SonicWall® GMS 9.1

Getting Started Guide

SONICWALL®

Contents

Part 1

Introducing GMS

- Introduction to GMS

1

Introduction to GMS

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

Part 2

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

1

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	• ESXi 6.5 • A CPU greater than quad core level • 16 GB RAM (more is recommended for increased performance) • 250 or 950 GB available disk space (depending on number of devices) • thick provisioning **NOTE:** GMS is not supported as a VMware virtual machine running in a cloud service, such as Amazon Web Services EC2.
Hard Drive	• **Spindle Speed**: 10,000 RPM or higher • **Cache**: 64 MB or higher • **Transfer rate**: 600 MBs or higher • **Average Latency**: 4 microseconds or lower
Java	• Java 8.0 plug-in
Browser	• 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 **NOTE:** Internet Explorer version 10.0 in Metro interfaces of Windows 8 is currently not supported. **NOTE:** When using Internet Explorer, turn off Compatibility Mode when accessing the GMS management interface. **NOTE:** Internet Explorer is not supported for Angular-based flow reports.

Network	• access to the Internet
	• either:
	  • an IP address automatically assigned through DHCP
	  • a static IP address

SonicWall Appliance and Firmware	• 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 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 will be installing 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 IP address or host name of your Simple Mail Transfer Protocol (SMTP) server. For example, mail.emailprovider.com.	
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.	

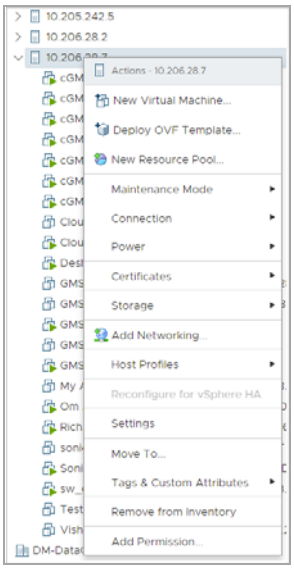
2

Installing the GMS OVA File

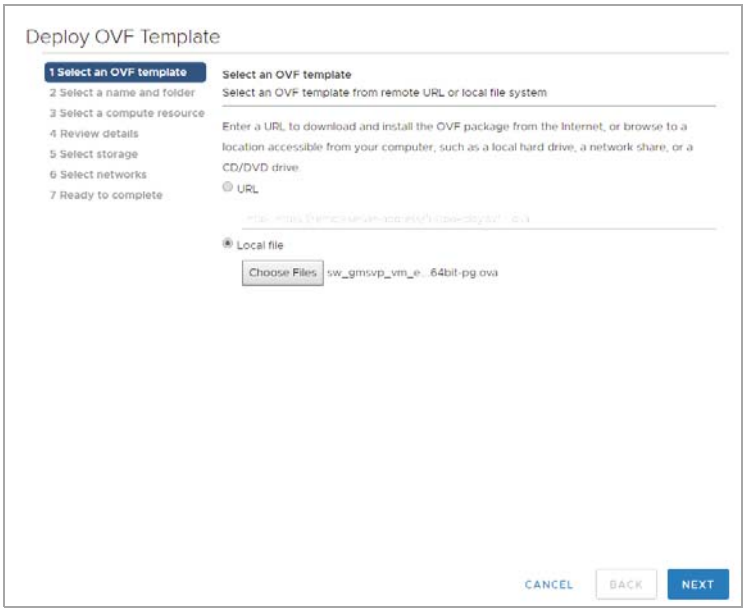
Before installing the SonicWall Global Management System, please read Before You Begin for the system requirements and other useful information.

To install GMS:

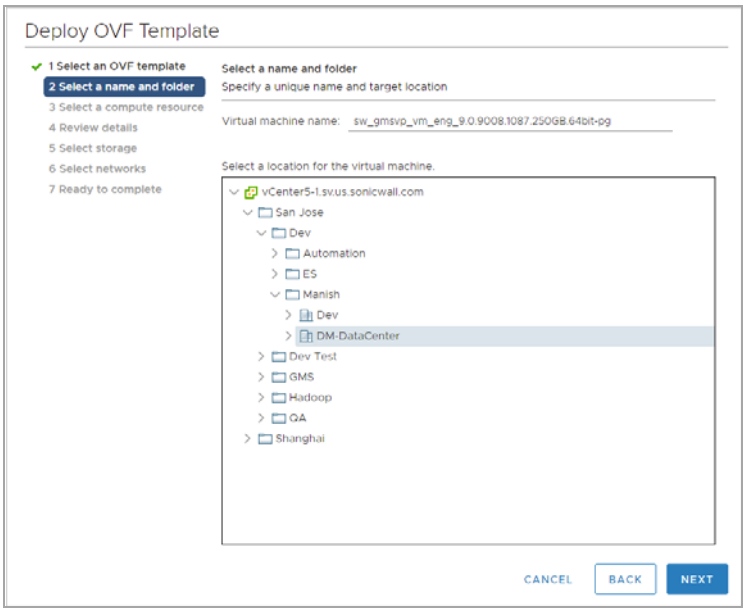
1 Select the ESXi server on which you want to deploy the virtual machine that will run GMS.



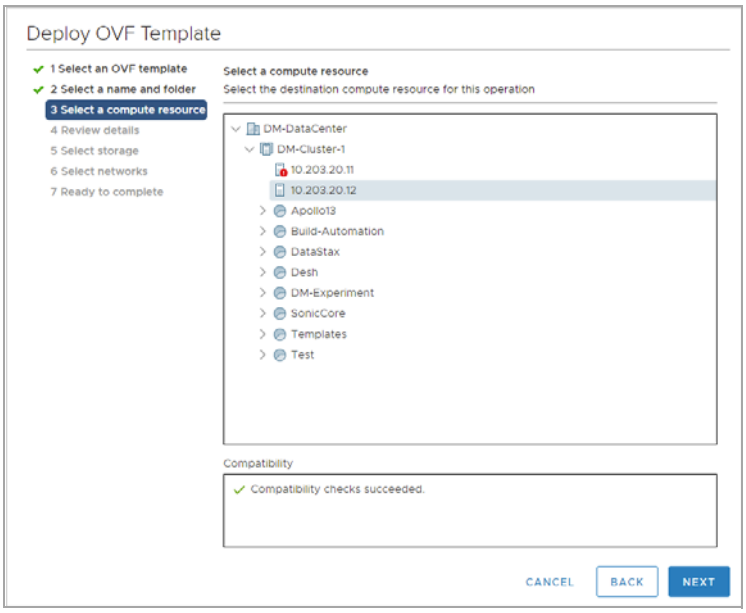
2 Choose the .ova file you want to install in the location where it is stored and click **Next**.



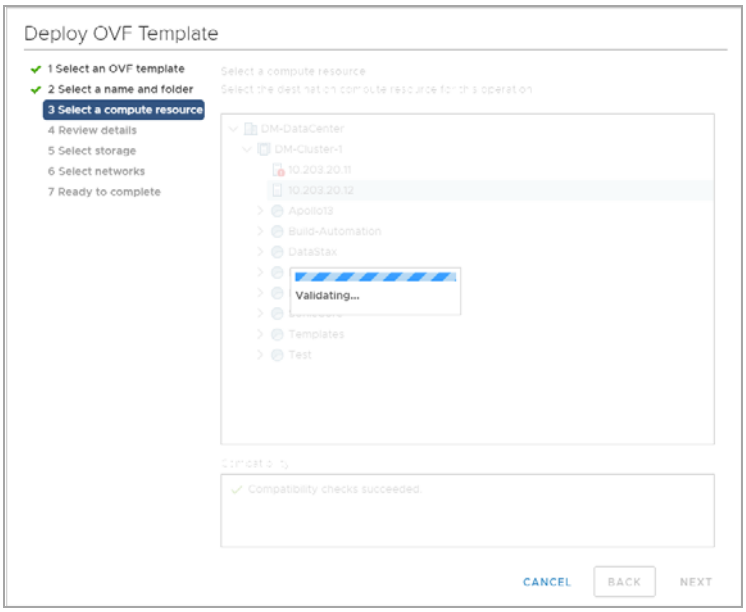
3 Change the name of the virtual machine and select the datastore.



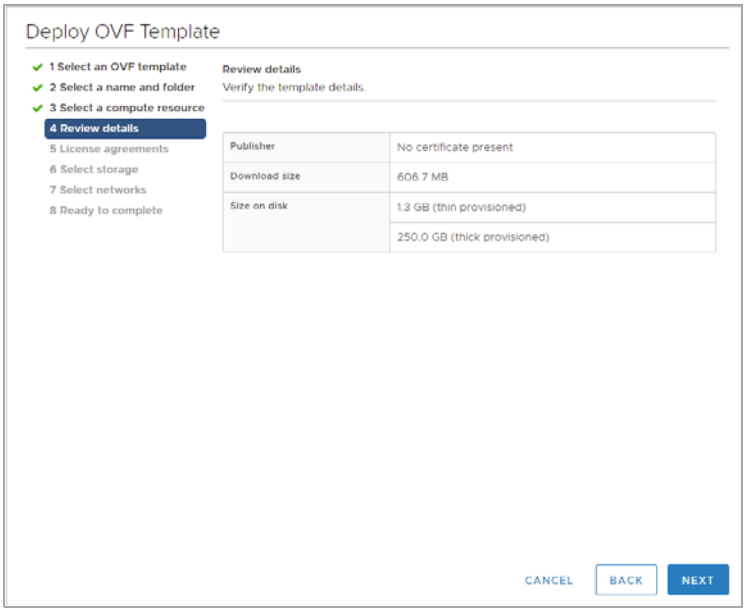
4 Select the ESXi resource to be used and click **Next**.



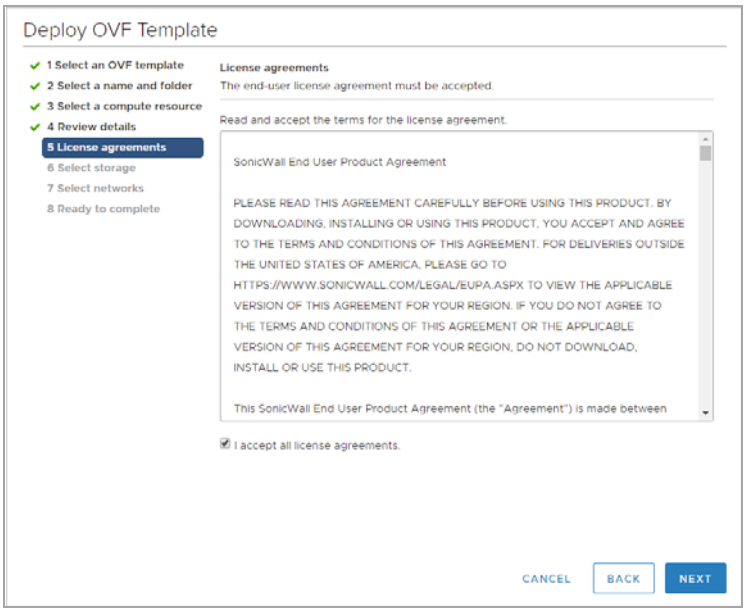
5 The .ova file you chose will be validated. When the validation has been completed and is successful, click **Next**.



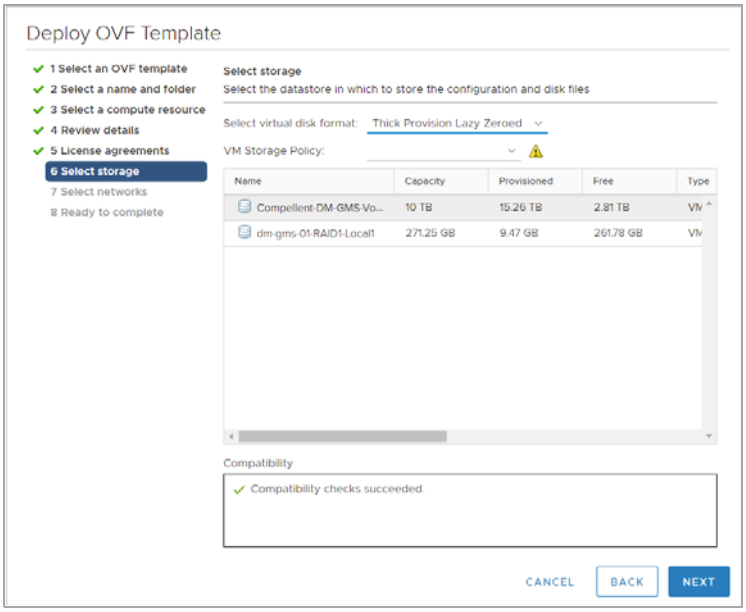
6 Verify the template details for your installation and click **Next**.



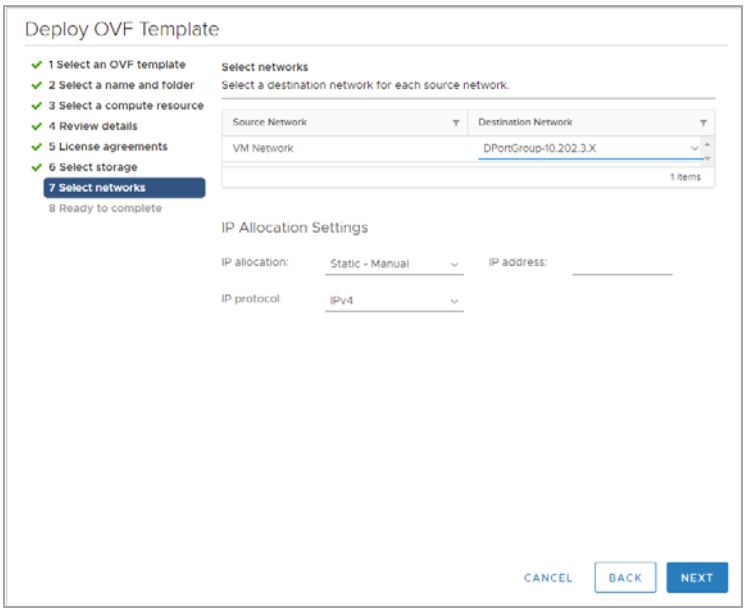
7 Agree to the license agreement by clicking **Next**.



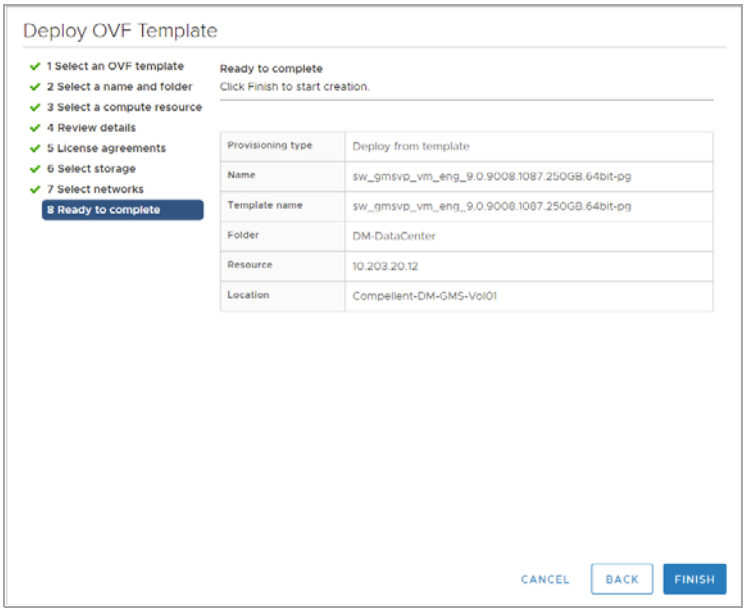
8 Choose the datastore, virtual disk format, and virtual machine storage policy to be used and click **Next**. These will be checked for compatibility with SonicWall GMS.



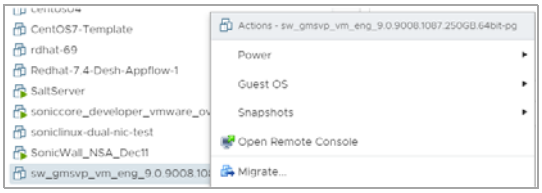
9 Select the network interface to be assigned to the virtual machine. You can use the IP allocation settings default values unless your local network configuration requires custom settings.



10 Click Finish to complete the installation of GMS from the `.ova` file. A progress bar displays showing the status of the installation completion.



11 Select the instance of the virtual machine and power it on.



The installation of your GMS is now completed. Next, you will need to configure the network settings for your GMS. See Setting Up the Network Configuration for more information.

