SonicWall[®] GMS 9.1

Getting Started Guide



Contents

Part 1. Introducing GMS
Introduction to GMS5
Part 2. Installing GMS
Before You Begin
System Requirements
Installation Quick Start
Record Configuration Information
Installing the GMS OVA File9
Setting Up the Network Configuration14
Configuring the System
Performing Basic Tasks and Manual Host Configuration
Power the Virtual Appliance On
Configure Host Settings on the Console19
Configure Host Settings on the Appliance Management Interface
Viewing the Settings Summary
Editing The Virtual Machine Settings 22
Setting the Install Mode23
Single Server Deployment
Distributed Deployment
Registering GMS
GMS Registration
Adding Devices
Basic Mode
Advanced Mode

Part 3. Using GMS

Using the GMS Management Interface41
Centralized Management and Monitoring41
Distributed Intelligent Platform Monitoring
Navigating the GMS Management Interface
Console View
Understanding GMS Icons
HOME View
HOME View (Flow Based)
HOME View (Syslog Based)

SonicWall Global Management System 9.1 Getting Started Guide Contents

HOME View (Management Only) 60
MANAGE View
Updates
Current Status
Tools
Connectivity
Policies
System Setup
Security Configuration
Logs and Reporting
REPORTS View
REPORTS View (Flow Based)
REPORTS View (Syslog Based)
ANALYTICS View
Status
Sessions
Flows
NOTIFICATIONS View
Tools
SonicWall Support
About This Document

Part 1

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 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

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

7

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.	

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.

1 Select an OVF template	Select an OVF template		
2 Select a name and folder	Select an OVF template from remote URL or local file system		
2 Select a compute resource 4 Review details 5 Select storage 6 Select networks 7 Ready to complete	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 The most strengthene on each stored strengthene on the strengthene of the strengthe		

9

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

1 Select an OVF template 2 Select a name and folder	Select a name and folder Specify a unique name and target location
3 Select a compute resource 4 Review details	Virtual machine name: sw_gmsvp_vm_eng_9.0.9008.1087.250GB.64bit-pg
6 Select networks	Select a location for the virtual machine.
7 Ready to complete	✓ Ø vCenter5-1.sv.us.sonicwall.com ✓ San Jose ✓ Dev ✓ Dev ✓ Automation
	> 🗈 ES > 💼 Manish > 💼 Dev
	 > m DM-DataCenter > m Dev Test > m GMS > m Hadoop > m GA
	2 🖬 onlangitar

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

1 Select an OVF template 2 Select a name and folder	Select a compute resource Select the destination compute resource for this operation
3 Select a compute resource 4 Review details 5 Select storage 6 Select networks 7 Ready to complete	 ✓ In DM-DataCenter ✓ In DM-Cluster-1 In 203.20.11 In 203.20.12 > Source > Build-Automation > D DataStax > DM-Experiment > SonicCore > Templates > Test
	Compatibility Compatibility checks succeeded. CANCEL BACK N

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

1 Select an OVF template 2 Select a name and folder 3 Select a compute resource	Select a compute resource Select the destination comoute resource for this operation
4 Review details 5 Select storage 6 Select networks 7 Ready to complete	CM-ObstaCenter CM-ObstaCenter CM-ObstaCenter CDM-Cbuster-1 CD2022012 Acodio:3 Suld-Automation Datastax O Datastax O Validating O Temblates Fest

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

2 Select a name and folder 3 Select a compute resource	Review details Verify the template det	ails.		
4 Review details	Bublisher			
5 License agreements	Publisher	No certificate present		
7 Select networks	Download size 606.7 MB			
8 Ready to complete	Size on disk	1.3 GB (thin provisioned)		
		250.0 GB (thick provisioned)		

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

1 Select an OVF template 2 Select a name and folder	License agreements The end-user license agreement must be accepted. Read and accept the terms for the license agreement.			
3 Select a compute resource 4 Review details				
5 License agreements 6 Select storage	SonicWall End User Product Agreement			
7 Select networks 8 Deady to complete	PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THIS PRODUCT. BY			
o ready to complete	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 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.			

