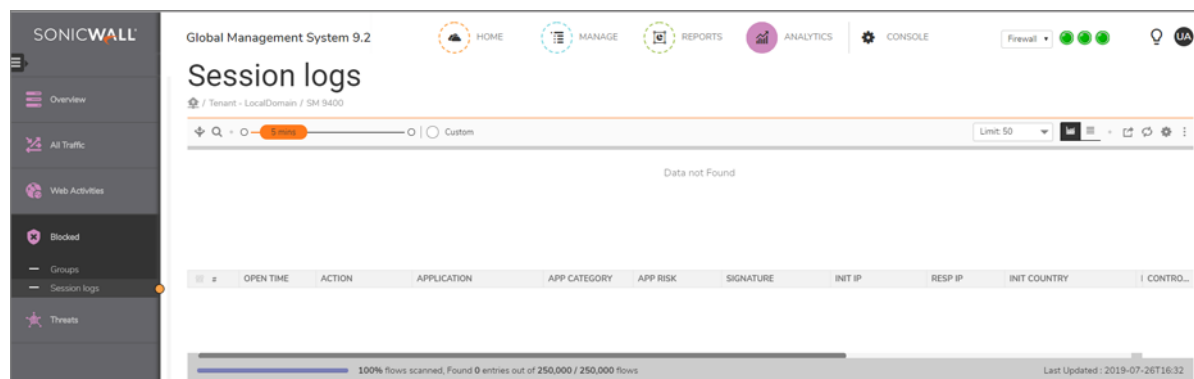
Blocked

The **Blocked** page displays information about all of the sessions blocked based on the policies configured.

Blocked > Groups



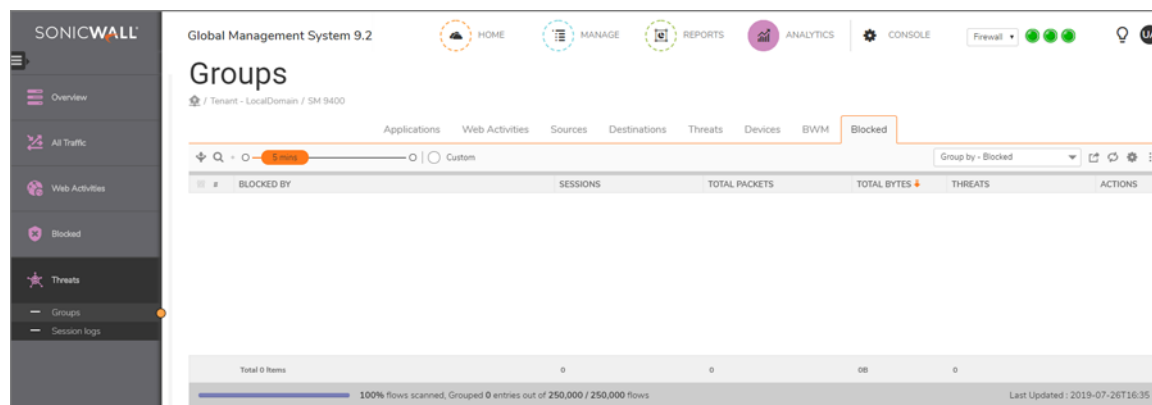
Blocked > Session Logs



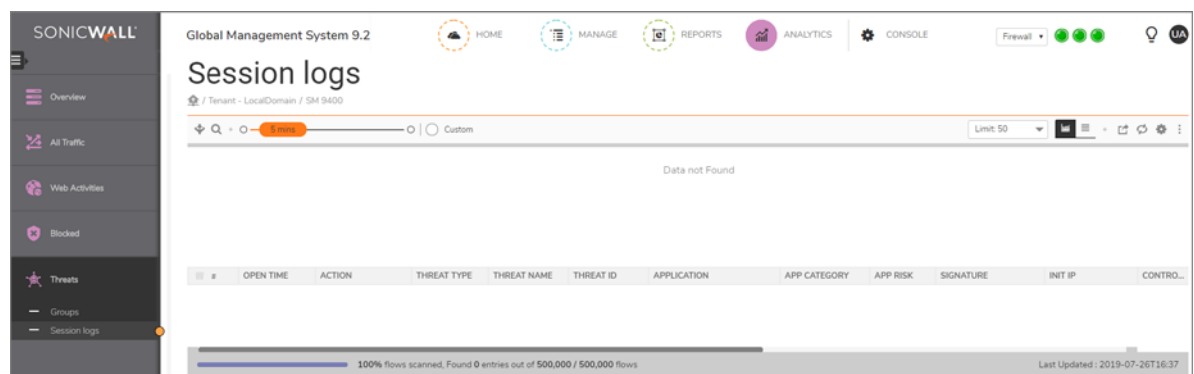
Threats

The **Threats** page displays information about the sessions that are marked as Threats by the firewall based on virus, spyware, or intrusion.

Threats > Groups



Threats > Session Logs



CONSOLE View

The **CONSOLE** view, accessed by clicking the **Gear icon**  in the top navigation, gives you the commands on the left-hand menu for the following topics:

- Appliance
- Control Center
- ZeroTouch
- Connectwise
- Workflow
- Tasks
- Diagnostics
- Web Services
- Log
- Management
- Reports
- Events
- Licenses
- Help

The **CONSOLE** represents the applications configuration panel. When you first select the **CONSOLE** view, the default shows the **CONSOLE | View Log** page. The **CONSOLE** view is the same for the **flow-based** and **syslog-based** modes, with the exception of **ANALYTICS** being present in the top navigation for the flow-based mode.

You can access **SEARCH CRITERIA** and **SEARCH RESULTS** in the **View Log** page. You can also use the **CONSOLE** view to perform basic management functions. For example, you can set the thresholds for **IPM**, **Service** and **Log Management**, and check your system **Status**.

Flow-based CONSOLE view

The screenshot displays the 'View Log' interface in the SonicWall Global Management System 9.2. The left-hand menu is visible, showing sections like Appliance, Control Center, ZeroTouch, ConnectSuite, WORKFLOW, Workflow, Tools, CURRENT STATUS, Diagnostics, Web Services, and TOOLS. The main area shows search criteria and results for flow-based logs.