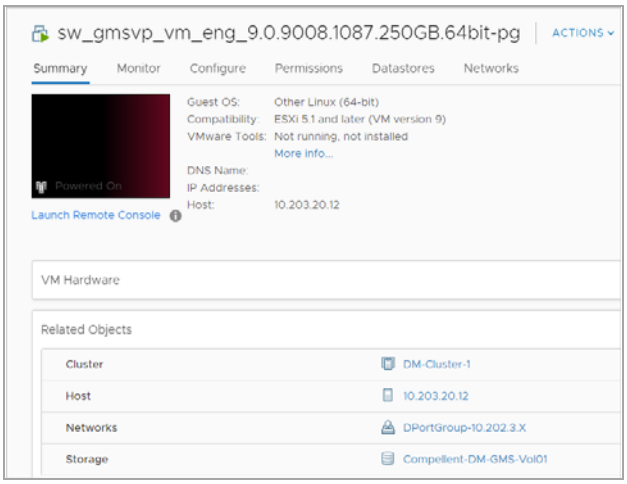
3

Setting Up the Network Configuration

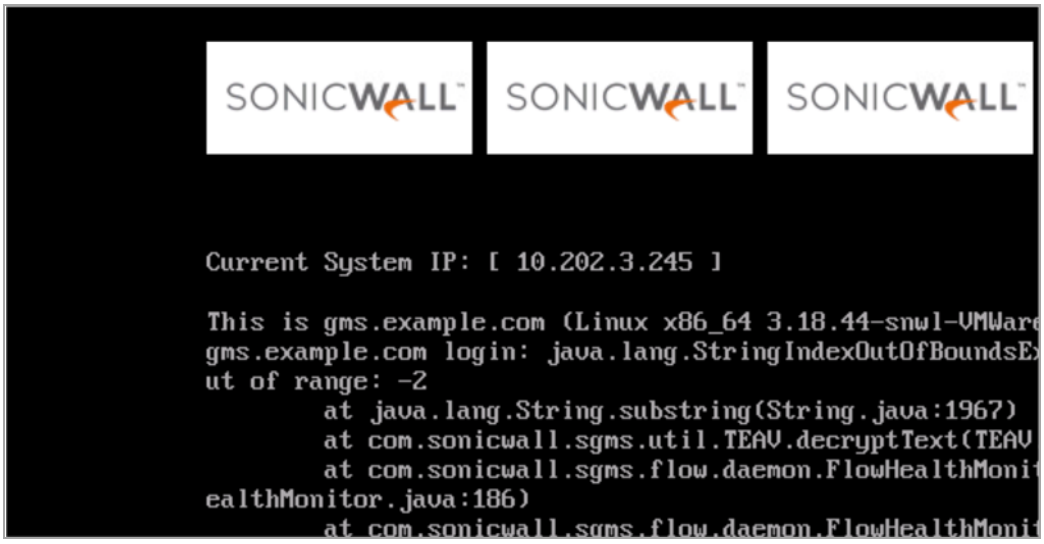
After installing GMS, you will need to configure its network settings.

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 will be automatically assigned to the virtual machine

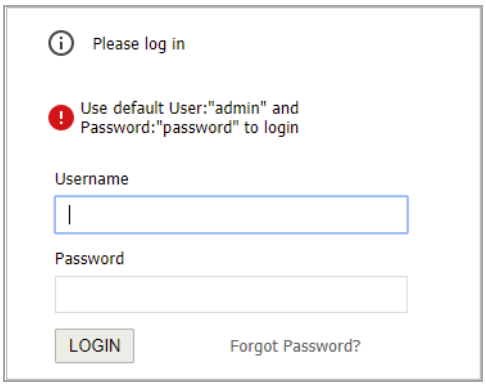


NOTE: If a DHCP server is not present, you will need to use the command-line interface to manually assign an IP address to the virtual machine.

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`



4

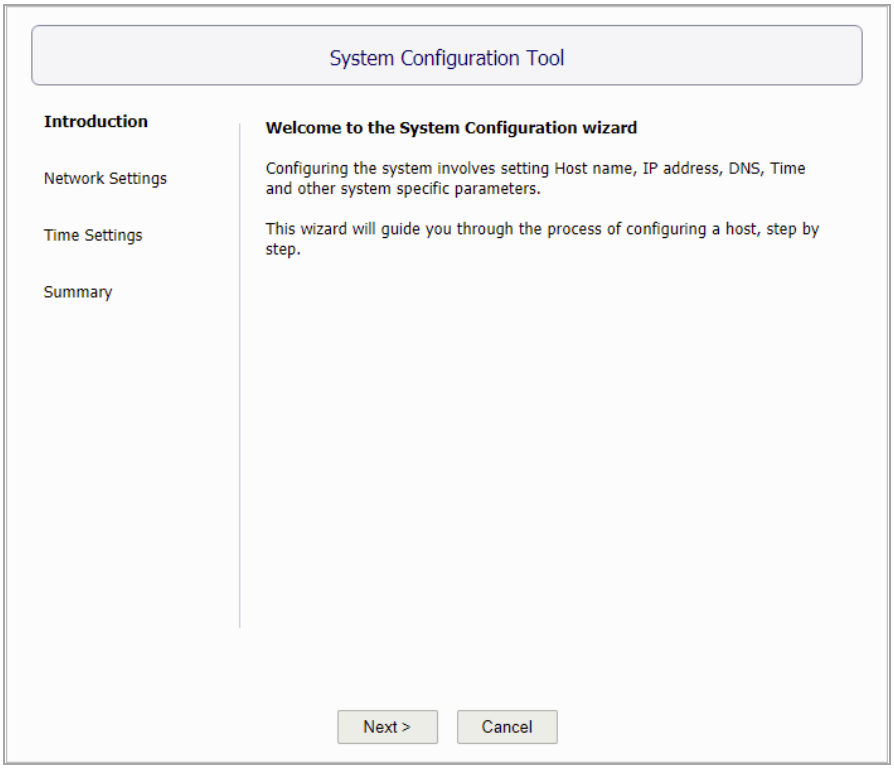
Configuring the System

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.

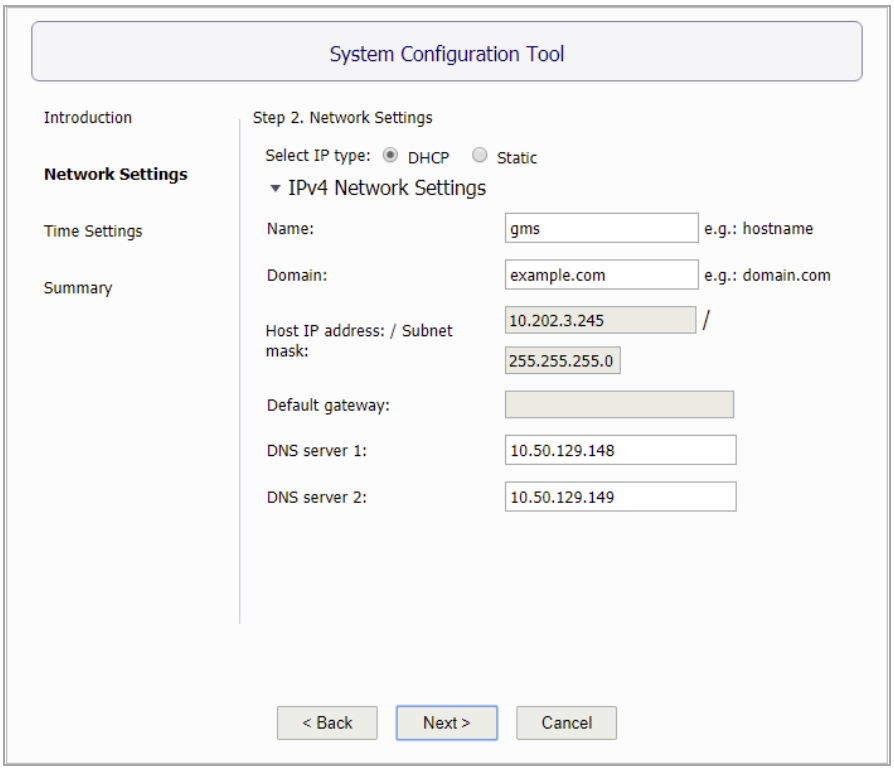
The first page of the System Configuration Tool displays.



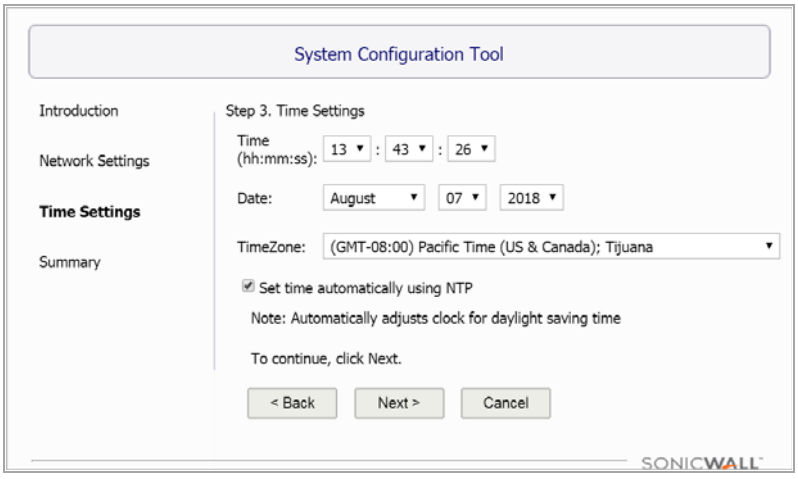
2 Click **Next** to proceed with the configuration.

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

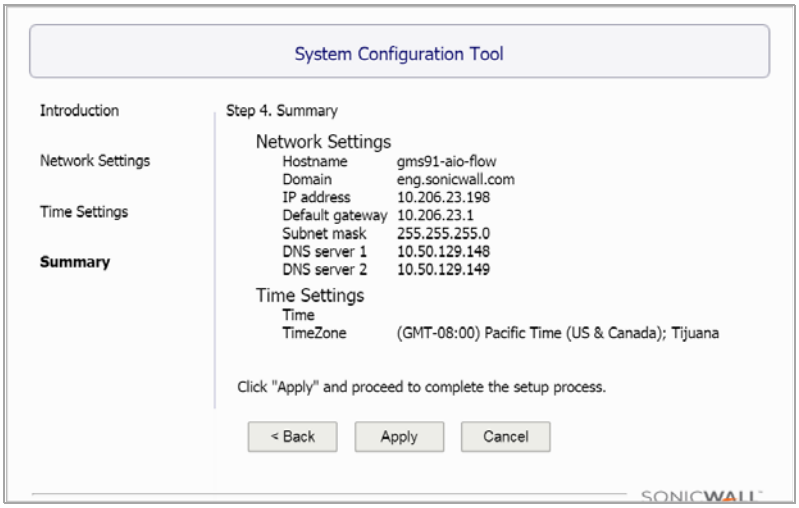
gateway are automatically populated by the DHCP server. You can opt to select the “Static” radio button to configure a static Host IP address / Subnet mask and the Default gateway address. Click **Next**.



4 If necessary, update the **Time**, **Date**, and **TimeZone** for your GMS installation and click **Next**.



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



- If no changes are required, you can 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**.

  The virtual machine might reboot after you apply your configuration settings. If it does, you will need to enter your username and password again in order 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 18

2 Configure Host Settings on the Console on page 19

3 Configure Host Settings on the Appliance Management Interface on page 20

This chapter also contains information on:

- Viewing the Settings Summary on page 21
- Editing The Virtual Machine Settings on page 22

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:

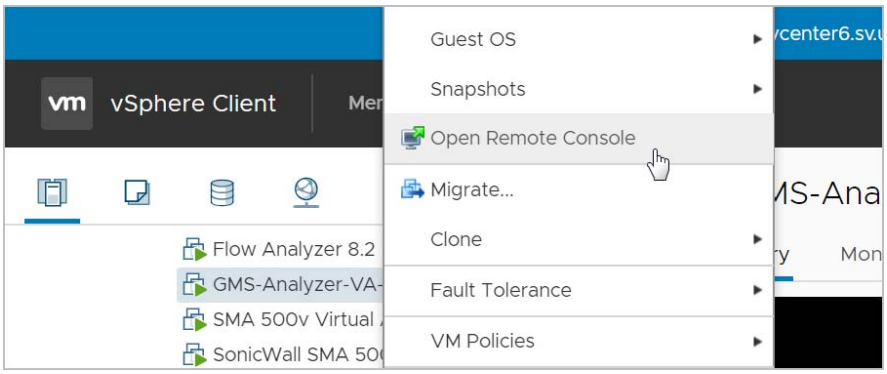
- Right-click the SGMS Virtual Appliance in the left pane and navigate to **Power > Power On** (or **Power > Power Off**) in the right-click menu.
- Select the GMS Virtual Appliance in the left pane and then click **Power on the virtual machine** (or **Shut down the virtual machine**) on the Getting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

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.

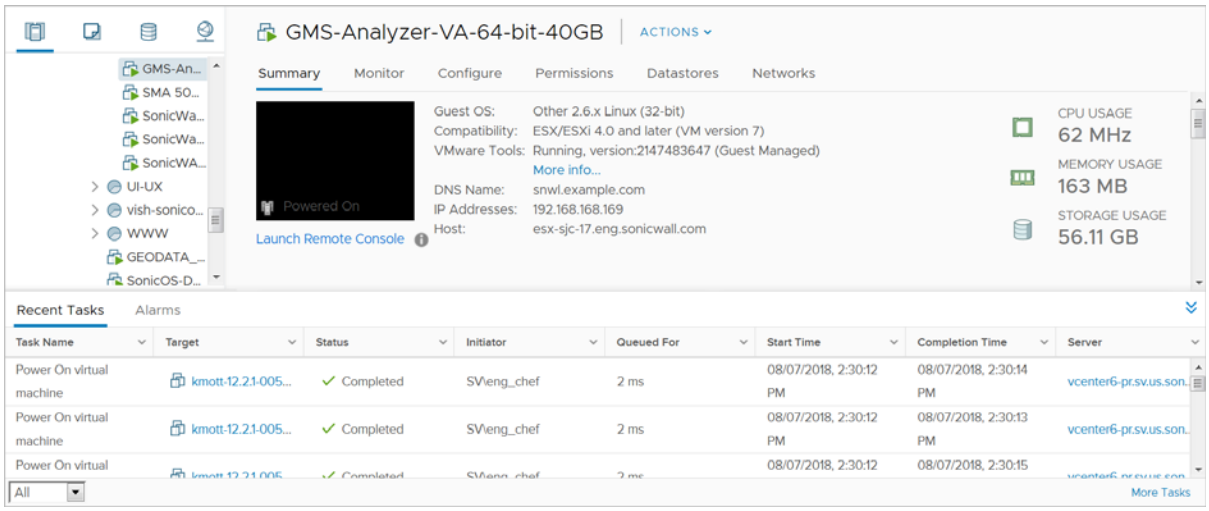
Viewing the Settings Summary

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.

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.

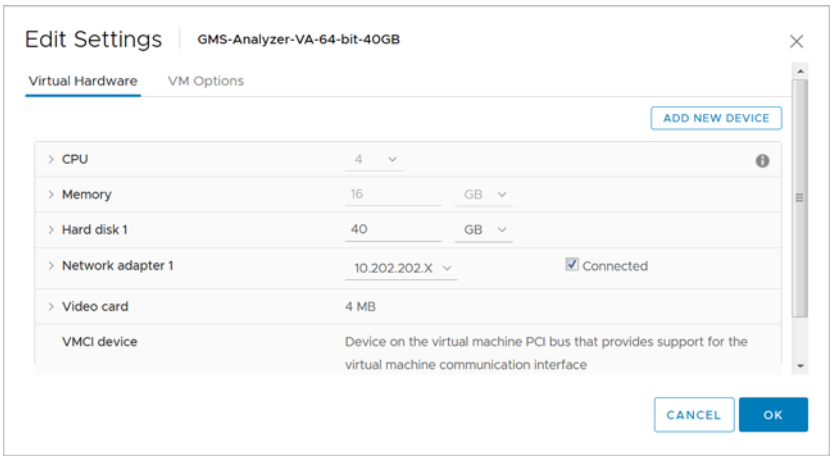


Editing The Virtual Machine Settings

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 E**dit 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**.

5

Setting the Install Mode

The Install Mode wizard allows you to select between a Single Server deployment vs 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.