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.

Select storage Select the datastore in which to store the configuration and disk files								
Select virtual disk format: This	k Provision Laz	y Zeroed 🗸 🗸						
VM Storage Policy:		<u> </u>						
Name	Capacity	Provisioned	Free	Туре				
Compellent-DM-GMS-Vo	10 TB	15.26 TB	2.81 TB	VN (
dm-gms-01-RAID1-Local1	271.25 GB	9.47 GB	261.78 GB	VN				
4								
< Compatibility								
	Select storage Select the datastore in which to Select virtual disk format: This VM Storage Policy: Name Compellent-DM-GMS-Vo dm.gms-01-RAID1-Local1	Select storage Select storage Select the datastore in which to store the config Select virtual disk format: Thick Provision Laz VM Storage Policy: Name Capacity Capa	Select storage Select the datastore in which to store the configuration and disk f Select virtual disk format: Thick Provision Lazy Zeroed VM Storage Policy: VM Storage Policy: Name Capacity Provisioned Competient-DM-GMS-Vo 10 TB 15.26 TB dm.gms-01-RAID1-Local1 271.25 GB 9.47 GB	Select throage Select the datastore in which to store the configuration and disk files Select virtual disk format: Thick Provision Lazy Zeroed VM Storage Policy: 				

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.

 1 Select an OVF template 2 Select a name and folder 	Select networks Select a destination network for each source network.						
 3 Select a compute resource 4 Review details 	Source Network			Destination Network	т		
 5 License agreements 	VM Network			DPortGroup-10.202.3.X			
6 Select storage					1 items		
8 Ready to complete							
	IP Allocation	Settings					
	IP allocation:	Static - Manual	~	IP address:			
	IP protocol:	IPv4	~				

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

 1 Select an OVF template 2 Select a name and folder 	Ready to complete Click Finish to start creation.						
3 Select a compute resource 4 Peview details							
5 License agreements	Provisioning type	Deploy from template					
6 Select storage	Name	sw_gmsvp_vm_eng_9.0.9008.1087.250GB.64bit-pg					
7 Select networks 8 Ready to complete	Template name	sw_gmsvp_vm_eng_9.0.9008.1087.250GB.64bit-pg					
	Folder	DM-DataCenter					
	Resource	10.203.20.12					
	Location	Compelient-DM-GMS-Vol01					

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

1.11.1.1.101.111.1.1.1.1.1.1.1.1.1.1.1.		
CentOS7-Template	Actions - sw_gmsvp_vm_eng_9.0.9008.1087.250GB.64bit-pg	1
ndhat-69	Power	۲
Redhat-7.4-Desh-Appflow-1	Guest OS	,
soniccore_developer_vmware_ov	Snapshots	,
nic-test	Note the console	
SonicWall_NSA_Dec11	P Martin	
Sw_gmsvp_vm_eng_9.0.9008.101	Cre Migrate	

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.

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



(i) 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

i Please log in	n	
Use default U Password:"pa	ser:"admin" and ssword" to login	
Username		
1		
Password		
LOGIN	Forgot Password?	



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.

System Configuration Tool							
Introduction	Welcome to the System Configuration wizard						
Network Settings	Configuring the system involves setting Host name, IP address, DNS, Time and other system specific parameters.						
Time Settings	This wizard will guide you through the process of configuring a host, step by step.						
Summary							
	Next > Cancel						

- 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 Configura	ation Tool					
Introduction	Step 2. Network Settings						
Network Settings	Select IP type: DHCP Static IPv4 Network Settings						
Time Settings	Name:	gms	e.g.: hostname				
Summary	Domain:	example.com	e.g.: domain.com				
Sammary	Host IP address: / Subnet mask:	10.202.3.245 255.255.255.0	/				
	Default gateway:						
	DNS server 1:	10.50.129.148					
	DNS server 2:	10.50.129.149					
	< Paak Navt S	Canaal					