SEARCH CRITERIA:

- Select Time of logs From: (mm/dd/yyyy)
- SonicWall Node: (text input)
- Message contains: (text input)
- To: (text input)
- Global Management System User: (text input)
- Severity: All (Alert, Warning and Info)
- Match case: ☐
- Exact Phrase: ☒
- All Words: ☐
- Any Word: ☐

SEARCH RESULTS:

10 Messages per screen (Range: 10-100) Apply

#	DATE	MESSAGE	SEVERITY	UNIT NAME/STATUS	GMS USER	USER IP
1	Jul 10, 2019 Wed (12:24:24 PM)	Successful login into the system by user: admin	INFO		admin@LocalDomain	10.21.120.202
2	Jul 9, 2019 Tue (06:00:48 PM)	Successful logout by the user: admin	INFO		admin@LocalDomain	10.21.120.202
3	Jul 9, 2019 Tue (06:00:26 PM)	Successful login into the system by user: admin	INFO		admin@LocalDomain	10.21.120.202
4	Jul 9, 2019 Tue (03:22:20 PM)	Successful login by the user: admin	INFO		admin@LocalDomain	10.21.120.202
5	Jul 9, 2019 Tue (02:49:14 PM)	Successful login into the system by user: admin	INFO		admin@LocalDomain	10.50.193.54
6	Jul 9, 2019 Tue (02:49:02 PM)	Unsuccessful login attempt into the system by user: admin	WARNING		admin@LocalDomain	10.50.193.54
7	Jul 9, 2019 Tue (01:30:12 PM)	Successful execution of task: Add New Split DNS: Proxy SonicWall.com Scheduler IP: 10.206.23.86	INFO	ea SM 9400	admin@LocalDomain	
8	Jul 9, 2019 Tue (01:30:10 PM)	Scheduled Task for Immediate Execution: Add New Split DNS: Proxy SonicWall.com	INFO	ea SM 9400	admin@LocalDomain	
9	Jul 9, 2019 Tue (01:27:32 PM)	Successful execution of task: Add New Split DNS: SonicWall.com Scheduler IP: 10.206.23.86	INFO	ea SM 9400	admin@LocalDomain	
10	Jul 9, 2019 Tue (01:27:24 PM)	Scheduled Task for Immediate Execution: Add New Split DNS: SonicWall.com	INFO	ea SM 9400	admin@LocalDomain	

Displaying 1-10 Next

Syslog-based CONSOLE view

The screenshot displays the 'View Log' interface in the SonicWall Global Management System 9.2, showing syslog-based search results. The left-hand menu is visible, showing sections like Appliance, Control Center, ZeroTouch, ConnectSuite, WORKFLOW, Workflow, Tools, CURRENT STATUS, Diagnostics, Web Services, and TOOLS. The main area shows search criteria and results for syslog-based logs.

SEARCH CRITERIA:

- Select Time of logs From: (mm/dd/yyyy)
- SonicWall Node: (text input)
- Message contains: (text input)
- To: (text input)
- Global Management System User: (text input)
- Severity: All (Alert, Warning and Info)
- Match case: ☐
- Exact Phrase: ☒
- All Words: ☐
- Any Word: ☐

SEARCH RESULTS:

100 Messages per screen (Range: 10-100) Apply

#	DATE	MESSAGE	SEVERITY	UNIT NAME/STATUS	GMS USER	USER IP
1	Jul 24, 2019 Wed (11:39:59 AM)	Successful login into the system by user: admin	INFO		admin@LocalDomain	monit-4os29hd@us.sonicwall.com (10.21.120.10)
2	Jul 24, 2019 Wed (11:38:04 AM)	Report data summarized: processed in 1.0 minutes.	INFO			10.206.23.126
3	Jul 24, 2019 Wed (11:37:04 AM)	Report data summarization started. All files have been queued for processing.	INFO			10.206.23.126
4	Jul 24, 2019 Wed (11:23:04 AM)	Report data summarized: processed in 1.0 minutes.	INFO			10.206.23.126
5	Jul 24, 2019 Wed (11:22:04 AM)	Report data summarization started. All files have been queued for processing.	INFO			10.206.23.126
6	Jul 24, 2019 Wed (11:08:04 AM)	Report data summarized: processed in 1.0 minutes.	INFO			10.206.23.126
7	Jul 24, 2019 Wed (11:07:04 AM)	Report data summarization started. All files have been queued for processing.	INFO			10.206.23.126
8	Jul 24, 2019 Wed (10:53:04 AM)	Report data summarized: processed in 1.0 minutes.	INFO			10.206.23.126
9	Jul 24, 2019 Wed (10:52:04 AM)	Report data summarization started. All files have been queued for processing.	INFO			10.206.23.126
10	Jul 24, 2019 Wed (10:38:04 AM)	Report data summarized: processed in 1.0 minutes.	INFO			10.206.23.126

The commands in the left-hand menu are divided into the **WORKFLOW**, **CURRENT STATUS**, **TOOLS**, **SYSTEM SETUP**, and **HELP** sections. Each section subcommands help you manage your system better.

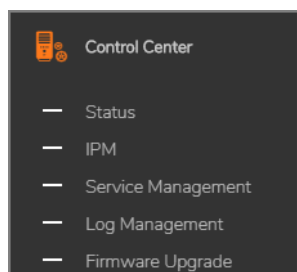
New feature commands have been introduced with 9.2 and include **Control Center**, **ZeroTouch**, **Connectwise**, **Scheduled Reports**, **Archive**, **Templates**, and Syslog-Based installations such as **Syslog Mount**.

Topics:

- [Control Center](#)
- [ZeroTouch](#)
- [Connectwise](#)
- [Reports](#)
- [Syslog-Based Installations](#)

Control Center

Control Center is accessible by clicking the Gear icon, next to **CONSOLE**, in the top navigation and selecting **Control Center** from the left-hand menu.



Each command represents a separate GMS function. Identifying information for the GMS function is clearly listed in each sub-command page. There are five feature functions for **Flow Based** and **Syslog Based** reporting:

Status

The **Control Center > Status** page gives you two Instance server sections with information. Each section provides the **Serial**, **IP Address**, **Role**, **OS**, **Memory**, **CPU**, and **Current Version** of software you are running.