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

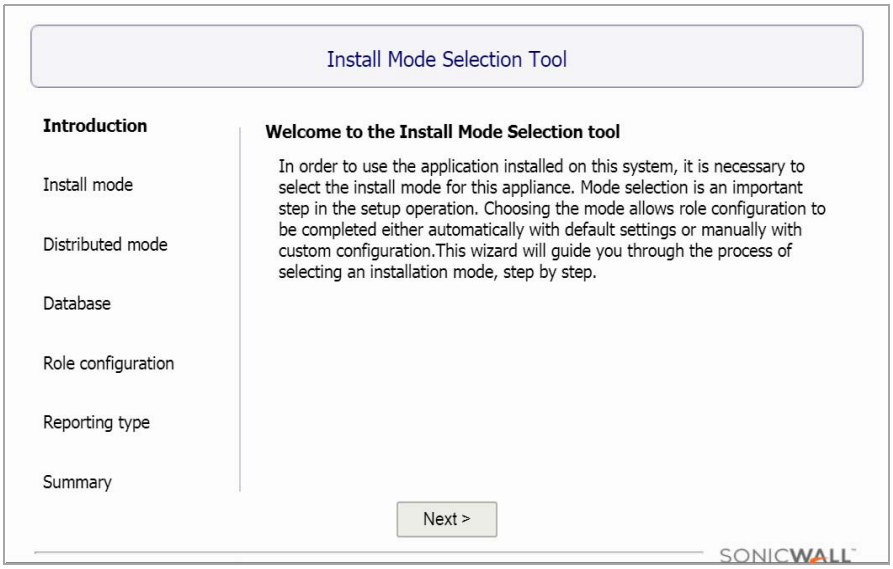
Topics:

Single Server Deployment

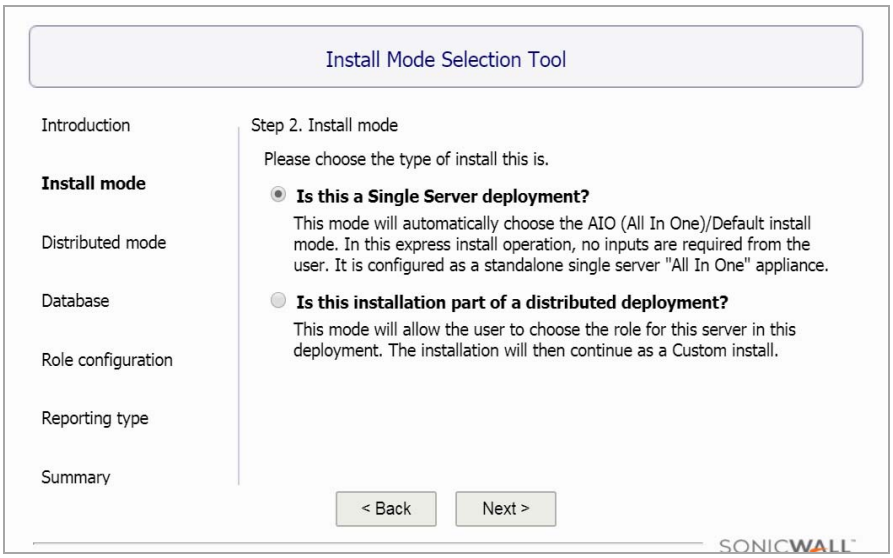
To set the Install mode for a Single Server deployment:

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

The first page of the Install Mode Selection Tool displays.



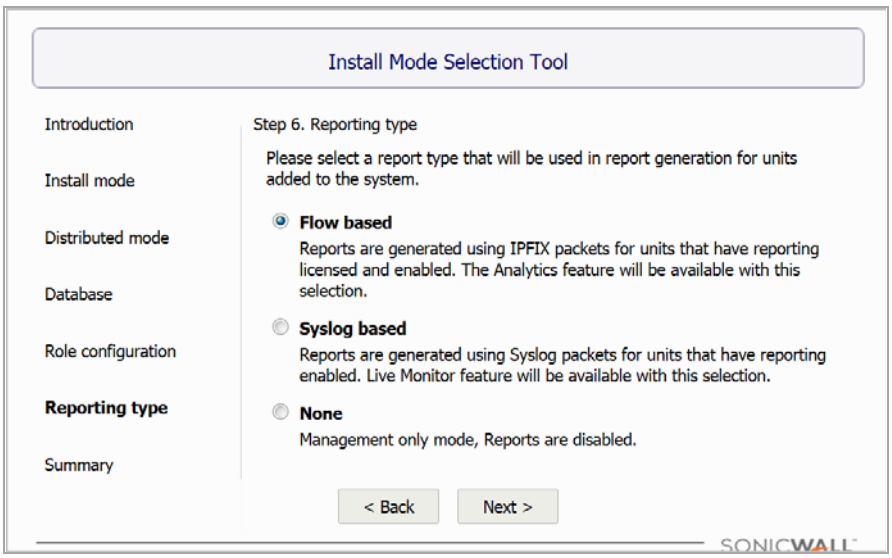
2 Click **Next**. The **Install mode** page of the Install Mode Selection Tool displays.



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

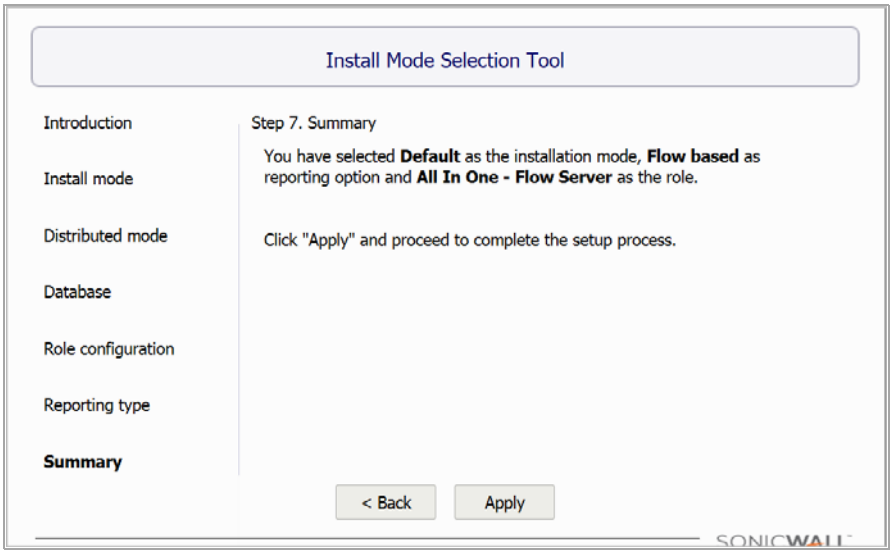
Installation roles (in the configuration files) also vary for these installation modes. These apply to the Primary server in the deployment.

4 Select the **Reporting type** you will use for this deployment.



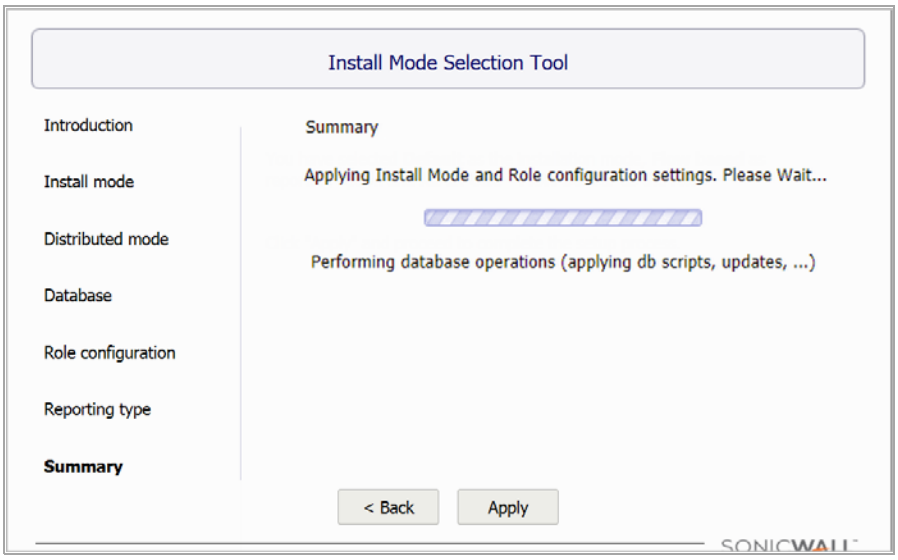
- **Flow based** - this mode includes management plus flow-based (IPFIX) reporting and analytics
- **Syslog based** - this mode includes management plus syslog-based reporting
- **None** - this mode provides management only of the GMS with no reporting

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

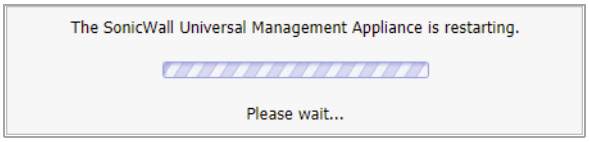


6 Click **Apply**. A status bar displays.

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



7 Click **OK**. The system reboots to complete the installation process.



8 Login into GMS again using the default administration account.

Distributed Deployment

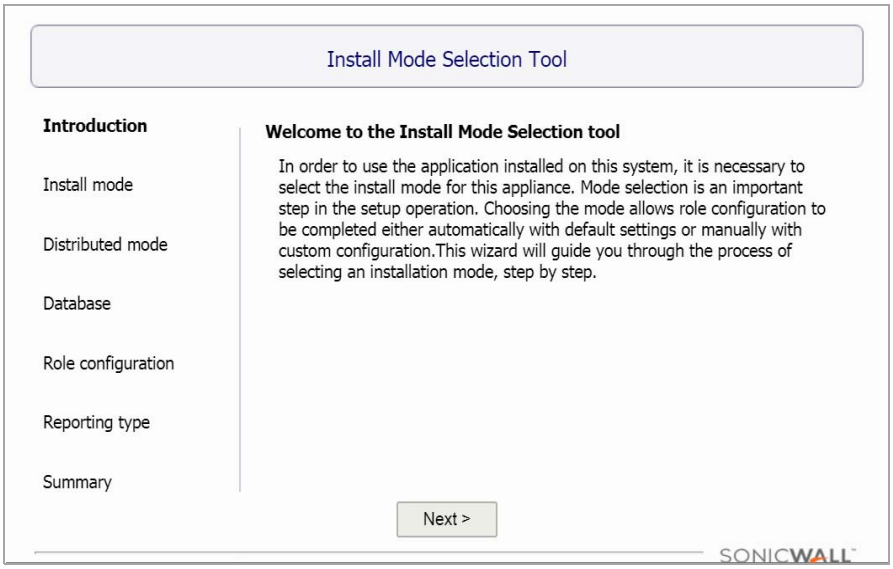
GMS 9.1 supports Ease of Installation for a distributed setup. GMS simplifies the installation process even when multiple servers (instances) are required for a larger deployment. The selection screen for this type of

deployment is applicable to Distributed Mode only. After you have chosen a distributed installation during the Install Mode process, these options appear.

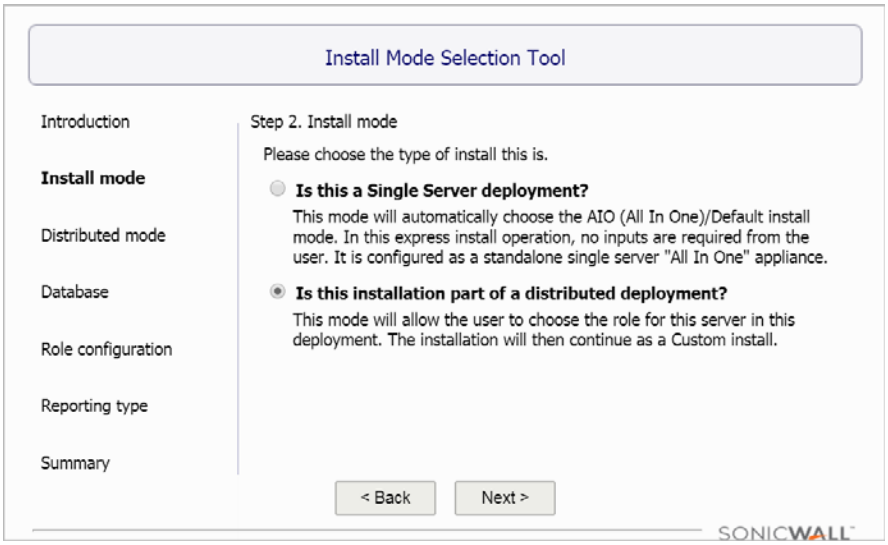
To set the Install mode for a Distributed deployment:

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

The first page of the Install Mode Selection Tool displays.

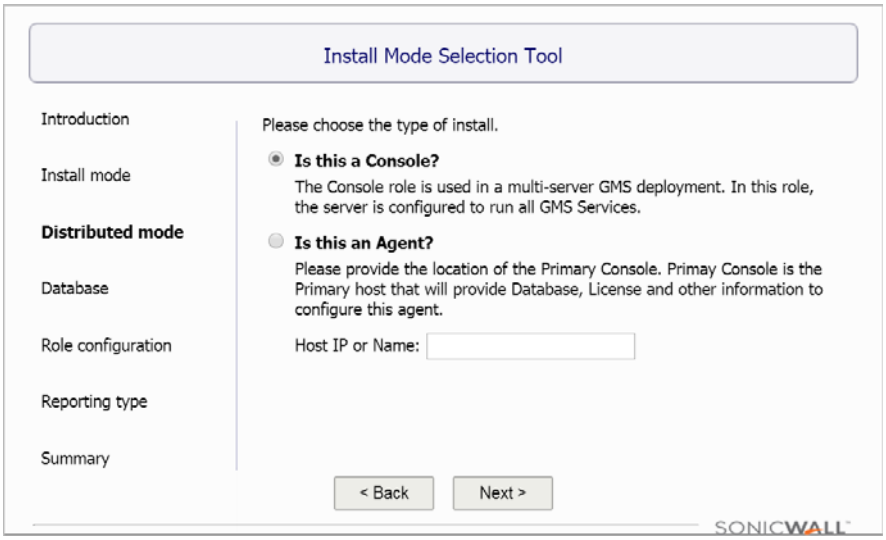


2 Click **Next**. The **Install mode** page of the Install Mode Selection Tool displays.



3 When you are installing for multiple servers as a distributed deployment, choose **Is this installation part of a distributed deployment?** and click **Next.**

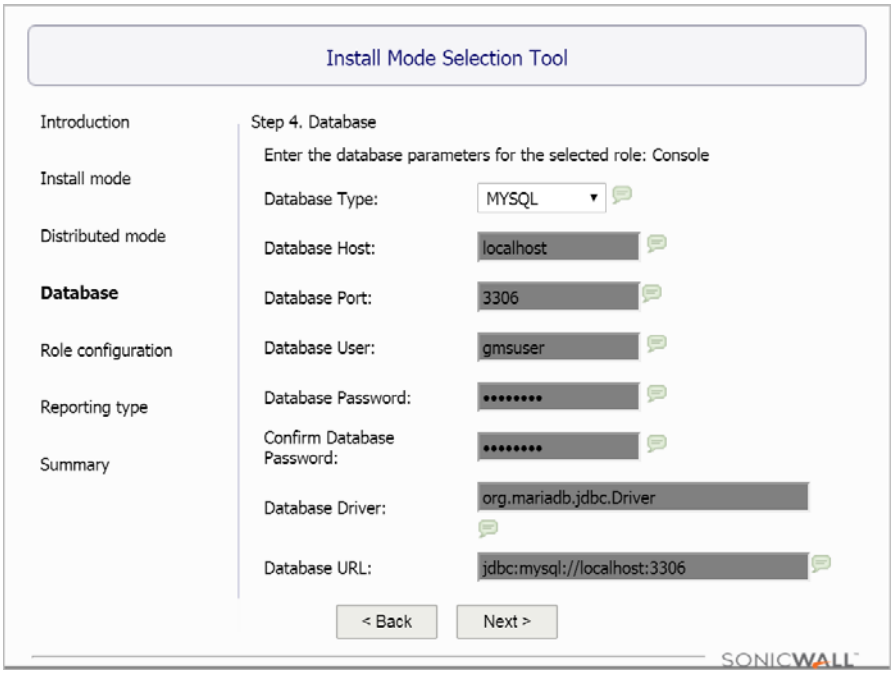
4 Choose the type of Installation, a **Console** or an **Agent**.



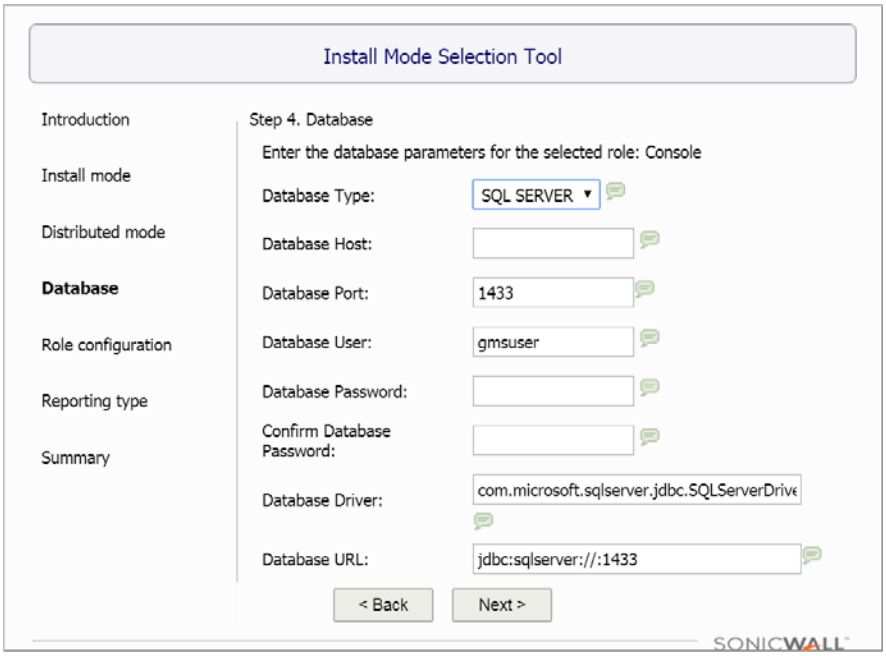
Console Installation

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



SQL Server Database



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.