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

	System Configuration Tool
Introduction	Step 3. Time Settings
Network Settings	Time (hh:mm:ss): 13 ▼ : 43 ▼ : 26 ▼
Time Settings	Date: August V 07 V 2018 V
Summary	TimeZone: (GMT-08:00) Pacific Time (US & Canada); Tijuana
	✓ Set time automatically using NTP
	Note: Automatically adjusts clock for daylight saving time
	To continue, click Next.
	< Back Next > Cancel
	SONICWALL

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**.

System Configuration Tool					
Introduction	Step 4. Summary				
Network Settings	Network Settings Hostname gms91-aio-flow Domain eng.sonicwall.com				
Time Settings Summary	Default gateway 10.206.23.195 Default gateway 10.206.23.1 Subnet mask 255.255.255.0 DNS server 1 10.50.129.148				
	Time Settings Time Time TimeZone (GMT-08:00) Pacific Time (US & Canada); Tijuana				
	Click "Apply" and proceed to complete the setup process.				
	< Back Apply Cancel				

- 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.

(i) 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.

(i) 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.

(i) 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 (i) 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.

	2	GM:		🖧 G	MS-Analyze	er-V	A-64-bit-	40GB	ACTIONS ~ s Datastores	; 1	Networks				
	> @ > @ > @	Son Son Son UI-UX Vish-so WWW	x 50 icWa icWA icWA pnico	M Pov Launch	vered On Remote Console (Gue Cor VM DN: IP A Hos	est OS: Of mpatibility: ES ware Tools: Ru M S Name: sn Addresses: 19 st: es	ther 2.6.x l SX/ESXI 4. unning, ver ore info nwl.examp 22.168.168.1 sx-sjc-17.er	Linux (32-bit) O and later (VM ve rsion:2147483647 (le.com 69 ng.sonicwall.com	Guest	7) Managed)			CPU USAGE 62 MHz MEMORY USAGE 163 MB STORAGE USAGE 56.11 GB	* III
	R	Sonico	S-D ▼												-
Recent Tas	ks	Alarr	ns												≈
Task Name		~	Target	~	Status	~	Initiator	~	Queued For	~	Start Time	Completion Time	~	Server	~
Power On virt machine	tual		🗗 kmott	-12.2.1-005	✓ Completed		SV\eng_chef		2 ms		08/07/2018, 2:30:12 PM	08/07/2018, 2:3 PM	0:14	vcenter6-pr.sv.us.sor	n. 🗐
Power On virt machine	tual		🛱 kmott	-12.2.1-005	✓ Completed		SV\eng_chef		2 ms		08/07/2018, 2:30:12 PM	08/07/2018, 2:3 PM	0:13	vcenter6-pr.sv.us.so	n.
Power On virt	tual		R kmot	12 21 005	Completed		S\Aena chef		2 me		08/07/2018, 2:30:12	08/07/2018, 2:3	0:15	voonter6 prevue eo More Tas	, ∓ sks

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.

ual Hardware VM Options				
				ADD NEW DEVICE
CPU	4 ~			θ
Memory	16	GB 🗸		
Hard disk 1	40	GB 🗸		
Network adapter 1	10.202.20	2.X ~	Connected	
Video card	4 MB			
VMCI device	Device on t virtual mach	he virtual machine nine communicatior	PCI bus that provides s interface	upport for the

- 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 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 on page 23
- Distributed Deployment on page 25

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.

Install Mode Selection Tool					
Introduction	Welcome to the Install Mode Selection tool				
Install mode	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				
Distributed mode	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.				
Database					
Role configuration					
Reporting type					
Summary					
	Next >				

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

Install Mode Selection Tool				
Introduction	Step 2. Install mode			
Install mode	Please choose the type of install this is. Is this a Single Server deployment? 			
Distributed mode	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.			
Database	Is this installation part of a distributed deployment?			
Role configuration	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.			
Reporting type				
Summary				
	< Back Next >			

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.