IPM

The **Control Center > IPM** page features three tabs for **Threshold Settings**, **Real-Time Monitor**, and **Historical View**. Each tab shows information for your instance. For more information about the IPM feature, see [Distributed Intelligent Platform Monitoring](#) as well as the following images:

Threshold Settings

Threshold Settings

Real-Time Monitor

Historical View

INSTANCE - GMS92-9203-1267

CPU/PROCESSOR

SEVERITY: MEDIUM

608075%

Reset

Apply

SEVERITY: HIGH

859590%

Reset

Apply

MEMORY/RAM

SEVERITY: MEDIUM

608075%

Reset

Apply

SEVERITY: HIGH

859590%

Reset

Apply

STORAGE/DISK

SEVERITY: MEDIUM

607566%

Reset

Apply

SEVERITY: HIGH

809585%

Reset

Apply

ESTIMATED CAPACITY

SEVERITY: MEDIUM

607566%

Reset

Apply

SEVERITY: HIGH

809585%

Reset

Apply

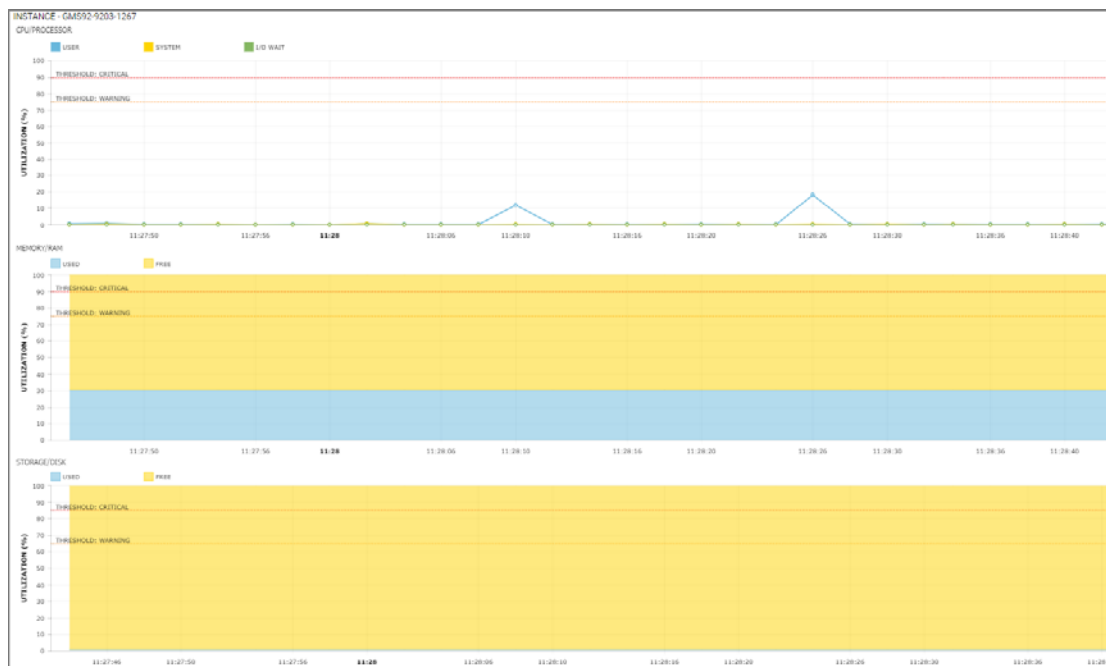
CAPACITY ESTIMATION SETTINGS

ENFORCE DISK CAPACITY ESTIMATION

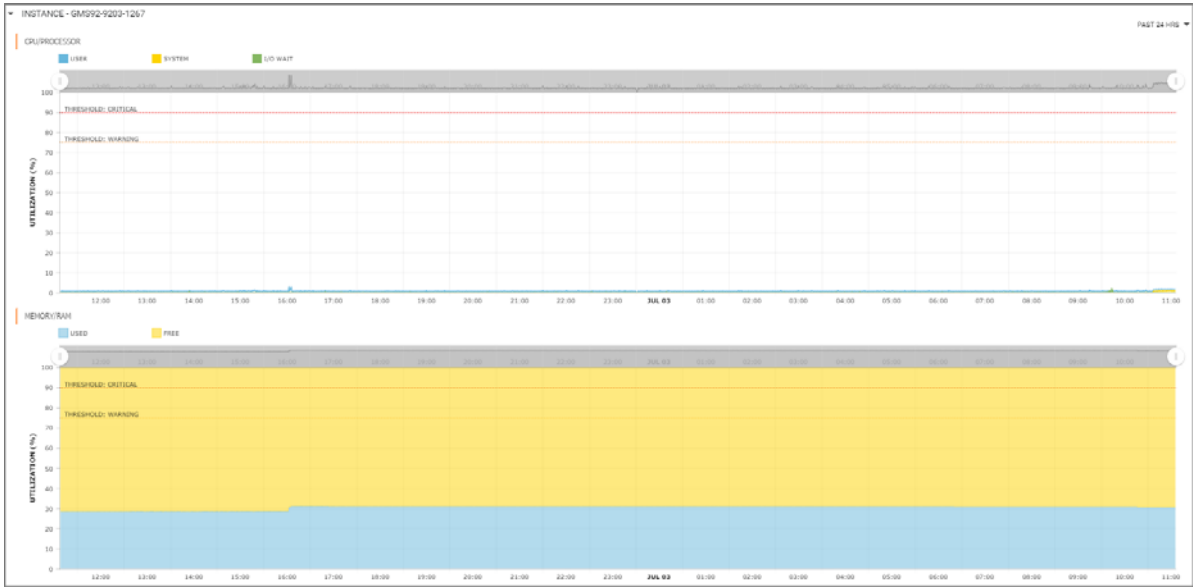
Apply

INSTANCE - FLOW SERVER_INSTANCE

Real-Time Monitoring



Historical View Data



Service Management

The **Control Center > Service Management** page provides two tabs for **Individual Service Management** and **Group Service Management**. All the installed service(s) of a GMS instance are listed in a tabular format. You can **START/STOP** service(s) by selecting the checkbox(es) of the service(s) you would like to include and click **Enable/Start**, or **Disable/Stop** to execute the actions.