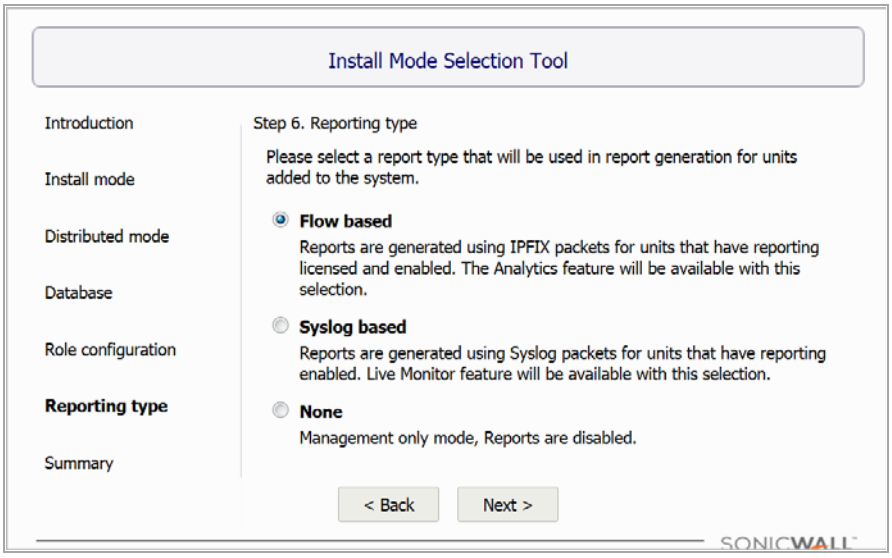
5 Select the **Database User**.

6 Enter and confirm a **Database Password**.

7 The **Database Driver** and **Database URL** should fill automatically.

8 Click **Next**. Missing information will return an error message.

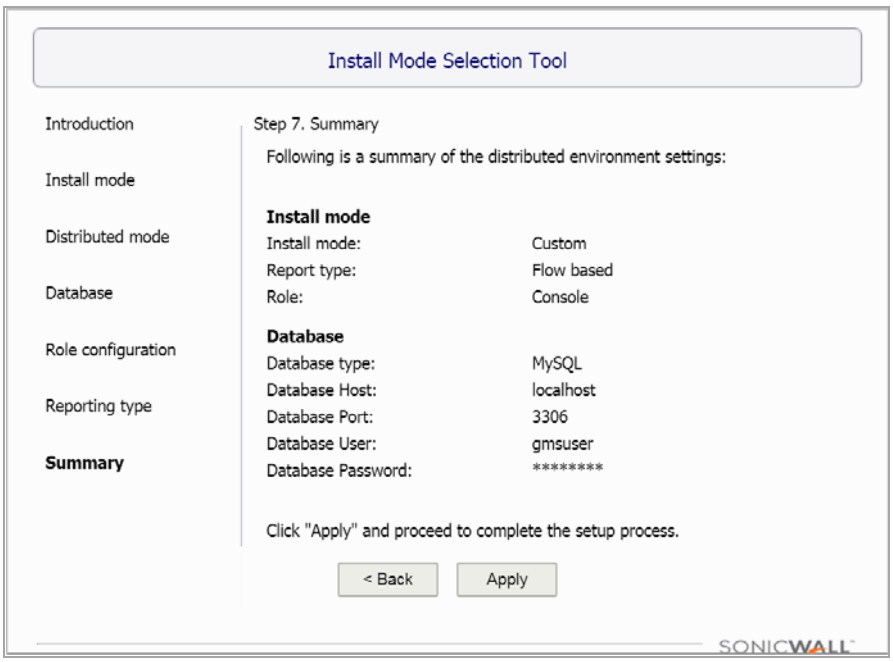
9 Select the **Reporting type** you will use for this GMS.



- **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

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

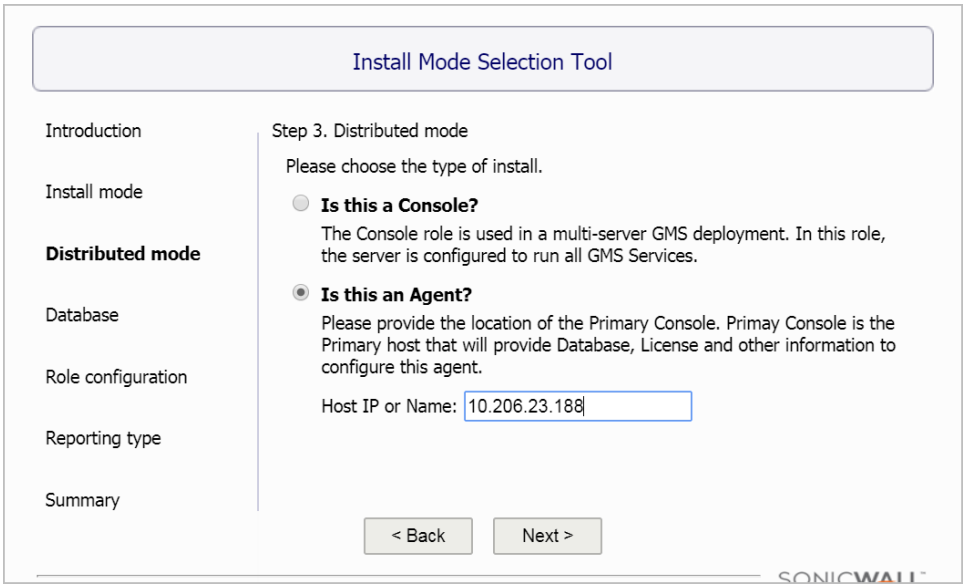


For Console registration information, see Registering GMS.

Agent Installation

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

When installing an agent, pointing to the primary console is all that is necessary. 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.



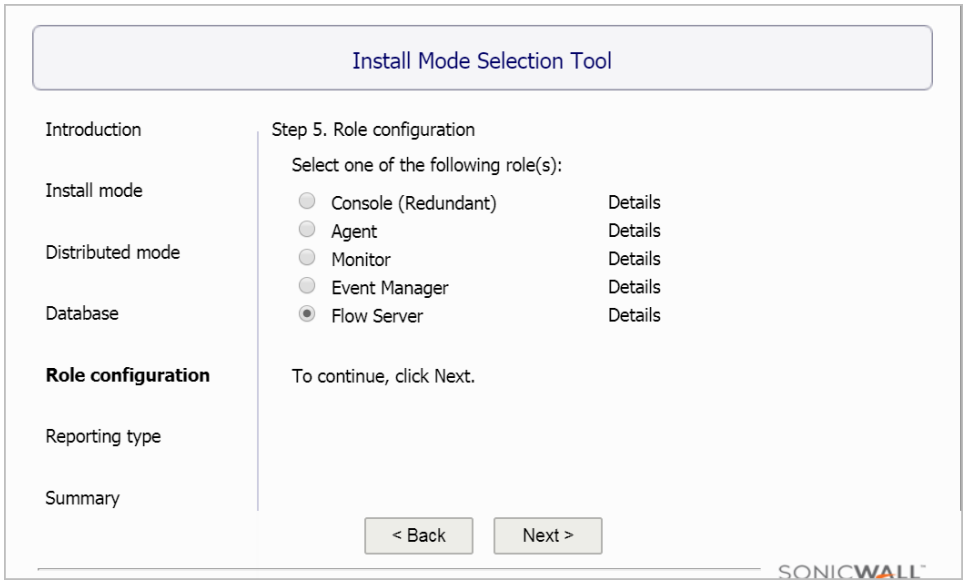
The wizard requests you enter the Host IP/Name of the server that is already setup as a Primary Console. The host being installed then contacts the Primary Console at the specified address to capture additional information to complete the setup. You do not have to re-enter these settings. GMS automatically 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 hostname or IP address 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.

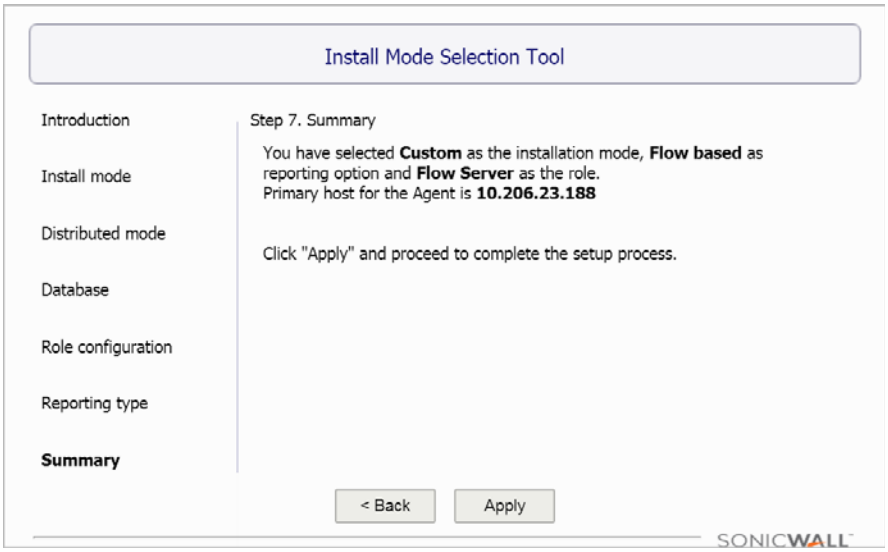


NOTE: The All-In-One option does not appear as a role in this step.

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

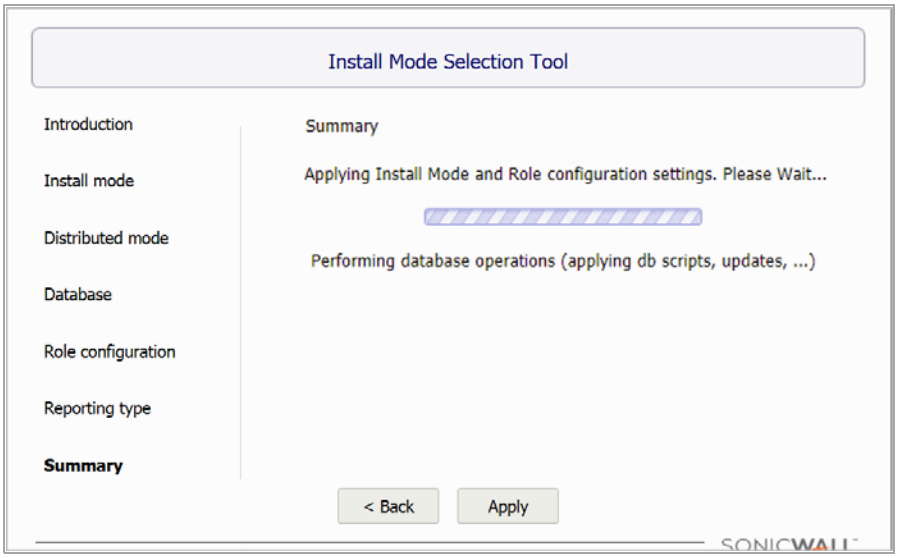
1 Select the desired role for this Agent instance.

2 Click **Next**.

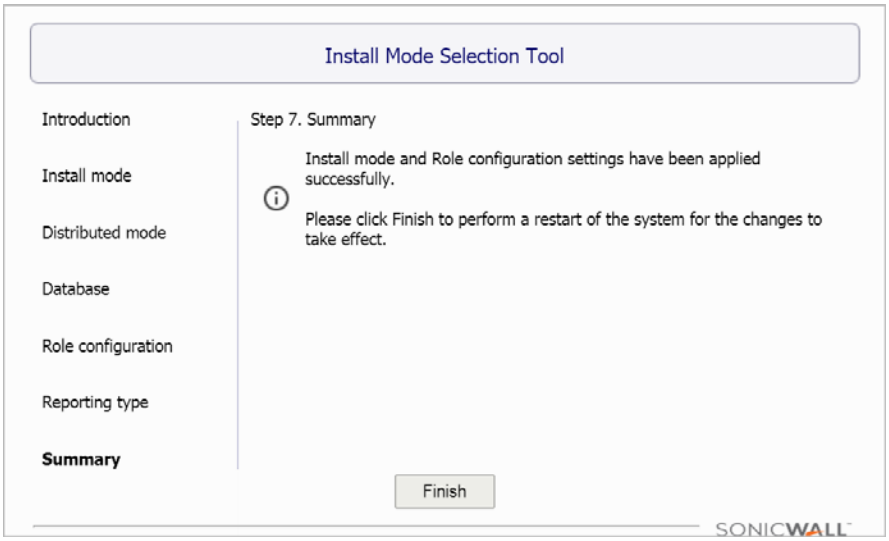


3 Click **Apply**. A status bar displays.

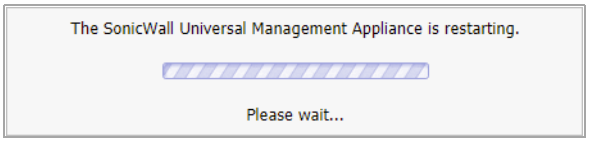
NOTE: The configuration of GMS could take up to 15 minutes to complete.



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



5 The system reboots to complete the installation process.



6 Login into GMS again using the default administration account.

You have completed the configuration of the reporting mode. Next, you will need to configure GMS. See Configuring the System for more information.

Easy Licensing

GMS 9.1 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.

6

Registering GMS

Registration for GMS agents is handled by the Easy Licensing feature introduced in GMS 9.1, 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

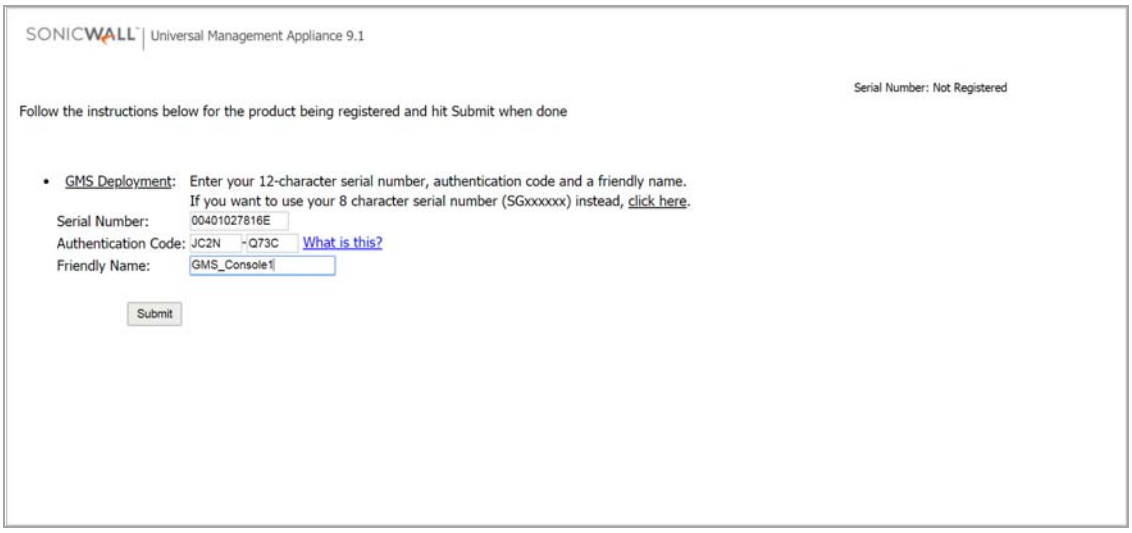
This section guides you through registering your GMS installation.

To register GMS (Console Only):

1 Enter your MySonicWall userid and password.

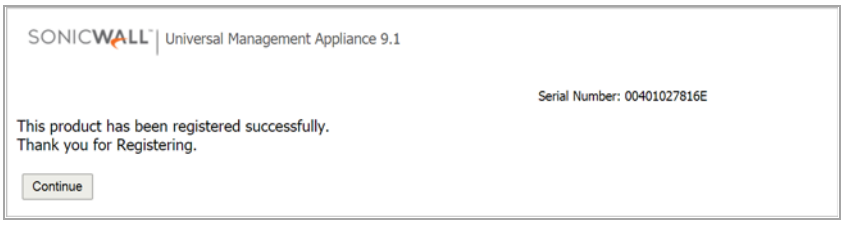
If you do not already have a MySonicWall account, you will need to create one before continuing.

2 Enter your **Serial Number** and **Authentication Code** for this GMS installation from the **Licenses** page and click **Submit**.