	Install Mode Selection Tool		
Introduction	Step 6. Reporting type		
Install mode	Please select a report type that will be used in report generation for units added to the system.		
Distributed mode	Flow based Reports are generated using IPFIX packets for units that have reporting licensed and enabled. The Analytics feature will be available with this		
Database	selection.		
Role configuration	Syslog based Reports are generated using Syslog packets for units that have reporting enabled. Live Monitor feature will be available with this selection.		
Reporting type	© None		
	Management only mode, Reports are disabled.		
Summary			
	< Back Next >		

- 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 Tool		
Introduction	Step 7. Summary	
Install mode	You have selected Default as the installation mode, Flow based as reporting option and All In One - Flow Server as the role.	
Distributed mode	Click "Apply" and proceed to complete the setup process.	
Database		
Role configuration		
Reporting type		
Summary		

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

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

Install Mode Selection Tool		
Introduction	Summary	
Install mode	Applying Install Mode and Role configuration settings. Please Wait	
Distributed mode	Performing database operations (applying db scripts, updates,)	
Database		
Role configuration		
Reporting type		
Summary		
	< Back Apply	

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

The SonicWall Universal Management Appliance is restarting.
Please wait

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.

Install Mode Selection Tool		
Introduction	Welcome to the Install Mode Selection tool	
Install mode	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	
Distributed mode	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.	
Database		
Role configuration		
Reporting type		
Summary		
	Next >	

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

Introduction	Step 2. Install mode		
	Please choose the type of install this is.		
Install mode	Is this a Single Server deployment?		
Distributed mode	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.		
Database	Is this installation part of a distributed deployment?		
Role configuration	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.		
Reporting type			
Summary			
	< Back Next >		

- 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 Tool	
Introduction	Please choose the type of install.	
Install mode	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.	
Distributed mode	Is this an Agent?	
Database	Please provide the location of the Primary Console. Primary Console is the Primary host that will provide Database, License and other information to configure this agent.	
Role configuration	Host IP or Name:	
Reporting type		
Summary		
	< Back Next >	

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.

	Install Mode	Selection Tool
Introduction	Step 4. Database	
	Enter the database para	meters for the selected role: Console
Install mode	Database Type:	Mysql 🔻 🗩
Distributed mode	Database Host:	localhost 🦻
Database	Database Port:	3306
Role configuration	Database User:	gmsuser
Reporting type	Database Password:	
Summary	Confirm Database Password:	······
	Database Driver:	org.mariadb.jdbc.Driver
	Database URL:	jdbc:mysql://localhost:3306
	< Back	Next >

MySQL Database

SQL Server Database

Install Mode Selection Tool		
Introduction	Step 4. Database	
	Enter the database parar	meters for the selected role: Console
Install mode	Database Type:	SQL SERVER 🔻 🔎
Distributed mode	Database Host:	P
Database	Database Port:	1433
Role configuration	Database User:	gmsuser 📁
Reporting type	Database Password:	9
Summary	Confirm Database Password:) I I I
	Database Driver:	com.microsoft.sqlserver.jdbc.SQLServerDrive
	Database URL:	jdbc:sqlserver://:1433
	< Back	Next >

- 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.