Individual Service Management

Service Management

/ Tenant - LocalDomain

Individual Service Management

Group Service Management

INSTANCE - GMS92-9203-1267

SERVICE	STATUS	PO
<input type="checkbox"/> SONICWALL UNIVERSAL MANAGEMENT SUITE - SCHEDULER	STARTED (ENABLED)	
<input checked="" type="checkbox"/> SONICWALL UNIVERSAL MANAGEMENT SUITE - REPORTS SCHEDULER	STARTED (ENABLED)	
<input type="checkbox"/> SONICWALL UNIVERSAL MANAGEMENT SUITE - MONITORING MANAGER	STARTED (ENABLED)	
<input type="checkbox"/> SONICWALL UNIVERSAL MANAGEMENT SUITE - SYSLOG COLLECTOR	STARTED (ENABLED)	
<input checked="" type="checkbox"/> SONICWALL UNIVERSAL MANAGEMENT SUITE - FLOW SUMMARIZER	STARTED (ENABLED)	
<input type="checkbox"/> SONICWALL UNIVERSAL MANAGEMENT SUITE - EVENT MANAGER	STARTED (ENABLED)	

Disable/Stop

Enable/Start

Group Service Management

Service Management

/ Tenant - LocalDomain

Individual Service Management

Group Service Management

ALL INSTANCES

SERVICE	INSTANCE	STATUS	PORT
<input type="checkbox"/> SONICWALL UNIVERSAL MANAGEMENT SUITE - SCHEDULER	GMS92-9203-1267	STARTED (ENABLED)	2999
<input checked="" type="checkbox"/> SONICWALL UNIVERSAL MANAGEMENT SUITE - REPORTS SCHEDULER	GMS92-9203-1267	STARTED (ENABLED)	21001
<input type="checkbox"/> SONICWALL UNIVERSAL MANAGEMENT SUITE - MONITORING MANAGER	GMS92-9203-1267	STARTED (ENABLED)	21005
<input type="checkbox"/> SONICWALL UNIVERSAL MANAGEMENT SUITE - SYSLOG COLLECTOR	GMS92-9203-1267	STARTED (ENABLED)	21004
<input checked="" type="checkbox"/> SONICWALL UNIVERSAL MANAGEMENT SUITE - FLOW SUMMARIZER	GMS92-9203-1267	STARTED (ENABLED)	21026
<input type="checkbox"/> SONICWALL UNIVERSAL MANAGEMENT SUITE - EVENT MANAGER	GMS92-9203-1267	STARTED (ENABLED)	21010

Disable/Stop

Enable/Start

Log Management

The **Control Center > Log Management** page provides two tabs for **Individual Log Management** and **Group Log Management**. Log Management provides a convenient way for you to download the log files of a GMS instance system. The Log Management user interface allows you to select a single or multiple log files from a predefined directory list. All the log files, along with the Technical Support Report (TSR), are zipped into a .ZIP file.

Individual Log Management

Log Management

Tenant - LocalDomain

Individual Log ManagementGroup Log Management

INSTANCE - GMS92-9203-1267

Search Text...

<input type="checkbox"/>	File Name	Category	File Size	Modified Date
<input type="checkbox"/>	appflow.log	Application Logs	1,692,503	Wed Jul 03 2019 11:59:09 GMT-0700 (Pacific Daylight Time)
<input type="checkbox"/>	appflows.log	Application Logs	1,535	Wed Jun 19 2019 13:19:40 GMT-0700 (Pacific Daylight Time)
<input type="checkbox"/>	archive.log	Application Logs	985	Wed Jun 19 2019 13:19:40 GMT-0700 (Pacific Daylight Time)
<input type="checkbox"/>	DbgAppliance0.log	Application Logs	3,636,036	Wed Jul 03 2019 12:00:09 GMT-0700 (Pacific Daylight Time)
<input type="checkbox"/>	DbgAppliance0.log.1	Application Logs	7,004	Tue Jun 18 2019 10:58:56 GMT-0700 (Pacific Daylight Time)
<input type="checkbox"/>	DbgAppliance1.log	Application Logs	10,000,145	Wed Jun 26 2019 01:47:09 GMT-0700 (Pacific Daylight Time)
<input type="checkbox"/>	DbgDatabaseUpdate.log	Application Logs	11,397	Wed Jun 19 2019 20:49:05 GMT-0700 (Pacific Daylight Time)
<input type="checkbox"/>	DbgEventManager0.log	Application Logs	9,091,551	Wed Jul 03 2019 12:00:18 GMT-0700 (Pacific Daylight Time)

Include the Technical Support Report (TSR)

Download Logs

Group Log Management

Log Management

Tenant - LocalDomain

Individual Log Management**Group Log Management**

Search Text...

<input type="checkbox"/>	File Name	Category	Instance	File Size	Modified Date
<input type="checkbox"/>	appflow.log	Application Logs	Flow Server_Instan...	1,221,969	Wed Jul 03 2019 11:57:39 GMT-0700 (Pacific Daylight Time)
<input type="checkbox"/>	appflows.log	Application Logs	Flow Server_Instan...	307	Wed Jun 19 2019 20:51:55 GMT-0700 (Pacific Daylight Time)
<input type="checkbox"/>	archive.log	Application Logs	Flow Server_Instan...	197	Wed Jun 19 2019 20:51:56 GMT-0700 (Pacific Daylight Time)
<input type="checkbox"/>	DbgAppliance0.log	Application Logs	Flow Server_Instan...	6,611,053	Wed Jul 03 2019 12:02:25 GMT-0700 (Pacific Daylight Time)
<input type="checkbox"/>	DbgDatabaseUpdate.log	Application Logs	Flow Server_Instan...	10,277	Wed Jun 19 2019 20:52:23 GMT-0700 (Pacific Daylight Time)
<input type="checkbox"/>	DbgVPScheduler0.log	Application Logs	Flow Server_Instan...	209	Wed Jun 19 2019 20:52:01 GMT-0700 (Pacific Daylight Time)
<input type="checkbox"/>	logdump.log	Application Logs	Flow Server_Instan...	197	Wed Jun 19 2019 20:51:56 GMT-0700 (Pacific Daylight Time)
<input type="checkbox"/>	network.log	Application Logs	Flow Server_Instan...	234	Wed Jun 19 2019 20:51:56 GMT-0700 (Pacific Daylight Time)

Include the Technical Support Report (TSR)

Download Logs

Firmware Upgrade

The **Control Center > Firmware Upgrade** page provides you with the capability of upgrading the firmware version of a GMS instance. You have two tabs to choose from: **Individual Upgrade** and **Group Firmware Upgrade**.