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

3 When your GMS is successfully registered, a confirmation message displays.



4 Click **Continue**.

7

Adding Devices

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

GMS support these modes for adding units:

- Basic Mode
- Advanced Mode

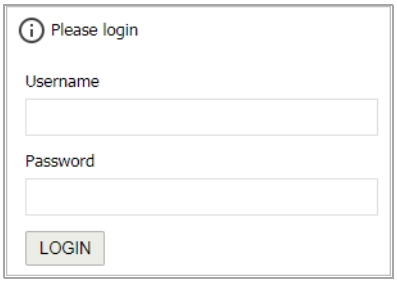
Basic Mode

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.

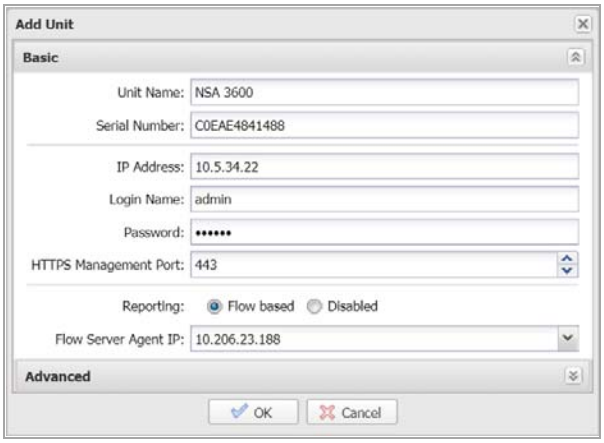
NOTE: You do not need to change any settings on the appliance itself in order to add it to GMS.

To add units to GMS in Basic mode:

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



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



3 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.)

4 If GMS was installed with a reporting mode, but you do not want reporting for this device, select **Disabled** for **Reporting**.

5 Enter the **Flow Server Agent IP** address.

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

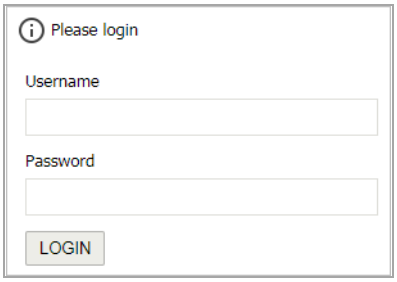
7 When the device has been successfully acquired, you can begin managing it through GMS.

Advanced Mode

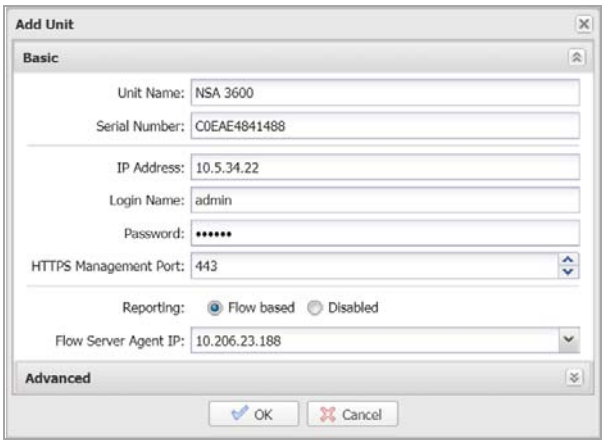
Advanced mode provides a more customized process for adding devices to GMS.

To add units to GMS in Advanced mode:

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



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



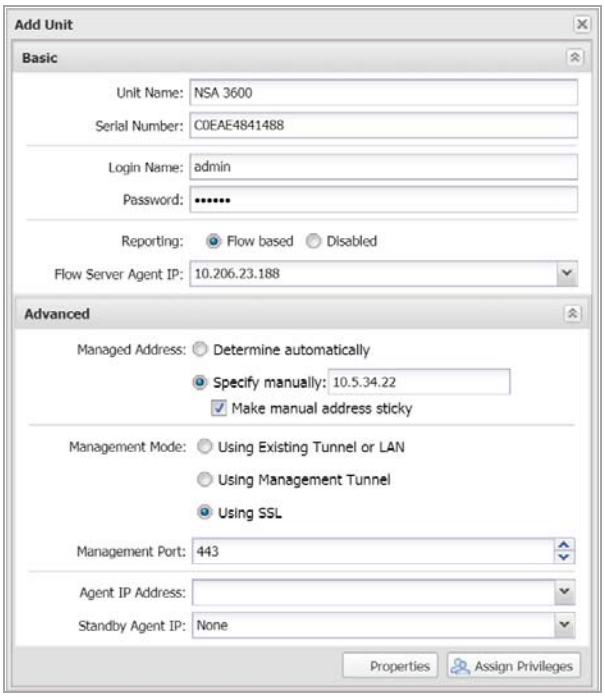
3 Enter the basic information about the device you are adding to GMS:

- 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.)

4 If GMS was installed with a reporting mode, but you do not want reporting for this device, select **Disabled** for **Reporting**.

5 Enter the **Flow Server Agent IP** address.

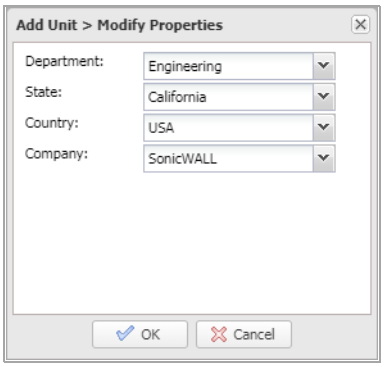
6 Click the double down arrows to the right of the **Advanced** heading. Additional installation options become visible.



7 Enter the advanced information about the device you are adding to GMS:

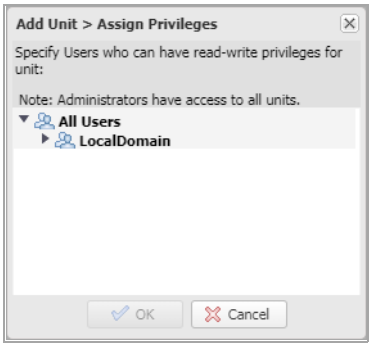
- Managed Address
- Management Mode
- Management Port
- Agent IP Address
- Standby Agent IP

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

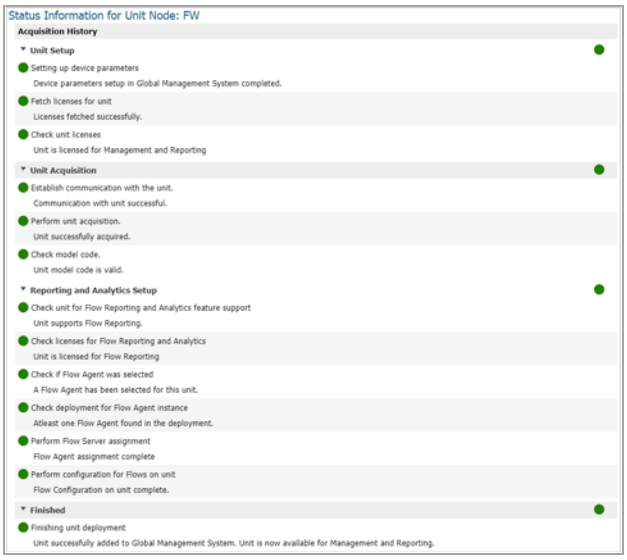


- Department
- State
- Country
- Company

9 Click the **Assign Privileges** button to assign specific access privileges to the device.



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



11 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 GMS for more information.

Part 3

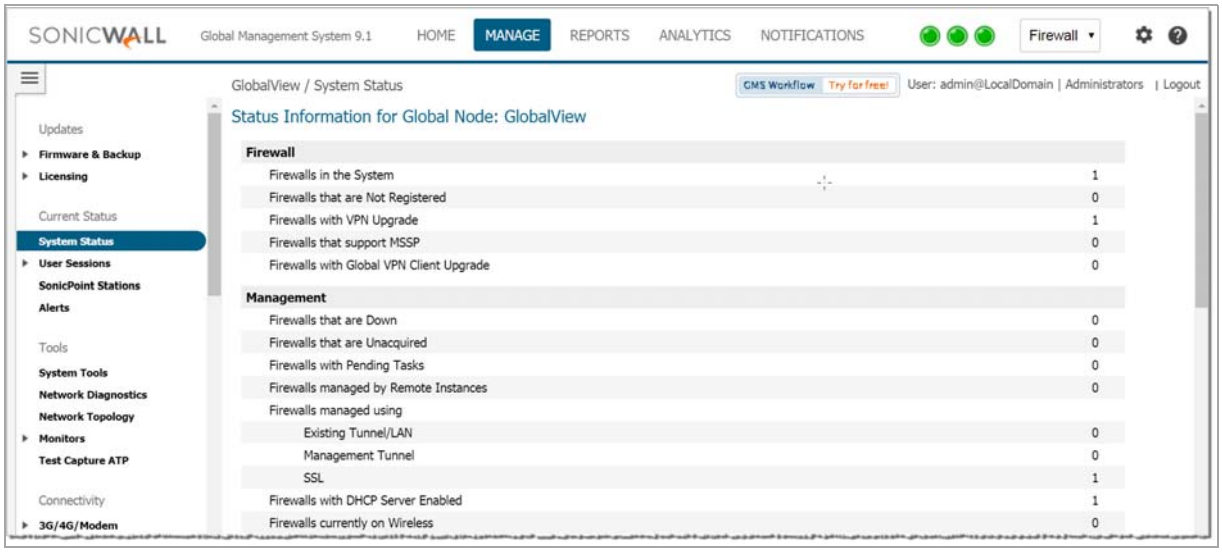
Using GMS

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

8

Using the GMS Management Interface

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



Topics:

- Centralized Management and Monitoring
- Distributed Intelligent Platform Monitoring
- Navigating the GMS Management Interface
- Console View
- Understanding GMS Icons

Centralized Management and Monitoring

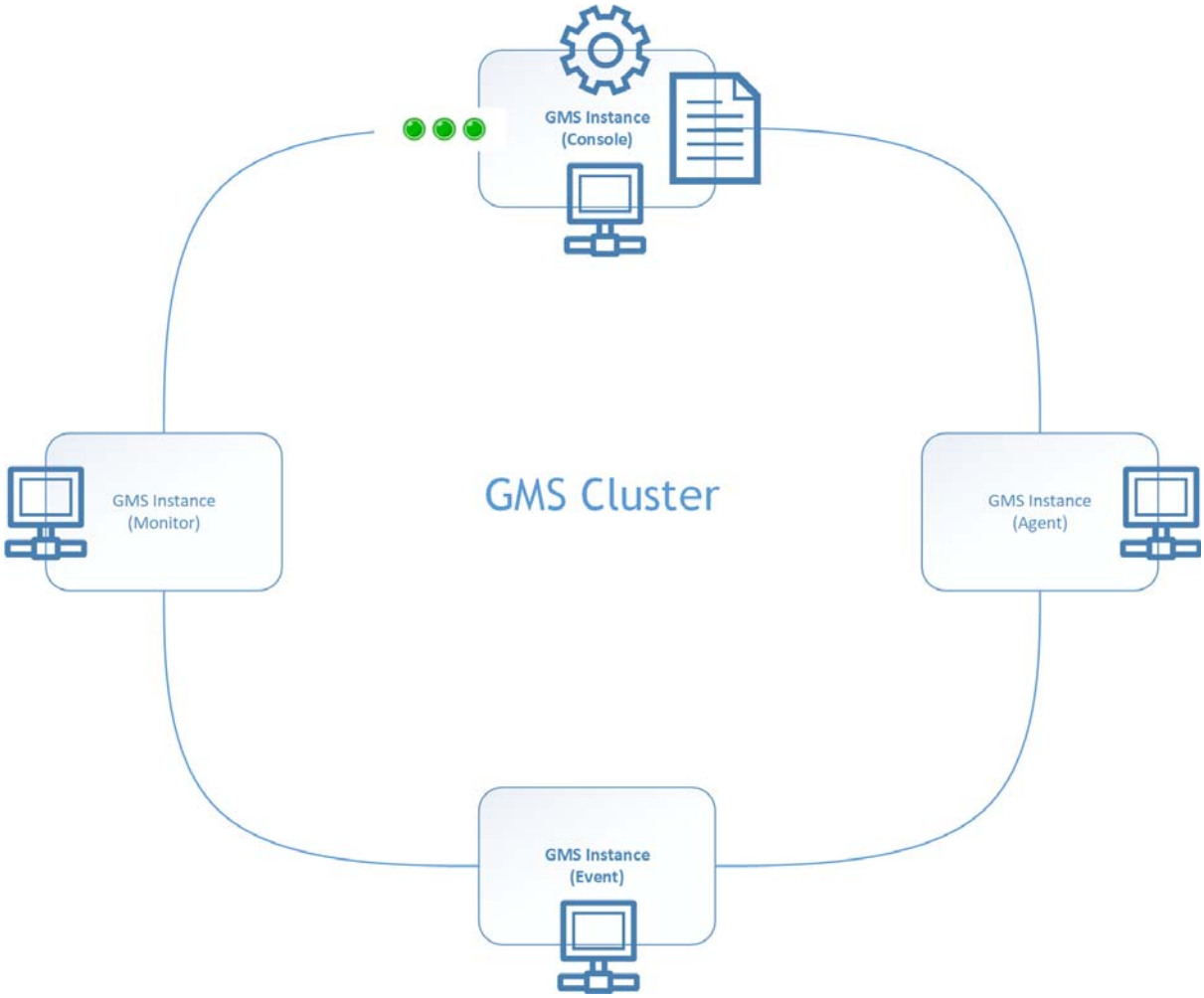
Topics:

- Centralized Management Control Center

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 in order to scale accurately. Previously, each GMS instance provided a UMH interface in order 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.

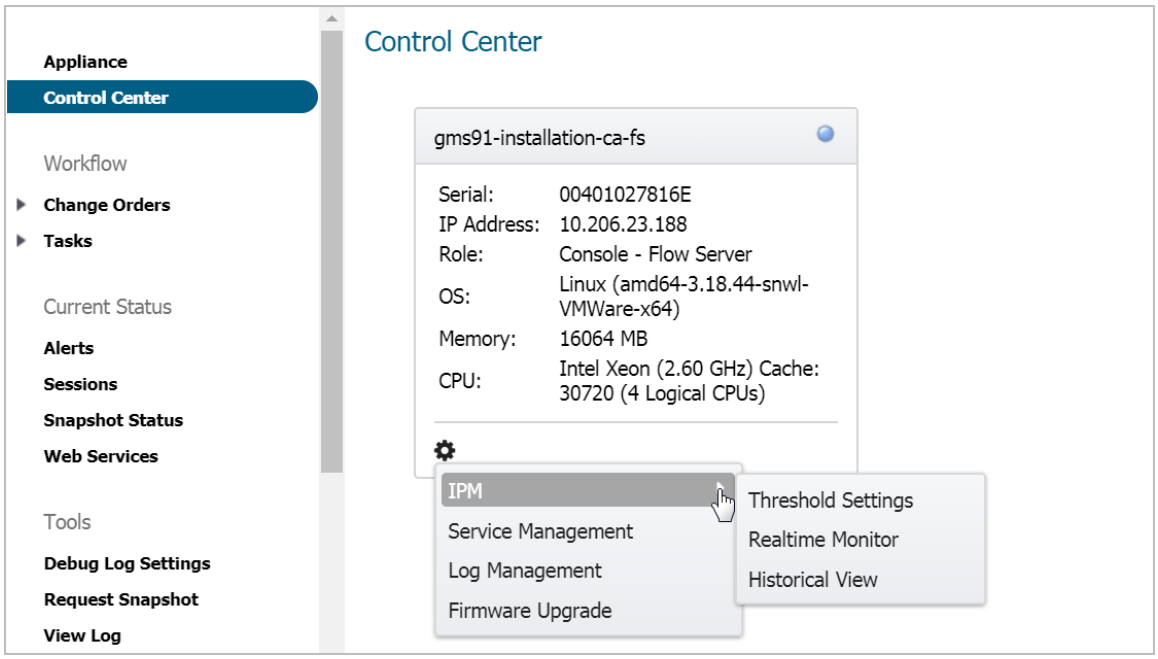
The represents the new Distributed IPM feature as described in the Distributed Intelligent Platform Monitoring section that follows.

The represents the operations you can perform on any GMS instance (including the Console itself). For example, the start/stop a service feature, upgrading the GMS firmware, and so on.

The represents your ability to examine system-level data on any GMS instance. For example, by downloading a log file from a GMS instance.

Centralized Management Control Center

The Centralized Management & Monitoring Control Center, is accessible by clicking the Gear icon in the top right corner of GMS and selecting **Control Center**.