Install Mode Selection Tool		
Introduction	Step 6. Reporting type	
Install mode	Please select a report type that will be used in report generation for units added to the system.	
Distributed mode	Flow based Reports are generated using IPFIX packets for units that have reporting licensed and enabled. The Analytics feature will be available with this	
Database	selection.	
Role configuration	Syslog based Reports are generated using Syslog packets for units that have reporting enabled. Live Monitor feature will be available with this selection.	
Reporting type	None	
	Management only mode, Reports are disabled.	
Summary		
	< Back Next >	
	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

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

	Install Mode Sel	ection Tool
Introduction	Step 7. Summary	
Install mode	Following is a summary of the distributed environment settings:	
Distributed mode	Install mode	Custom
	Report type:	Flow based
Database	Role:	Console
Pala configuration	Database	
Role configuration	Database type:	MySQL
Departing to the	Database Host:	localhost
Reporting type	Database Port:	3306
_	Database User:	gmsuser
Summary	Database Password:	*****
	Click "Apply" and proceed to	complete the setup process.
	< Back	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.

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.

Introduction	Step 3. Distributed mode		
	Please choose the type of install.		
Install mode	Is this a Console?		
Distributed mode	The Console role is used in a multi-server GMS deployment. In this role, the server is configured to run all GMS Services.		
Database	Is this an Agent? Please provide the location of the Primary Console. Primary Console is the Primary host that will provide Database. License and other information to		
Role configuration	configure this agent. Host IP or Name: 10.206.23.188		
Reporting type			
Cummers and			

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.

Install Mode Selection Tool			
Introduction	Step 5. Role configuration		
Install mode	Select one of the following role(s Console (Redundant)	s): Details	
Distributed mode	Agent Monitor Event Manager	Details Details Details	
Database	 Flow Server 	Details	
Role configuration	To continue, click Next.		
Reporting type			
Summary			
	< Back Nex	xt >	

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.

Install Mode Selection Tool			
Introduction	Step 7. Summary		
Install mode	You have selected Custom as the installation mode, Flow based as reporting option and Flow Server as the role. Primary host for the Agent is 10.206.23.188		
Distributed mode	Click "Apply" and proceed to complete the setup process.		
Database			
Role configuration			
Reporting type			
Summary			
	< Back Apply		

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

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

Install Mode Selection Tool		
Introduction	Summary	
Install mode	Applying Install Mode and Role configuration settings. Please Wait	
Distributed mode	Performing database operations (applying db scripts, updates,)	
Database		
Role configuration		
Reporting type		
Summary		
	< Back Apply	

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

	Install Mode Selection Tool		
Introduction	Step 7. Summary		
Install mode	Install mode and Role configuration settings have been applied successfully.		
Distributed mode	Please click Finish to perform a restart of the system for the changes to take effect.		
Database			
Role configuration			
Reporting type			
Summary			

5 The system reboots to complete the installation process.

The SonicWall Universal Management Appliance is restarting.
Please wait

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.

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

GMS Registration

This section guides you through registering your GMS installation.

To register GMS (Console Only):

1 Enter your MySonicWall userid and password.

	Management Appliance 9.1
Please register your SonicWall pr	roduct
mySonicWall.com Login	Senai number, not registereu
mySonicWall.com is a one-stop upgrades and changes. mySon more information on mySonicV	p resource for registering all your SonicWall Internet Security Appliances and managing all your SonicWall security service nicWall provides you with an easy to use interface to manage services and upgrades for multiple SonicWall appliances. For Nall, please visit the <u>FAQ</u> . If you do not have a mySonicWall account, please click <u>here</u> to create one.
MuSonicWall username/email:	
Password:	
	Submit
Forgot your Licername or Passy	word?
rorgot your osemanie or rassy	NOLE .

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**.

	sal Management Applian	ce 9.1		
Follow the instructions belo	w for the product being	registered and hit Submit when	done	Serial Number: Not Registered
<u>GMS Deployment</u> : Serial Number:	Enter your 12-characte	r serial number, authentication c r 8 character serial number (SGx	ode and a friendly name. xxxxx) instead, <u>click here</u> .	
Authentication Code: Friendly Name:	JC2N -Q73C Wha GMS_Console1	t is this?		
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.