Individual Upgrade

Firmware Upgrade

/ Tenant - LocalDomain

Individual Upgrade

Group Firmware Upgrade

GMS92-9203-1267 - 9.2.9205.1285.0000

Choose the file

Choose

Upload

Cancel

FLOW SERVER_INSTANCE - 9.2.9205.1285.0000

Choose the file

Choose

Upload

Cancel

Group Firmware Upgrade

Firmware Upgrade

/ Tenant - LocalDomain

Individual Upgrade

Group Firmware Upgrade

Instances Upgrade

<input type="checkbox"/>	Instance Name	Current Version	Status
<input type="checkbox"/>	gms92-9203-1267	9.2.9205.1285.0000	Upgraded on 2019-06-12 14:48:27.0
<input type="checkbox"/>	Flow Server_Instance	9.2.9205.1285.0000	Upgraded on 2019-06-19 20:50:07.0

Choose the file

Choose

Upload

Cancel

ZeroTouch

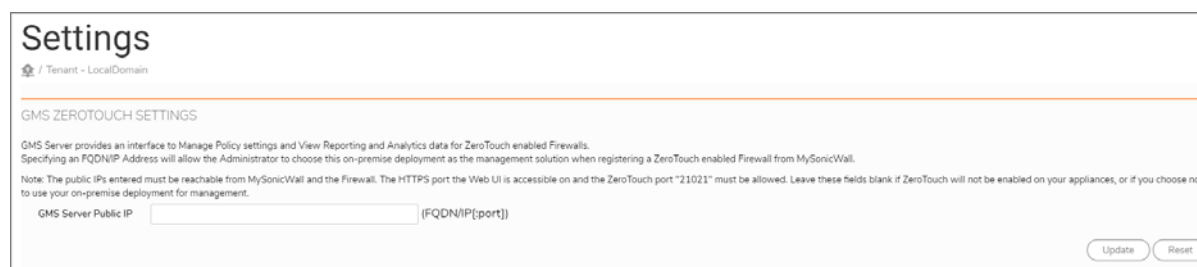
ZeroTouch settings are accessible by clicking the **Gear icon**, next to **CONSOLE**, in the top navigation and selecting **ZeroTouch** in the left-hand command menu.

GMS server provides an interface to Manage Policy settings and View Reporting and Analytics data for ZeroTouch-enabled firewalls.

Specifying an **FQDN/IP Address** next to **GMS Server Public IP** allows the administrator to choose this on-premise deployment as the management solution. When registering a ZeroTouch-enabled firewall from MySonicWall, this on-premises GMS server IP is shown in the drop-down values, to be selected as the management solution.

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

GMS ZeroTouch Settings



Settings
Tenant - LocalDomain

GMS ZERO TOUCH 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 (FQDN/IP[:port])

Update Reset

To Enter a GMS Server Public IP Address for GMS ZeroTouch Settings:

- 1 Go to **CONSOLE | ZeroTouch > Settings**.
- 2 Enter the **GMS Server Public IP** address in the text field provided next to **(FQDN/IP[:port])**.
- 3 Click **Update** or **Reset**.

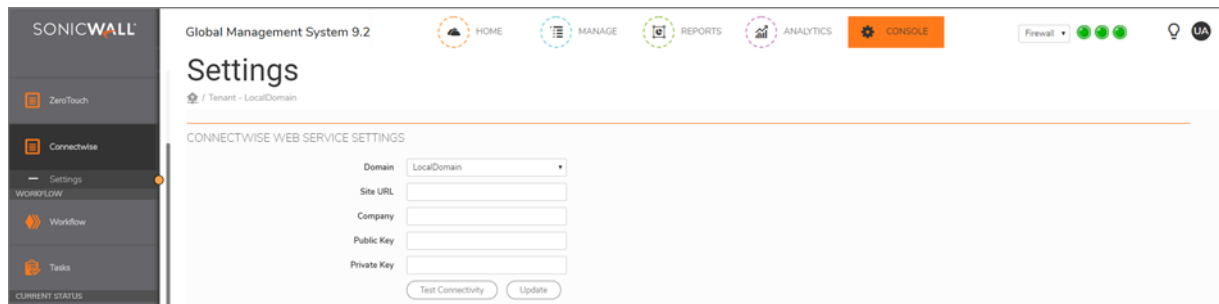
Connectwise

Connectwise is accessible by clicking the **Gear icon**, next to **CONSOLE**, in the top navigation and selecting **Connectwise** in the left-hand command menu. Click on the **Connectwise** command to access the **GMS Connectwise Settings**.

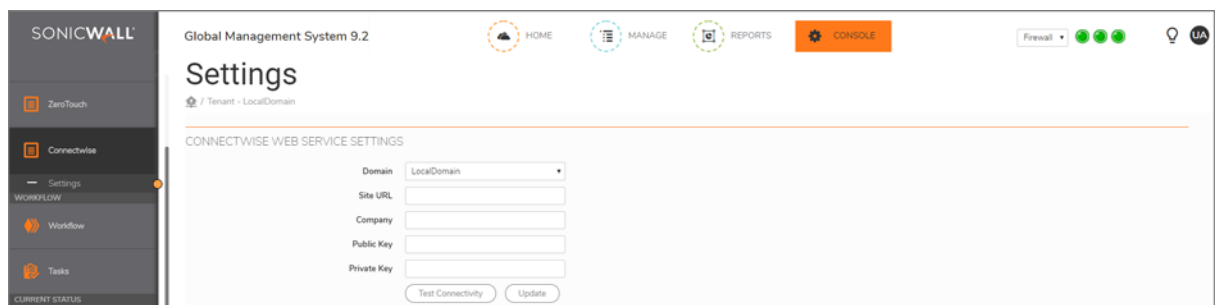
Connectwise helps manage and map all your firewalls by creating a configuration whenever a unit is deleted or created from GMS. You can create GMS-generated alerts automatically in the Connectwise Manage ticketing system. You can track, document, and communicate all open tickets during the correction process until all are resolved and closed.