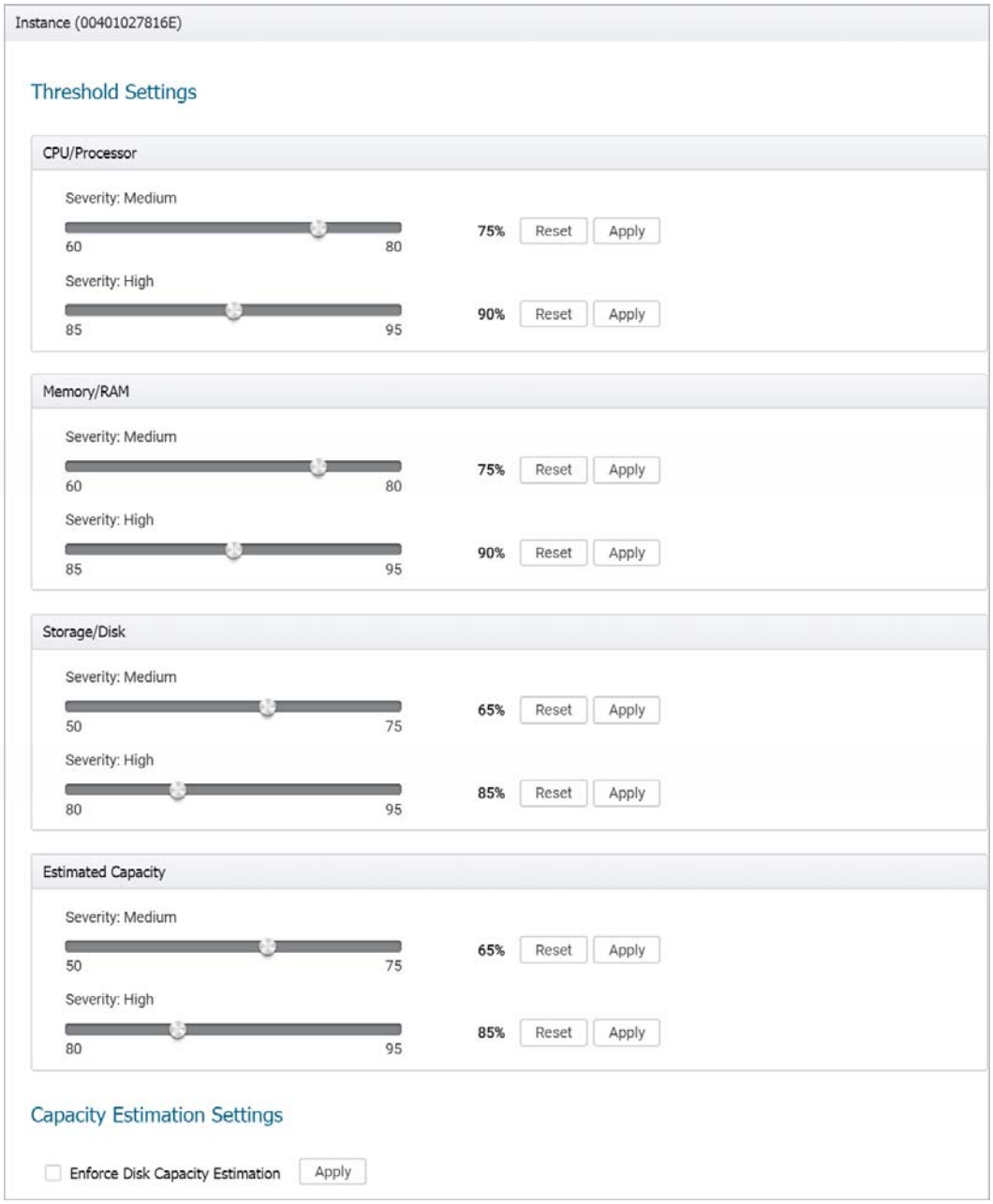


Each tile-based panel represents a separate GMS instance. Identifying information of the GMS instance is clearly listed in the panel. The core functionality is represented in the drop-down menu when you click the Gear icon. There are four feature functions:

IPM

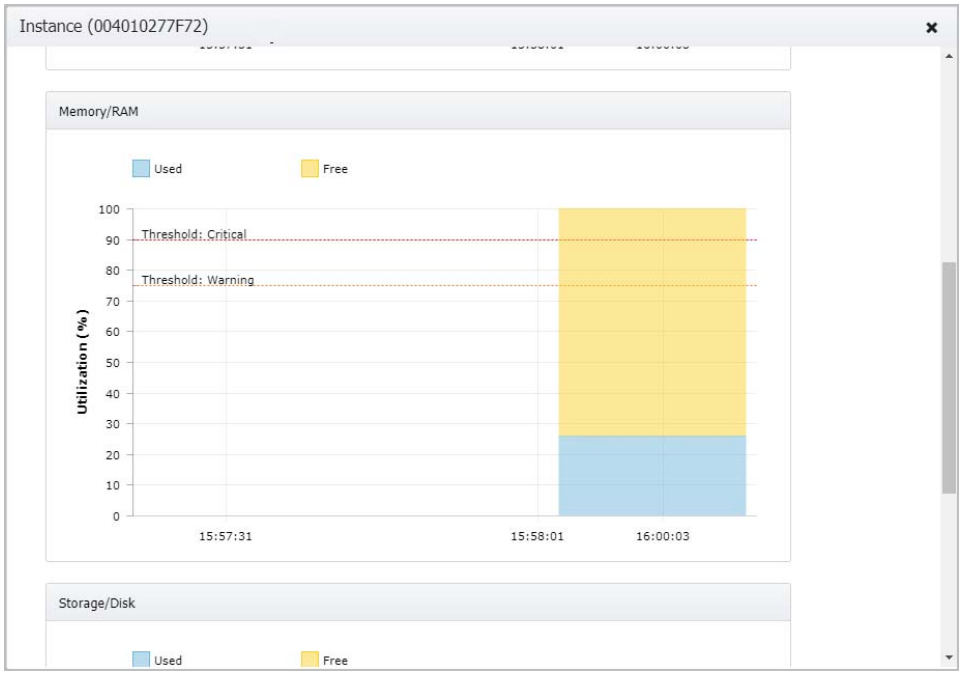
For more information about the IPM feature, see Distributed Intelligent Platform Monitoring as well as the following images:

Threshold Settings



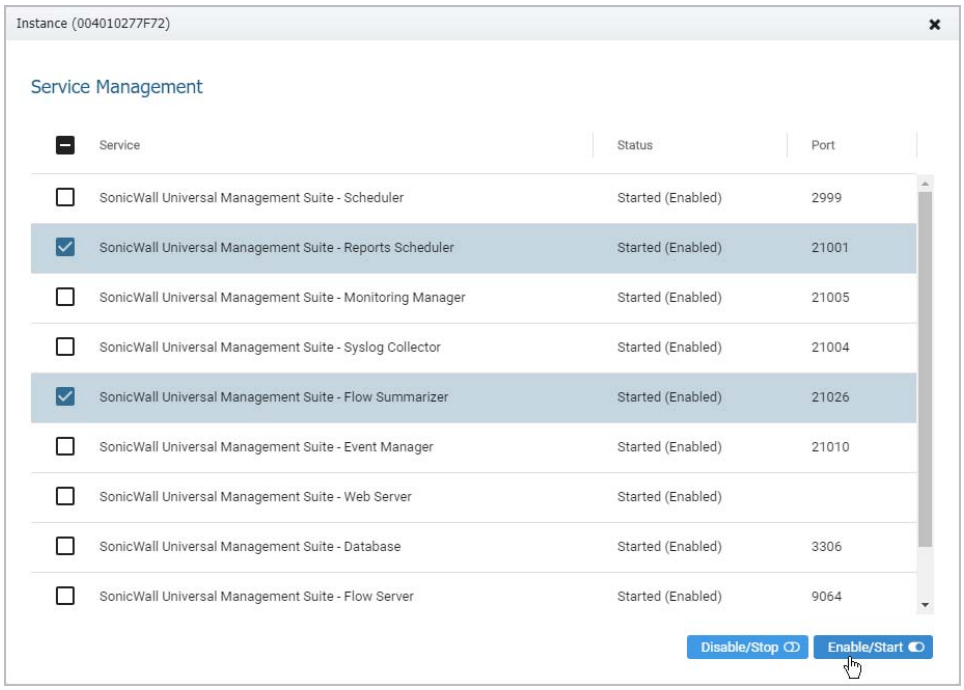
Realtime Monitoring

Historical Data View



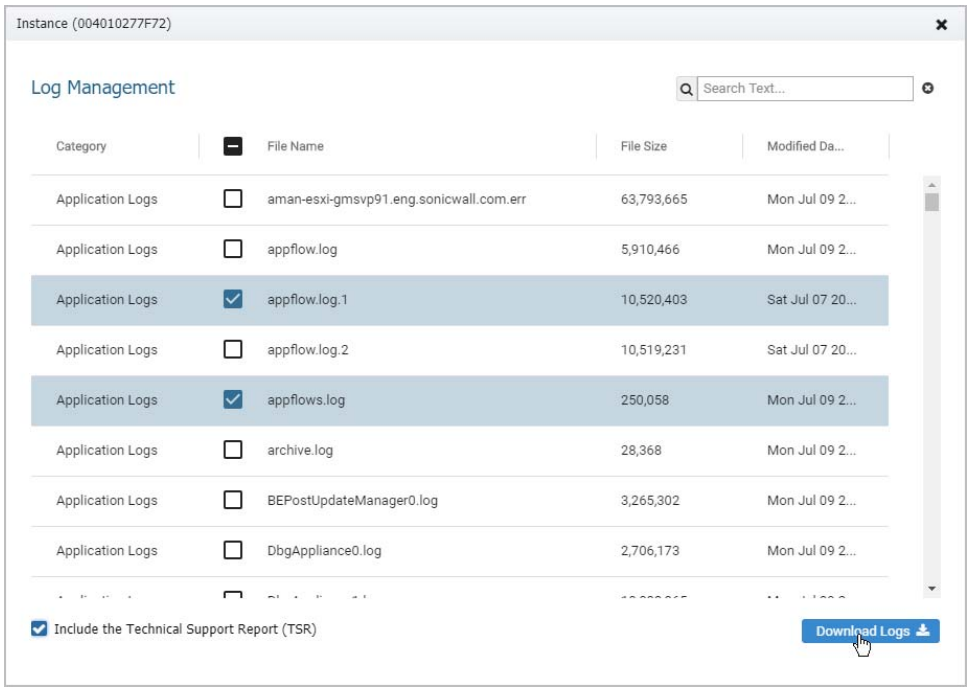
Service Management

Through the service management user interface, 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.



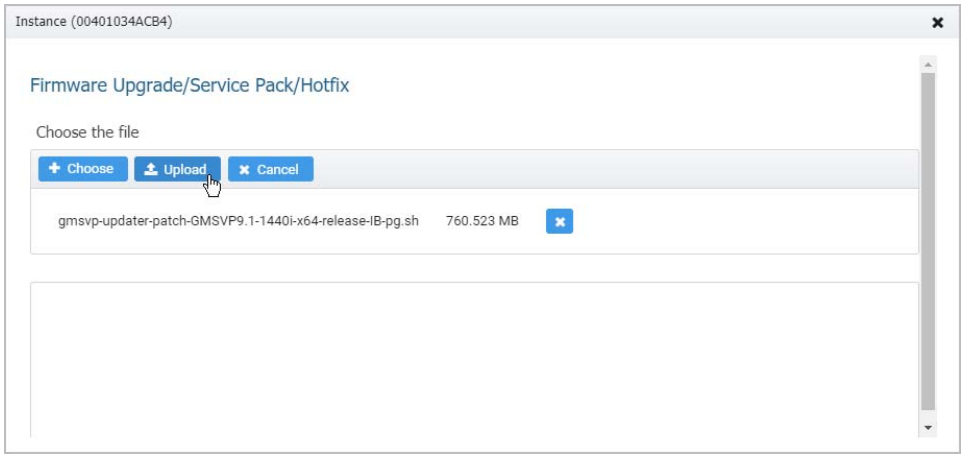
Log Management

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 are zipped into a .ZIP file and can then be downloaded onto your file system.



Firmware Upgrade

Firmware Upgrade provides you with capability of upgrading the firmware version of a GMS instance. This functionality is available within a drop-down menu of a GMS instance.



Distributed Intelligent Platform Monitoring

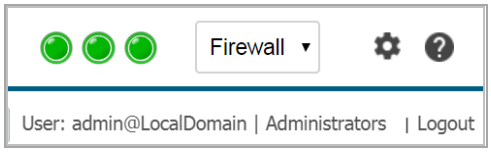
Topics:

- 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 to right, the status indicators display the current status of:

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

The possible visible states of these indicators are:


Initial


Normal


Warning

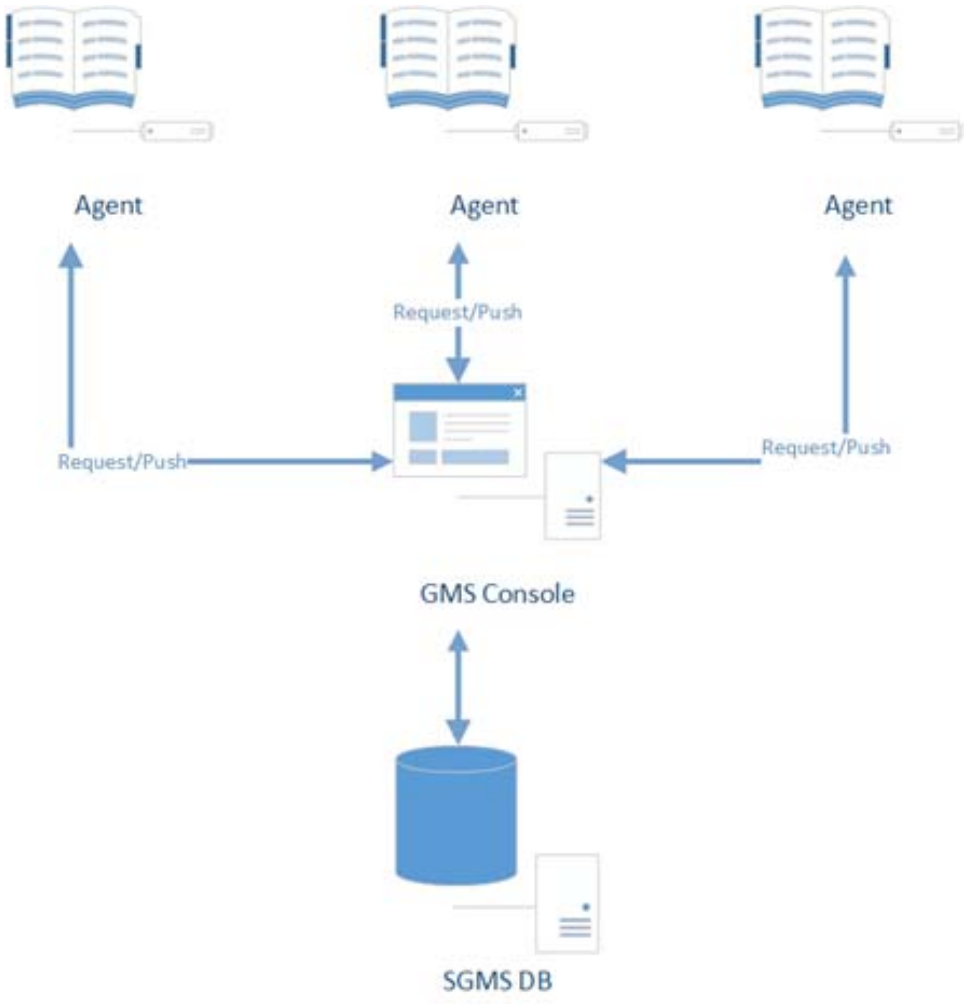

Critical

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 in order 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 in order to reflect the LED status.

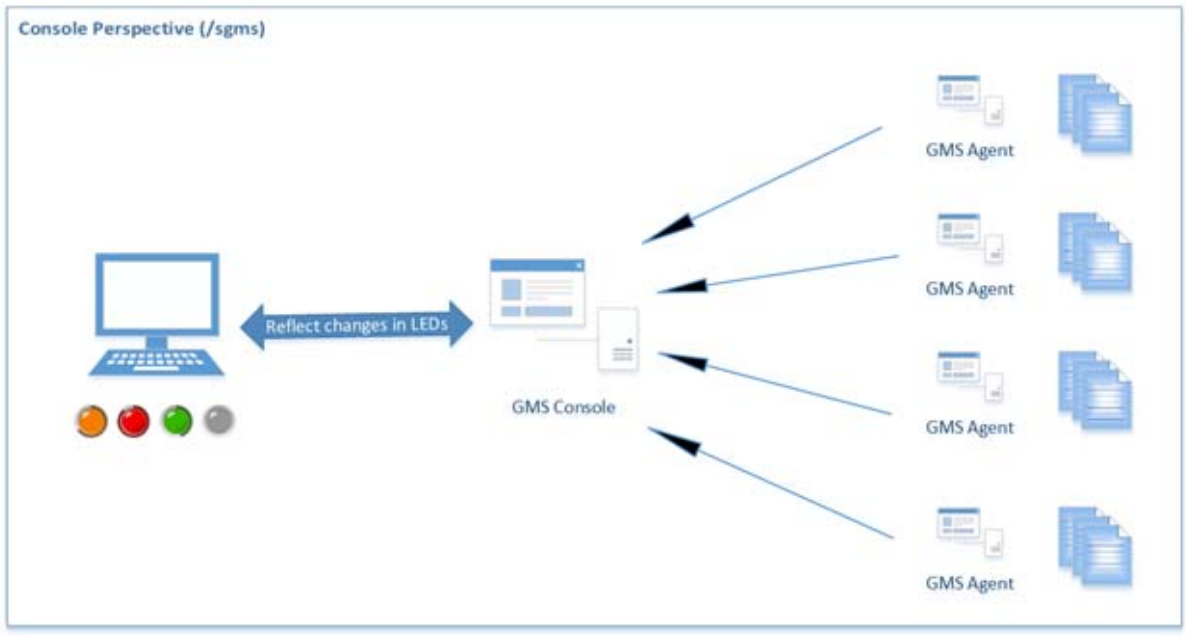


Distributed LED State

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

Agent Perspective

Console Perspective



The functionally 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.