SONICWALL Universal Management Appliance 9.1	
	Serial Number: 00401027816E
This product has been registered successfully. Thank you for Registering.	
Continue	

4 Click Continue.

Adding Devices

7

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:

i) Please login	
Username	
Password	
LOGIN	

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

Add Unit		×
Basic		*
Unit Name:	NSA 3600	
Serial Number:	C0EAE4841488	
IP Address:	10.5.34.22	
Login Name:	admin	
Password:		
HTTPS Management Port:	443	\$
Reporting:	Flow based O Disabled	
Flow Server Agent IP:	10.206.23.188	*
Advanced		
	V OK X Cancel	

- 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.

cquisition History	
Unit Setup	
Setting up device parameters	
Device parameters setup in Global Management System completed.	
Fetch licenses for unit	
Licenses fetched successfully.	
Check unit licenses	
Unit is licensed for Management and Reporting	
Unit Acquisition	
Establish communication with the unit.	
Communication with unit successful.	
Perform unit acquisition.	
Unit successfully acquired.	
Check model code.	
Unit model code is valid.	
Reporting and Analytics Setup	
Check unit for Flow Reporting and Analytics feature support	
Unit supports Flow Reporting.	
Check licenses for Flow Reporting and Analytics	
Unit is licensed for Flow Reporting	
Check if Flow Agent was selected	
A Flow Agent has been selected for this unit.	
Check deployment for Flow Agent instance	
Atleast one Flow Agent found in the deployment.	
Perform Flow Server assignment	
Flow Agent assignment complete	
Perform configuration for Flows on unit	
Flow Configuration on unit complete.	
' Finished	

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.

i) Please login	
Username	
Password	
LOGIN	
2 Click the plus (+) sign at the top left of the GMS management interface. The Add Unit dialog box displays.

Add Unit		×
Basic		
Unit Name:	NSA 3600	
Serial Number;	C0EAE4841488	
IP Address:	10.5.34.22	
Login Name:	admin	
Password:		
HTTPS Management Port:	443	*
Reporting:	Flow based Disabled	
Flow Server Agent IP:	10.206.23.188	~
Advanced		(*)
Flow Server Agent IP: Advanced	10.206.23.188	

- 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.

dd Unit		
Basic		3
Unit Name:	NSA 3600	
Serial Number:	C0EAE4841488	
Login Name:	admin	
Password:	•••••	
Reporting:	Flow based O Disabled	
Flow Server Agent IP:	10.206.23.188	*
Advanced		3
Managed Address:	 Determine automatically Specify manually: 10.5.34.22 Make manual address sticky 	
Management Mode:	Using Existing Tunnel or LAN Using Management Tunnel Using SSL	
Management Port:	443	* *
Agent IP Address:		~
Standby Agent IP:	None	~

- 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:

aporemente	Engineering	~
ate:	California	¥
ountry:	USA	×
ompany:	SonicWALL	~

- 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.

equisition History		
Unit Setup		
Setting up device par	ters	
Device parameters se	in Global Management System completed.	
Fetch licenses for unit		
Licenses fetched suc	fully.	
Check unit licenses		
Unit is licensed for M	gement and Reporting	
Unit Acquisition		•
Establish communicat	with the unit.	
Communication with	t successful.	
Perform unit acquisiti		
Unit successfully acq	d.	
Check model code.		
Unit model code is vi		
Reporting and Anal	cs Setup	•
Check unit for Flow R	rting and Analytics feature support	
Unit supports Flow R	rting.	
Check licenses for Flo	eporting and Analytics	
Unit is licensed for Fl	Reporting	
Check if Flow Agent v	selected	
A Flow Agent has be	elected for this unit.	
Check deployment for	w Agent instance	
Atleast one Flow Age	ound in the deployment.	
Perform Flow Server a	anment	
Flow Agent assignme	omplete	
Perform configuration	Flows on unit	
Flow Configuration o	it complete.	
Finished		•
Finishing unit deployn	4	