Connectwise can also send status alerts to the stakeholders using various communication tools until a service tickets is acknowledged or closed. These include email, text messages (SMS), phone calls and even iOS and Android push notifications.

Flow-based GMS Connectwise Settings



Syslog-based GMS Connectwise Settings



To Set Your Connectwise Web Service Settings:

- 1 Enter a **Domain** name in the **LocalDomain** field.
- 2 Enter a **Site URL** in the text field provided.
- 3 Enter a **Company** name in the text field provided.
- 4 Enter a **Public Key**, or RSA in the text field provided.
- 5 Enter a **Private Key**, or your new SSL certificate ID, in the text field provided.
- 6 Click **Test Connectivity** or **Update**.

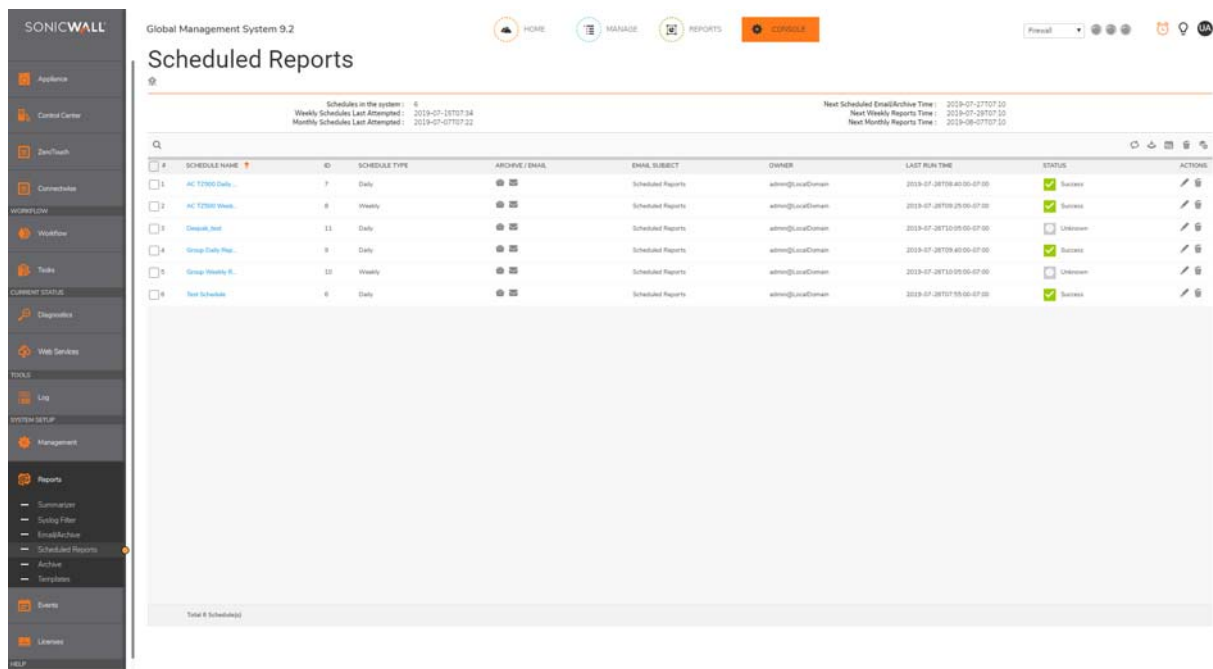
Reports

Reports is accessible by clicking the **Gear icon**, next to **CONSOLE**, in the top navigation and selecting **Reports** in the left-hand command menu. For **Flow** reports, click on the **Reports** command to access **Email/Archive**, **Scheduled Reports**, **Archive**, and **Templates**. For **Syslog** reports, click on the Reports command to access **Summarizer**, **Syslog Filter**, **Email/Archive**, **Scheduled Reports**, **Archive**, and **Templates**.

Scheduled Reports

To create Scheduled Reports for Flow-based and Syslog-based reporting:

- 1 Go to **CONSOLE | Reports > Scheduled Reports**.
- 2 Click on the plus icon at the top right of the Scheduled Reports table.



The **CREATE SCHEDULE** dialog displays for the **SCHEDULE INFO** step 1.

- 3 Under the **TASK INFO** section, enter the **Schedule Name** in the text field provided and choose the **Schedule Interval** and **Report Type** you want.
- 4 Check whether you want the report via **Email** or if you want to **Archive** it.
- 5 Under the **FORMAT/SETTINGS** section, choose whether you want your **Report Format** as **PDF** or **XML**.
- 6 Check whether you want a **Zip Report** and a **Password protect**.
- 7 Click **Next** to continue to the additional **CREATE SCHEDULE** steps 2 (**SELECT UNITS**), 3 (**SELECT REPORTS**), 4 (**SELECT COVER LOGO**), 5 (**PERMISSION SETTINGS**), and 6 (**REVIEW**).

NOTE: GMS 9.2 schedule creation user interface supports only one unit per schedule (new schedules). Schedules created with multiple units in GMS 9.1 are still supported.

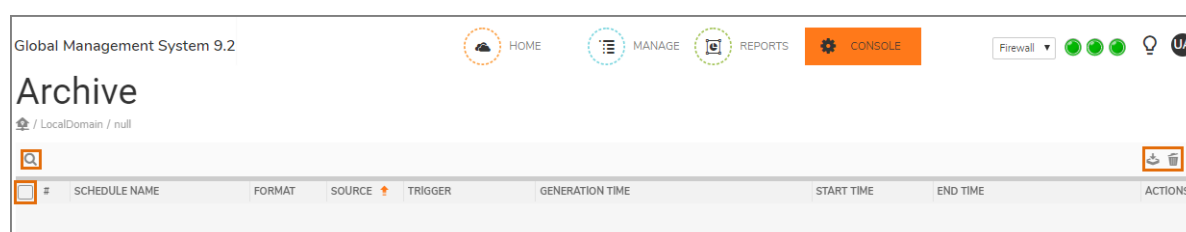
Archive

You can save your reports to an **Archive** and you can see them in the Archive table. Each archived report has some important identifying information, which you can see under the Archive table columns, which are: **SCHEDULE NAME**, **FORMAT**, **SOURCE**, **TRIGGER**, **GENERATION TIME**, **START TIME**, **END TIME**, and **ACTIONS**. The table is the same for flow and syslog reports.