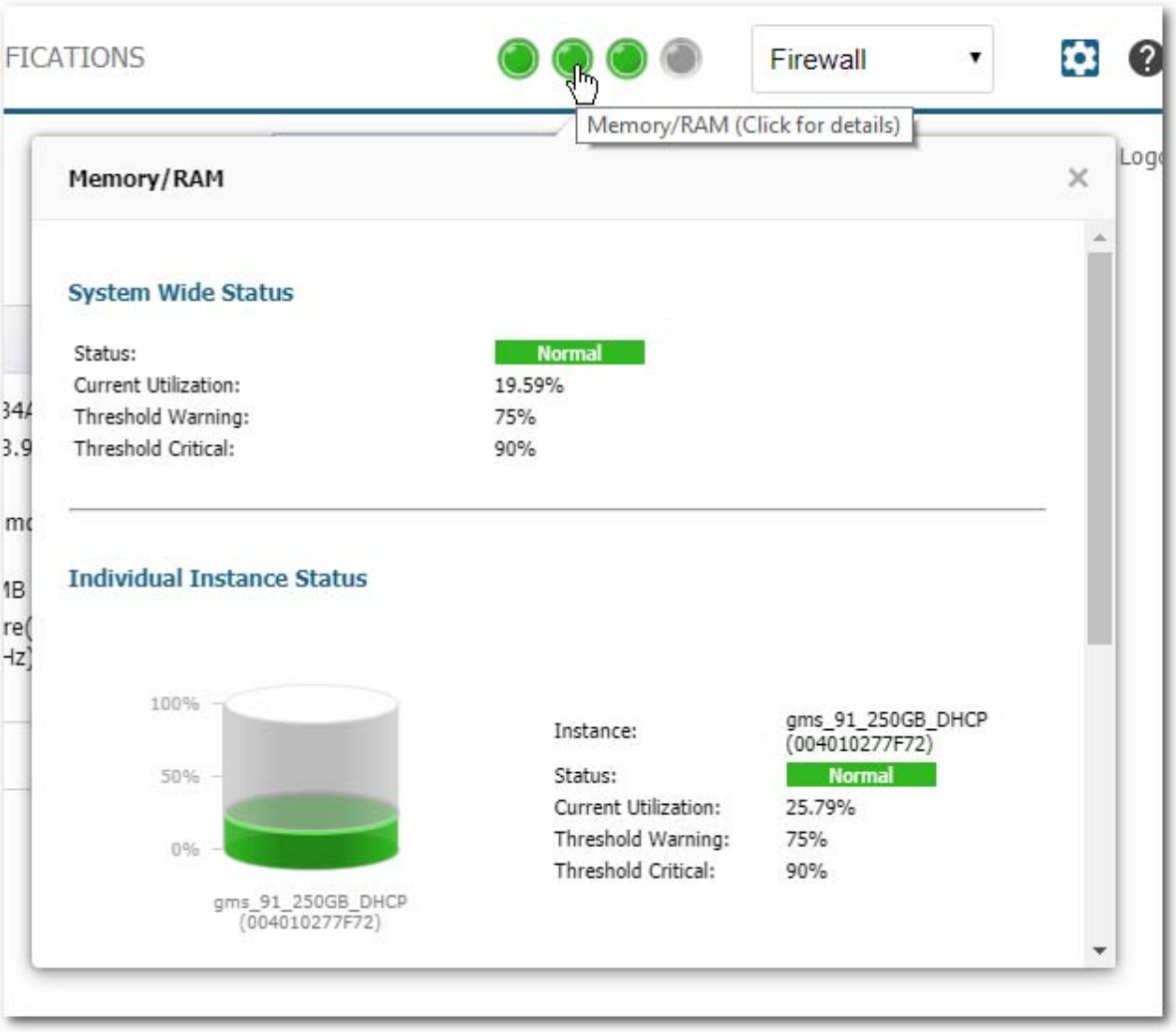
The highest severity from all the data is shown only in the outer ring of the LED. The LED status changes depending on the average of all the agent's data over a period of 24 hours.

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

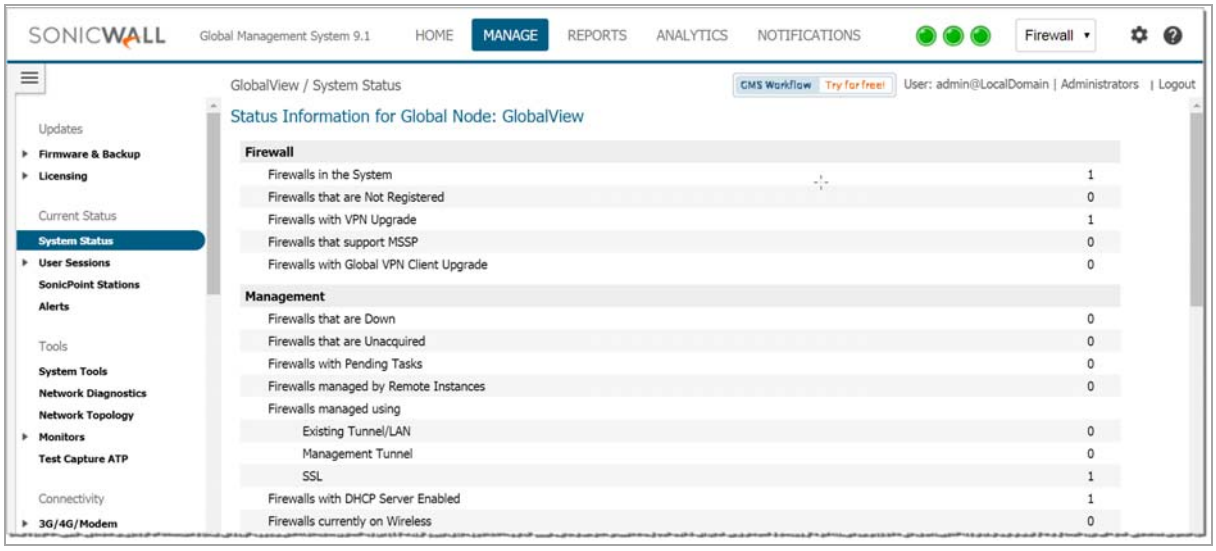
Enhanced Informative Tooltip Display

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.



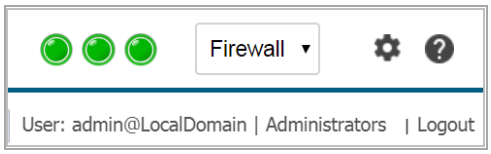
Navigating the GMS Management Interface



The GMS management interface consists of these panes:

- Left pane: Use this pane to manage and group units for management and reporting. (This panel is not available in Console, Appliance, and Notifications views.)
- Middle pane: Use this pane to access settings and functionality available depending on which view you have selected at the top of the window.

Use the drop-down list on the upper right of the GMS management interface to choose the type of units you want displayed in the left pane.



The GMS Management Interface contains these major views:

- HOME View
- MANAGE View
- REPORTS View
- ANALYTICS View
- NOTIFICATIONS View
- Console View

HOME View

The **HOME** view displays the Dashboard, the current status of the system, and summary charts for several different reporting topics.

NOTE: The items available on the **HOME** view will be different depending on the **Reporting Mode** with which you installed GMS. See for Setting the Install Mode more information.

For more information about using the **HOME** view, see HOME View.

MANAGE View

The **MANAGE** view is used to configure 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

NOTE: The **REPORTS** view is only available if you installed GMS with the **Reporting Mode** set to either **Flow based** or **Syslog based**. See for Setting the Install Mode more information.

The **REPORTS** view is an essential component of the network security that is used to view and schedule reports about critical network events and activity, such as security threats, inappropriate Web use, and bandwidth levels.

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 activity handled by your devices.

For more information about using the **ANALYTICS** view, see ANALYTICS View.

NOTIFICATIONS View

The **NOTIFICATIONS** view helps you monitor, and provide you with notifications about the status of, the SonicWall appliances and other network devices managed by your GMS.

NOTE: The items available on the **NOTIFICATIONS** view will be different depending on the **Reporting Mode** with which you installed GMS. See for Setting the Install Mode more information.

For more information about using the **NOTIFICATIONS** view, see NOTIFICATIONS 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.

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.
	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.

Status Icon Descriptions (Continued)

	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 the Console, Appliance, or System views.

9

HOME View

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

Topics:

- HOME View (Flow Based)
- HOME View (Syslog Based)
- HOME View (Management Only)

HOME View (Flow Based)

The **HOME** view is the default view managing an appliance through GMS. From it can access these pages:

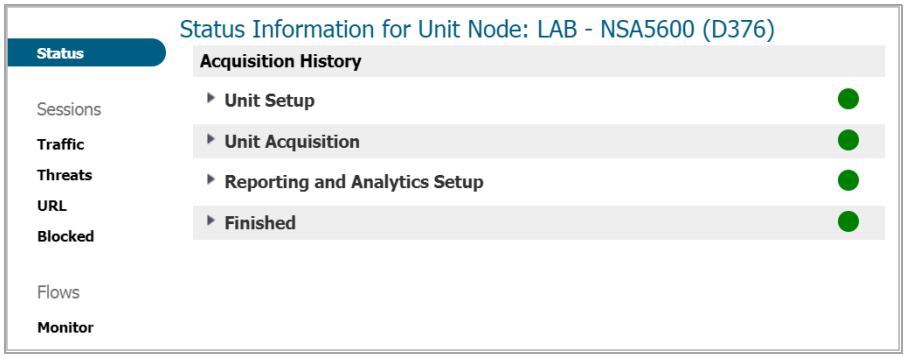
Topics:

- Status
- Dashboard
- Summary by Topic
- Live Monitor

Status

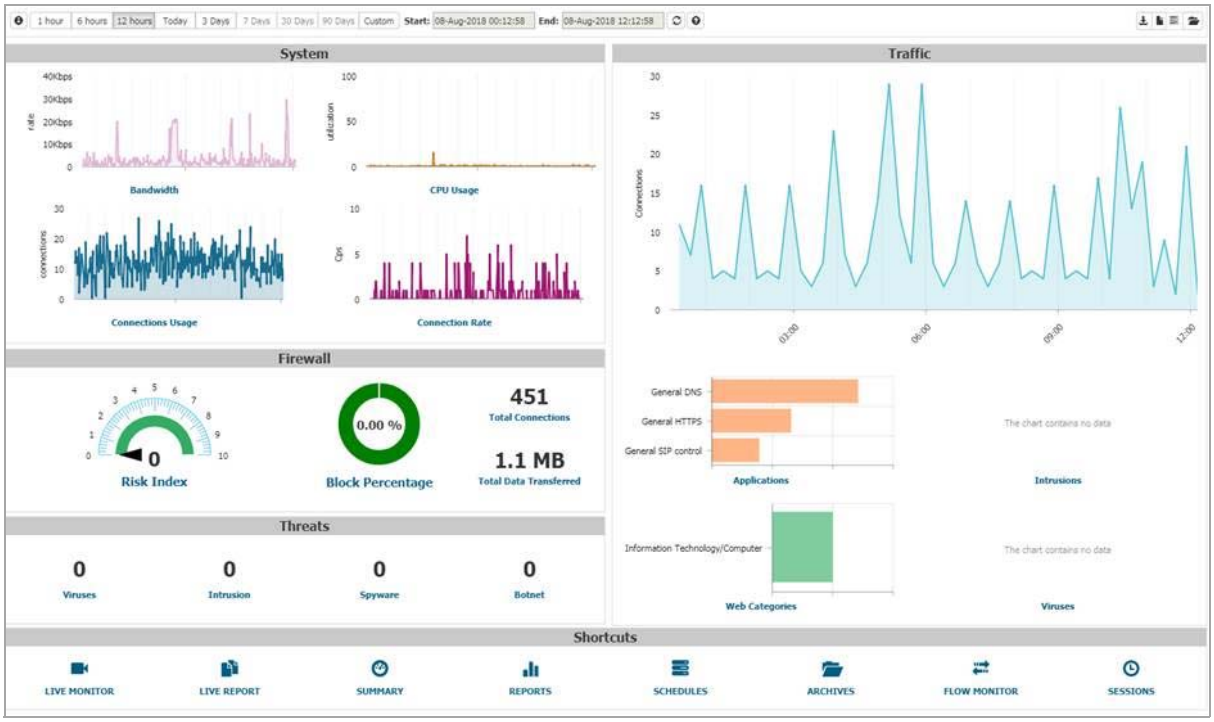
The **Status** page displays the current system status for the appliance, along with any applicable statistics and licensing information:

- Firewall
- Management
- Subscription
- Firewall Models



Dashboard

The Dashboard page provides a view intended to work as a customizable dashboard where you are able to monitor the latest happenings with your SonicWall GMS deployment, your network, the IT and Security World, as well as the rest of the world.



Upon initial login, you see a default Dashboard view. You are able to further customize this page by configuring and adding preferred components.

Summary by Topic

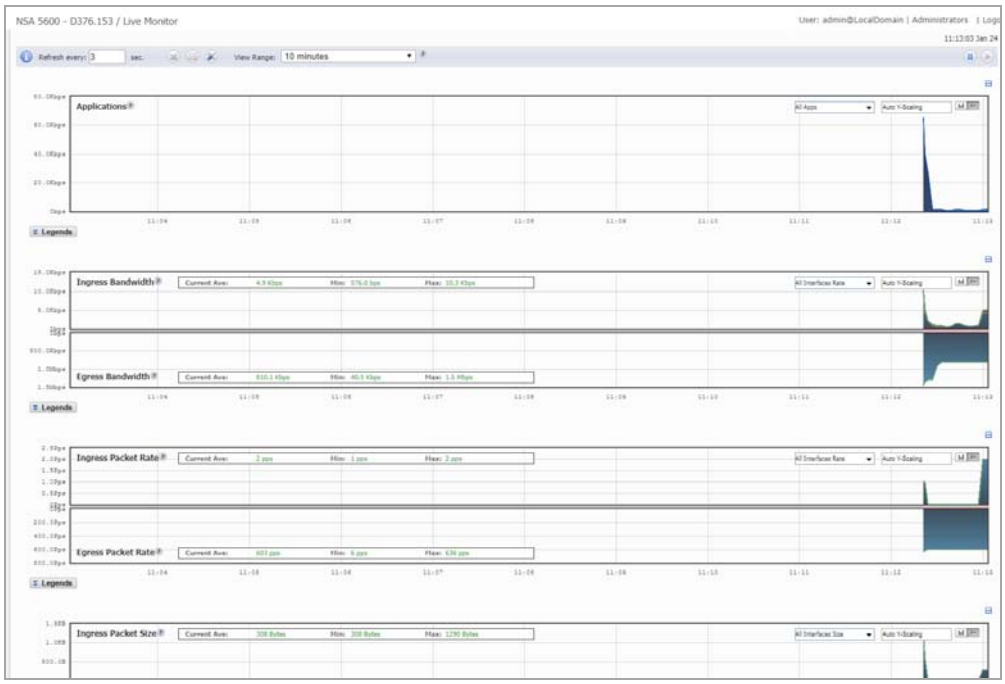
The Summary by Topic section provides access to these summary reports:

- Applications
- Blocked
- Threats
- Users

- Viruses
- Intrusions
- Spyware
- Web Categories
- Sources
- Destinations
- Source Locations
- Destination Locations
- BW Queues
- Botnet

Live Monitor

The **Live Monitor** page provides a real-time, multi-functional display with information about hardware multi-core utilization, applications, bandwidth usage, packet rate, packet size, connection rate, connection count, and memory usage.



NOTE: For more information on using the features of the **Live Monitor**, see *SonicOS 6.5 Monitor.*

HOME View (Syslog Based)

The **HOME** view is a customizable executive summary of your GMS deployment. The Dashboard tab provides powerful network visualization reporting, monitoring, and search filtering tools consolidated into one area of the management user interface.