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

Using the GMS Management Interface

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

SONICWALL	Global Management System 9.1 HOME MANAGE REPORTS ANALYT	ICS NOTIFICATIONS	🕘 🅘 Firewall 🔹 🗱
	GlobalView / System Status	CMS Workflow Try for free! User: a	dmin@LocalDomain Administrators Log
Updates	Status Information for Global Node: GlobalView		
Firmware & Backup	Firewall		
Licensing	Firewalls in the System		1
	Firewalls that are Not Registered		0
Current Status	Firewalls with VPN Upgrade		1
System Status	Firewalls that support MSSP		0
User Sessions	Firewalls with Global VPN Client Upgrade		0
SonicPoint Stations	Management		
Alerts	Firewalls that are Down		0
Tools	Firewalls that are Unacquired		0
System Tools	Firewalls with Pending Tasks		0
Network Diagnostics	Firewalls managed by Remote Instances		0
Network Topology	Firewalls managed using		
Monitors	Existing Tunnel/LAN		0
Test Capture ATP	Management Tunnel		0
street out the proceed of the	SSL		1
Connectivity	Firewalls with DHCP Server Enabled		1
3G/4G/Modem	Firewalls currently on Wireless		0

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**.

· · ·	Control Center
Appliance	
Control Center	
	gms91-installation-ca-fs O
Workflow	
Change Orders	Serial: 00401027816E
	IP Address: 10.206.23.188
Tasks	Role: Console - Flow Server
Current Status	OS: Linux (amd64-3.18.44-snwl- VMWare-x64)
Alerts	Memory: 16064 MB
Sessions	CPU: Intel Xeon (2.60 GHz) Cache: 30720 (4 Logical CPUs)
Snapshot Status	
Web Services	¢
	IPM Threshold Settings
Tools	Service Management Realtime Monitor
Debug Log Settings	
Paguast Spanshot	Historical View
Request Snapsnot	Firmware Upgrade
View Log	

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

stance (00401027816E)		
Threshold Settings		
CPU/Processor		
Severity: Medium		
60	80	75% Reset Apply
Severity: High		
85	95	90% Reset Apply
Memory/RAM		
Severity: Medium		
60	80	75% Reset Apply
Severity: High		
85	95	90% Reset Apply
Storage/Disk		
Severity: Medium		
50	75	65% Reset Apply
Severity: High		
80	95	85% Reset Apply
Estimated Capacity		
Severity: Medium		
50	75	65% Reset Apply
Severity: High		
80	95	85% Reset Apply
Capacity Estimation Settings		
Enforce Disk Capacity Estimation	Apply	

Realtime Monitoring



45

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.

e management		
Service	Status	Port
SonicWall Universal Management Suite - Scheduler	Started (Enabled)	2999
SonicWall Universal Management Suite - Reports Scheduler	Started (Enabled)	21001
SonicWall Universal Management Suite - Monitoring Manager	Started (Enabled)	21005
SonicWall Universal Management Suite - Syslog Collector	Started (Enabled)	21004
SonicWall Universal Management Suite - Flow Summarizer	Started (Enabled)	21026
SonicWall Universal Management Suite - Event Manager	Started (Enabled)	21010
SonicWall Universal Management Suite - Web Server	Started (Enabled)	
SonicWall Universal Management Suite - Database	Started (Enabled)	3306
SonicWall Universal Management Suite - Flow Server	Started (Enabled)	9064

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.