Click on the column names to make the orange up-arrow appear next to them. You can then sort the items in each column and drag to relocate the columns.

You can download and delete one or more Archive reports by selecting multiple rows and clicking the check box on the left of the table and the icons at the top right of the table.

You can also search the Archive by clicking the **search icon** on the top left of the table and entering the search text in the field provided.



Global Management System 9.2

HOME MANAGE REPORTS CONSOLE

Firewall

Archive

/ LocalDomain / null

Search icon

#	SCHEDULE NAME	FORMAT	SOURCE	TRIGGER	GENERATION TIME	START TIME	END TIME	ACTIONS
---	---------------	--------	--------	---------	-----------------	------------	----------	---------

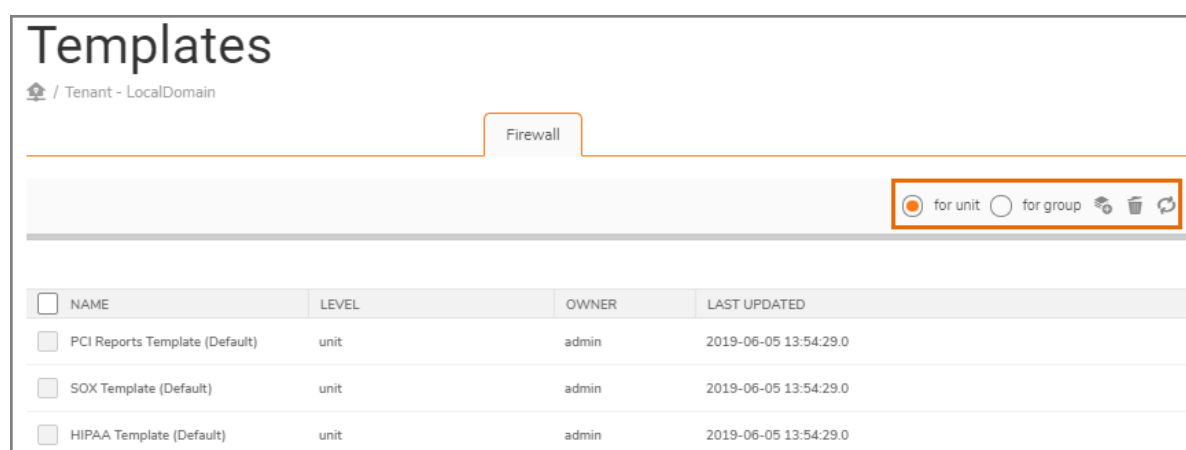
Templates

Templates help you configure the settings that allow firewalls to operate on the network. Templates are the building blocks to configure the network and the device. You can use templates to define interface and zone configurations, to manage the server profiles for log in, flow and syslog access, or to define VPN configurations.

You can create a template for a unit firewall or for a group of firewalls. And three templates are provided at the unit and group level in the Templates table. The templates are **PCI Reports Template (Default)**, **SOX Template (Default)**, and **HIPAA Template (Default)**.

Each template has important identifying information, which you can see under the Templates table columns, which are: **NAME**, **LEVEL**, **OWNER**, and **LAST UPDATED**. The table is the same for flow and syslog reports.

You can delete or reload one or more templates by selecting multiple rows and clicking the check box on the left of the table and the icons at the top right of the table.



Templates

/ Tenant - LocalDomain

Firewall

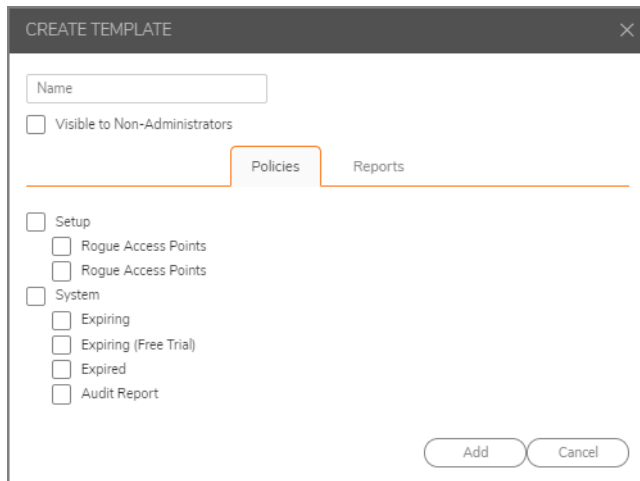
for unit for group

NAME	LEVEL	OWNER	LAST UPDATED
PCI Reports Template (Default)	unit	admin	2019-06-05 13:54:29.0
SOX Template (Default)	unit	admin	2019-06-05 13:54:29.0
HIPAA Template (Default)	unit	admin	2019-06-05 13:54:29.0

To create a template:

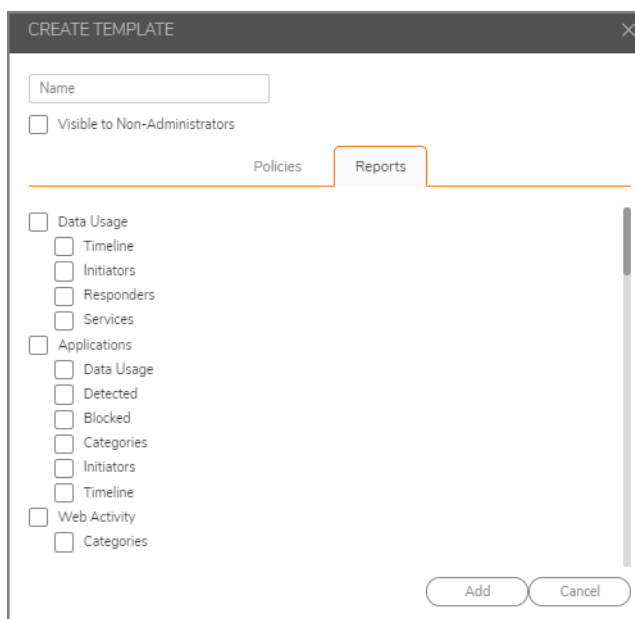
- 1 Click on the radio button **for unit** or **for group** depending on the template you want to create.
- 2 Click on the **Add Template** icon on the top right of the **Templates** table. The **CREATE TEMPLATE** dialog displays for Policies or Reports, depending on the tab you choose.