Upon initial login, you see a default **Home** view. You are able to further customize this view by configuring and adding preferred components. The **HOME** view also provides administrators with a centralized location to create Universal Scheduled Reports for reporting solutions.

From it can access these pages:

Topics:

Universal Dashboard

The **Universal Dashboard** page provides the administrator—upon initial login with factory defaults—a geographical map displaying GMS deployment information.

The Geographical View displays the following SonicWall GMS elements graphically:

- SonicWall GMS-managed units—such as Firewall, SMA, and Email Security (ES) appliances
- SonicWall GMS-host servers—such as UMH hosts in server, console agent, or database role configurations
- Auto-discovered units behind the SonicWall GMS remotely-managed units—such as configured network address objects like public servers

Depending on the administrative access privileges that a logged in user has, the right subset of objects in the previous image are displayed on the geographical map.

NOTE: See “Using the Universal Dashboard” in the *GMS 9.0 Administration Guide* for more information about using and configuring the Universal Dashboard.

Universal Scheduled Reports

The **Universal Scheduled Reports** page displays the results of any Universal Scheduled Reports. It provides management interfaces to let the user setup schedules and configure reports to be exported in a periodic fashion and in various report formats. The Universal Scheduled Reporting application streamlines the configuration processes to unify and enhance the existing functionality to the system-wide usage patterns. This allows the user to collect report data from multiple appliances and create a single global report.

NOTE: See “Using the Universal Scheduled Reports Application” in the *GMS 9.0 Administration Guide* for more information about using and configuring the Universal Dashboard.

My Default Page

My Default Page Includes a default settings widgets page.

HOME View (Management Only)

The **HOME** view is a customizable executive summary of your GMS deployment. The Dashboard tab provides powerful network visualization reporting, monitoring, and search filtering tools consolidated into one area of the management user interface.

Upon initial login, you see a default **Home** view. You are able to further customize this view by configuring and adding preferred components. The **HOME** view also provides administrators with a centralized location to create Universal Scheduled Reports for reporting solutions.

From it can access these pages:

Topics:

Universal Dashboard

The **Universal Dashboard** page provides the administrator—upon initial login with factory defaults—a geographical map displaying GMS deployment information.

The Geographical View displays the following SonicWall GMS elements graphically:

- SonicWall GMS-managed units—such as Firewall, SMA, and Email Security (ES) appliances
- SonicWall GMS-host servers—such as UMH hosts in server, console agent, or database role configurations
- Auto-discovered units behind the SonicWall GMS remotely-managed units—such as configured network address objects like public servers

Depending on the administrative access privileges that a logged in user has, the right subset of objects in the previous image are displayed on the geographical map.

NOTE: See “Using the Universal Dashboard” in the *GMS 9.0 Administration Guide* for more information about using and configuring the Universal Dashboard.

My Default Page

My Default Page Includes a default settings widgets page.

10

MANAGE View

The MANAGE view is used to configure 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.

To open the MANAGE view, click the appropriate appliance at the top of the SonicWall GMS management interface and then click the MANAGE view.

Topics:

Updates

The **Updates** page allows you to manage your:

- Firmware & Backup: firmware upgrade installation
- Licensing: register SonicWall appliances, service licenses, search licenses, license sharing, and used activation codes

NOTE: For more information on using the features of the **Updates** page, see *SonicOS 6.5 Updates*.

Current Status

The **Current Status** section provides you with information about:

- System Status: current system status
- User Sessions: active users
- SonicPoint Stations: status of any attached SonicPoint units
- Alerts: system status alerts

Tools

The **Tools** section provides you with access to tools to:

- System Tools: restart your appliances, gather diagnostics information, synchronize your appliances
- Network Diagnostics: perform diagnostics for your network
- Network Topology: display the current network topology
- AccessPoints FloorPlan: displays the location of any SonicPoint or SonicWave access points
- Monitors: connections, CPU, processes, and VPN
- Test Capture ATP: upload files to be scanned

Connectivity

The **Connectivity** section allows you to manage:

- 3G/4G/Modem: base settings, advanced settings, and connection profiles
- Access Points (SonicPoint/SonicWave): base settings, floor plan view, IDS, advanced intrusion and detection (IDP), Virtual Access Point, FairNet, and wi-fi multimedia connections
- VPN: base settings, configuration, and L2TP server
- SSL VPN: server settings, portal settings, client settings, and client routes

NOTE: For more information on using the features of the **Connectivity** page, see *SonicOS 6.5 Connectivity*.

Policies

The **Policies** section allows you to manage:

- Rules: rules for network access, routing, address mapping, and VPN access
- Objects: address and service objects

NOTE: For more information on using the features of the **Policies** page, see *SonicOS 6.5 Policies*.

System Setup

The **System Setup** section allows you to set up these features:

- Appliance: base settings, SNMP, passwords, login security, web management, certificates, and system time and schedules
- Network: interfaces, PortShield interfaces and X?]Series switches, failover and load balancing, zones, VLAN translation, DNS, DNS proxy, routing, ARP, neighbor discovery, MAC-IP anti-spoof, DHCP server, IP helper, web proxy, and dynamic DNS
- DHCP: base settings, DHCP over VPN, dynamic ranges, static entries, option objects and groups, and trusted agents
- Switching: VLAN trunking, link aggregation, and port mirroring

- VoIP: consistent NAT and SIP and H.323 settings
- Virtual Assist: allows users to support customer technical issues without having to be on-site with the customer
- Users: user authentication, local users and groups, guest services and accounts, web login, RADIUS accounting, customized pre- and post-login banners, acceptable use policies, and login pages, partitions (adding authentication partitions and partition selection policies)
- High Availability: base setup, advanced settings, and monitoring settings
- WAN Acceleration: status, TCP acceleration, WFS acceleration, and web cache

NOTE: The pages available in the **System Setup** section may vary depending on the features available and supported on the managed device.

NOTE: For more information on using the features of the **System Setup** page, see *SonicOS 6.5 System Setup*.

Security Configuration

The **Security Configuration** section allows you to configure:

- Firewall Settings: firewall settings, flood protection, multicast, Quality of Service mapping, SSL control, and advanced settings
- Deep Packet Inspection (DPI): SSL client deployment and SSL server deployment
- DPI-SSH: configure
- Anti-Spam: base setup and real-time blacklist filter
- Security Services: general settings, Content Filter Service (CFS), client AV enforcement, Gateway Anti-Virus, intrusion prevention, Anti-Spyware, Geo-IP filter, and botnet filter
- External IDS:
- Content Filter: general settings, policies, exclusion list, custom list, custom categories, web features, and special settings for N2H2 and Websense Enterprise

NOTE: For more information on using the features of the **Security Configuration** page, see *SonicOS 6.5 Security Configuration*.

Logs and Reporting

The **Logs and Reporting** section allows you to set options for GMS reporting:

- Appflow Settings: Flow reporting, GMS Flow Server, Appflow Server
- Log Settings: base setup and name resolution

NOTE: For more information on using the features of the **Logs and Reporting** page, see *SonicOS 6.5 Logs and Reporting*.

11

REPORTS View

The **REPORTS** view is an essential component of the network security that is used to view and schedule reports about critical network events and activity, such as security threats, inappropriate Web use, and bandwidth levels.

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.

What you see on the **REPORTS** view depends on the **Reporting Type** you set when you installed GMS. (See Setting the Install Mode for more information.)

Topics:

- REPORTS View (Flow Based)
- REPORTS View (Syslog Based)

REPORTS View (Flow Based)

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

Topics:

- Status
- Reports by Topic
- Scheduled Reports
- Live Reports

Status

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

- Acquisition History
- Firewall
- System
- Flow Management

Reports by Topic

The **Reports by Topic** section provides access to reports of these types:

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

The reports are available with these views:

- Chart
- Table
- Timeline

Scheduled Reports

The **Scheduled Reports** section allows you to:

- On Demand: view reports immediately
- Archive: access archived reports

Live Reports

The **Live Reports** section and page displays historical data for the usage of the system, applications, and network interfaces.

REPORTS View (Syslog Based)

To open the **REPORTS** view, select the Firewall, Email Security, or SMA view at the top 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

12

ANALYTICS View

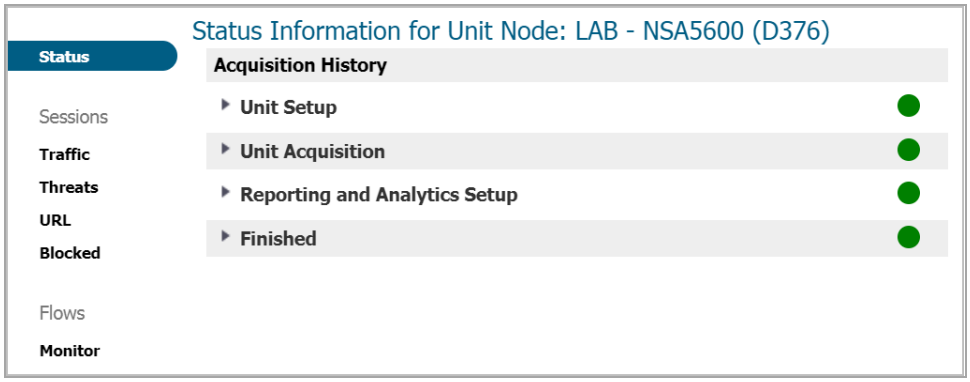
The **ANALYTICS** view provides you with access to detailed information about the activity handled by your devices.

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.

Topics:

- Status
- Sessions
- Flows

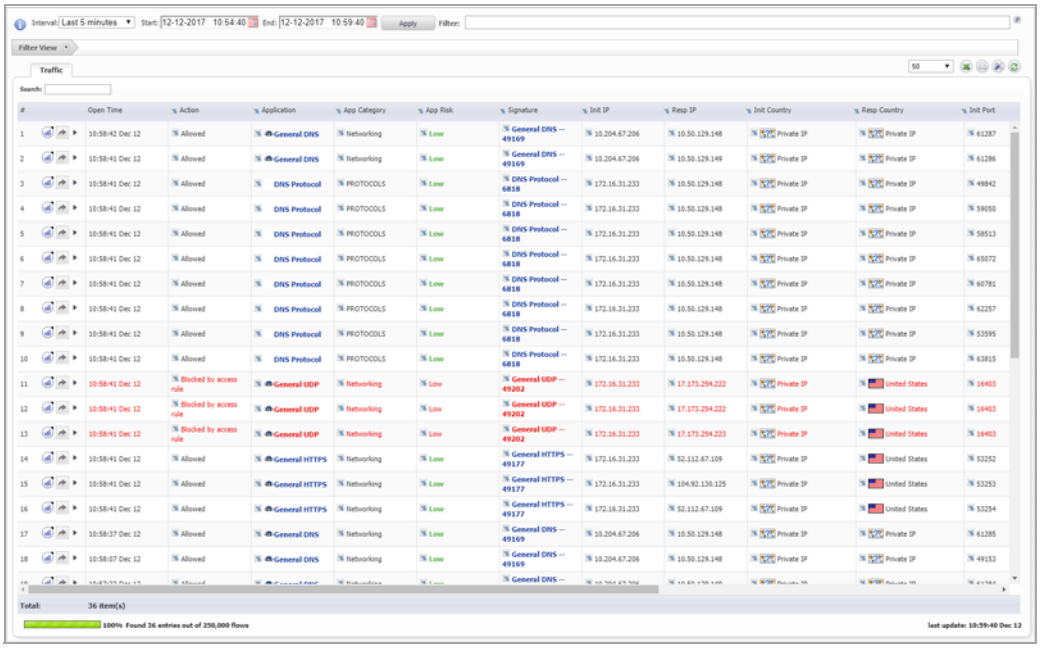
Status



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

- Acquisition History
- Firewall
- System
- Flow Management

Sessions



The **Sessions** section displays flow logs from the device for these items:

- Traffic
- Threats
- URL
- Blocked

Filters can be created and applied to help you locate specific data within the logs.

Traffic

The **Traffic** page displays all of the sessions going through the firewall.

Threats

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

URL

The **URL** page lists all of the sessions that are accessing URLs.

Blocked

The **Blocked** page displays information about all of the sessions blocked based on the policies configured in the **MANAGE | Policies** section.

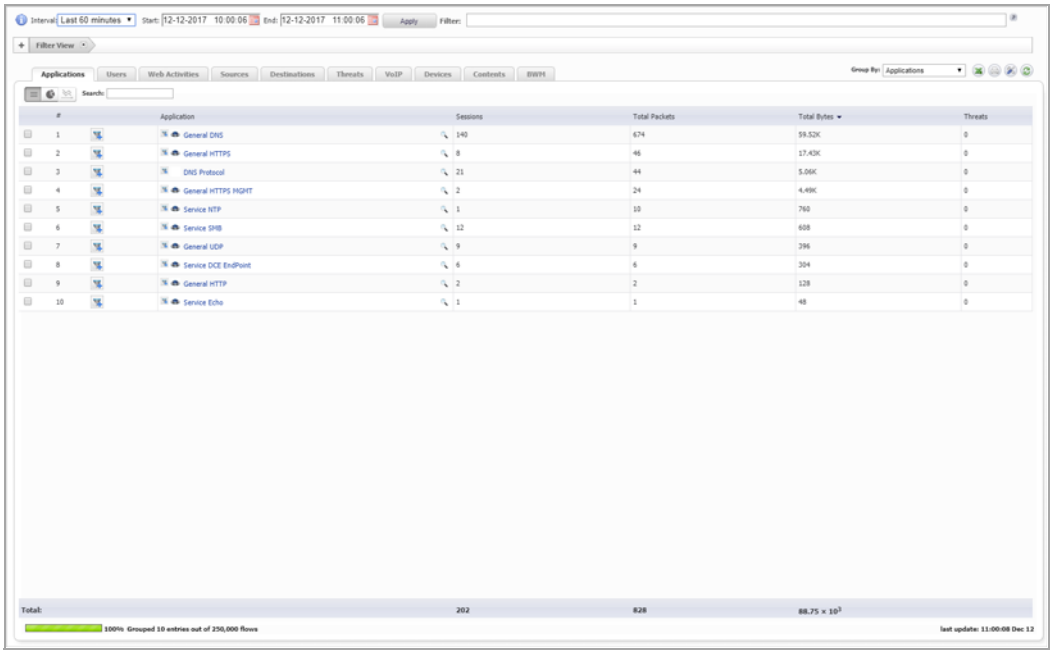
Flows

The **Flows** section provides you with access to these pages:

- Monitor

Monitor

The **Monitor** page lets you visualize the traffic data by applications, users, URLs, initiators, responders, threats, VoIP, VPN, devices, or contents. Filters can be created and applied to help you locate specific data.



13

NOTIFICATIONS View

The **NOTIFICATIONS** view helps you monitor, and provide you with notifications about the status of, the SonicWall appliances and other network devices managed by your GMS.

Topics:

Tools

The **Tools** section contains a selection of tools you can use to monitor the status of the SonicWall appliances and other network devices managed by your GMS.

Topics:

Net Monitor page

The **Net Monitor** page displays information about your licensing of the GMS Net Monitor.

The GMS Net Monitor periodically tests the status of SonicWall appliances and other network devices. When configured, it enables you to monitor the status of your network and immediately respond when SonicWall appliances and other network devices become unavailable.

The Net Monitor enables you to categorize different groups of SonicWall appliances or other network devices. You can categorize them by device type, geography, or any other organizational scheme. Additionally, you can assign devices within each category a high, medium, or low priority.

Real-Time Syslog

NOTE: The **Real-Time Syslog** page is only available if you installed GMS with the **Reporting Type** set to **Syslog based**. See Setting the Install Mode for more information.

The **Real-Time Syslog** page displays real-time data from the syslog reports.

Live Monitor

NOTE: The **Live Monitor** page is only available if you installed GMS with the **Reporting Type** set to **Syslog based**. See Setting the Install Mode for more information.

The **Live Monitor** section and page provides access to the Live Monitor reporting results.

Live Monitoring allows you to monitor a network through the correlation of syslogs received from appliances throughout a deployment. The syslogs are received by the Event Manager Receiver Service that then feeds them into an Event Correlation Engine. The engine sends the messages through user-defined rules, and if a rule condition is met, the engine forwards the object to be turned into an alert for Live Monitoring.

These alerts are sent to email, traps, other user-defined destinations, and to the new Live Monitoring user interface, if a user is currently monitoring. Viewing alerts in the Live Monitoring interface provides greater flexibility to monitor a network, and to analyze traffic based on protocols, web usage and productivity, or even to detect viruses and attacks in the network.

Live Monitoring is a powerful tool when rules are created properly, allowing you to monitor various amounts of information on the unit(s) efficiently. Be aware that while the alerts keep you updated with what is being sent and received, this might bombard your inbox or trap listener with a heavy amount of notifications. This happens only when the rule is lenient; if the rule is strict, there is not a large number of notifications.

A

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.

GMS Getting Started Guide
Updated - August 2018
Software Version - 9.1
232-004477-00 Rev A