Template for Policies



The screenshot shows the 'CREATE TEMPLATE' dialog box with the 'Policies' tab selected. At the top, there is a text field for 'Name' and a checkbox for 'Visible to Non-Administrators'. Below these are two tabs: 'Policies' (active) and 'Reports'. Under the 'Policies' tab, there are two main categories: 'Setup' and 'System'. Under 'Setup', there are two sub-items: 'Rogue Access Points' (listed twice). Under 'System', there are five sub-items: 'Expiring', 'Expiring (Free Trial)', 'Expired', and 'Audit Report'. At the bottom right, there are 'Add' and 'Cancel' buttons.

Template for Reports



The screenshot shows the 'CREATE TEMPLATE' dialog box with the 'Reports' tab selected. It has the same top section as the Policies dialog: a 'Name' text field and a 'Visible to Non-Administrators' checkbox. The 'Reports' tab is active, and it contains a scrollable list of report categories. The categories are: 'Data Usage' (with sub-items 'Timeline', 'Initiators', 'Responders', 'Services'), 'Applications' (with sub-items 'Data Usage', 'Detected', 'Blocked', 'Categories', 'Initiators', 'Timeline'), and 'Web Activity' (with sub-item 'Categories'). At the bottom right, there are 'Add' and 'Cancel' buttons.

- 3 Enter the name of your template in the text field provided.
- 4 Check whether you want the template Visible to Non-Administrators.
- 5 Click the **Policies** or **Reports** tab for your template.
- 6 Click **Add**.

Syslog-Based Installations

The **CONSOLE | Appliance > Syslog Agent > Syslog Mount** page lists the drives available on the system. The user can select an external mounted drive to store syslog data. When an external disk is selected, Syslog files, reporting data, backup files, and scheduled reports are saved in an external disk.

Mounting an external disk is mandatory in 40 GB installations. In 40 GB installations, Syslog-related services are turned off until the external mount is selected.

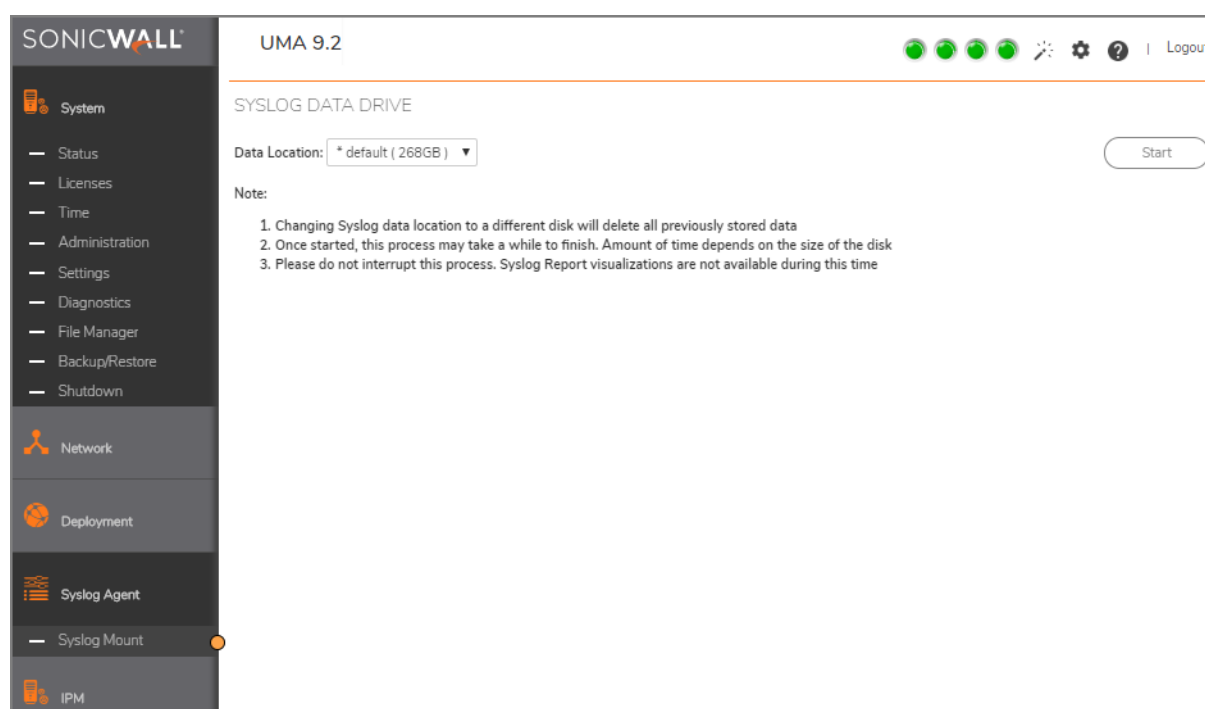
NOTE: Changing Syslog data location to a different disk deletes all previously stored data. Once started, this process may take a while to finish. The amount of time depends on the size of the disk. Do not interrupt this process. Syslog Report visualizations are not available during this time.

To mount an external hard drive:

- 1 Go to **CONSOLE | Appliance > Syslog Agent > Syslog Mount**.

The **SYSLOG DATA DRIVE** page displays.

- 2 Select the **Data Location** in the text field provided. The default is (268GB).
- 3 Click **Start**.



SonicWall Support

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

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to <https://www.sonicwall.com/support>.

The Support Portal enables you to:

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

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

About This Document

Legend



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



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



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

SonicWall® Global Management System Getting Started Guide
Updated - October 2019
Software Version - 9.2
232-005117-00 Rev A

Copyright © 2019 SonicWall Inc. All rights reserved.

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

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

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

End User Product Agreement

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

Open Source Code

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

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