Log Management		Q Sea	irch Text	
Category	File Name	File Size	Modified Da	
Application Logs	aman-esxi-gmsvp91.eng.sonicwall.com.err	63,793,665	Mon Jul 09 2	
Application Logs	appflow.log	5,910,466	Mon Jul 09 2	
Application Logs	appflow.log.1	10,520,403	Sat Jul 07 20	
Application Logs	appflow.log.2	10,519,231	Sat Jul 07 20	
Application Logs	appflows.log	250,058	Mon Jul 09 2	
Application Logs	archive.log	28,368	Mon Jul 09 2	
Application Logs	BEPostUpdateManager0.log	3,265,302	Mon Jul 09 2	
Application Logs	DbgAppliance0.log	2,706,173	Mon Jul 09 2	
a 15 at a		*******		

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.

rmware Upgrade/Service Pack/Hotfix	
hoose the file	
+ Choose 🛓 Upload 🗙 Cancel	
C	
ginsvp-upuater-patch-omovP-9.1-1440+хо4-тегеазено-рузыт 700.525 мв	

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.

	Firewall •	\$	0
User: admin@LocalD	omain Admini	strators	Logout

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:



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

SONICWALL	Global Management System 9.1 HOME MANAGE REPORTS ANALYTICS NOTIFICATIO	NS 🕘 🕘 🔵 Firewall 🔹 🛱
	GlobalView / System Status	for free! User: admin@LocalDomain Administrators Log
Updates	Status Information for Global Node: GlobalView	
Firmware & Backup	Firewall	
Licensing	Firewalls in the System	1
	Firewalls that are Not Registered	0
Current Status	Firewalls with VPN Upgrade	1
System Status	Firewalls that support MSSP	0
User Sessions	Firewalls with Global VPN Client Upgrade	0
SonicPoint Stations	Management	
Alerts	Firewalls that are Down	0
Tools	Firewalls that are Unacquired	0
System Tools	Firewalls with Pending Tasks	0
Network Diagnostics	Firewalls managed by Remote Instances	0
Network Topology	Firewalls managed using	
Monitors	Existing Tunnel/LAN	0
Test Capture ATP	Management Tunnel	0
0.0000000000000000000000000000000000000	SSL	1
Connectivity	Firewalls with DHCP Server Enabled	1
3G/4G/Modem	Firewalls currently on Wireless	0

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.

(i) 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.
Θ	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.
0	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.
ÇD	One blue box with a lightning flash indicates that one or more tasks are pending or running on the appliance.
1	Two blue boxes with a lightning flash indicate that tasks are currently pending or running on two or more appliances within the group.
1	Three blue boxes with a lightning flash indicate that tasks are currently pending or running on three or more appliances within the group.
C	One blue box with a clock indicates that one or more tasks are scheduled on the appliance.
69	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.
6	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.
0	Two yellow boxes indicate that two or more appliances in the group have been added to SonicWall GMS management, but not acquired.
Θ	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.
F	One yellow box with a lightning flash indicates that one or more tasks are pending on the provisioned appliance.
B	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.
1	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.
2	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.
0	Two red boxes indicate that two or more appliances in the group are no longer sending heartbeats to SonicWall GMS.
0	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)

çà	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.
(B)	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.
3	A box with a dot in the top-left corner indicates that the appliance is being managed by GMS using a static IP address.
C	This icon indicates a fail over to a secondary Ethernet port.
Ċ	This icon indicates the a modem is connected using a dialup.
î ⁿ⁾⁾	This icon indicates the wireless is connected using WWAN.
8	This icon indicates the unit's Task Pending status is "Immediate."
Θ	This icon indicates the unit's Task Pending status is "Scheduled."
\$	Use this icon to switch between the Console, Appliance, or System views.

HOME View

9

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

Acquisition History	
Unit Setup	•
Unit Acquisition	
Reporting and Analytics Setup	•
► Finished	•
r rinisheu	
	Acquisition History Unit Setup Unit Acquisition Reporting and Analytics Setup Finished

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.

	SC X Y	New Range: 10 m	inutes	• *						
Annie atione #					-			and some	a) San Vitadas	_
proprietations								Concession of the second	• [[]]]	
P.K.										
11-24		33.08	23.04	22-54	12-08	11-08	33159	83/34	83-58	
et [_
Ingress Bandwidth®	Current Roel	4.3 Kbps	Miler: \$76.0 bps	Plan: 35.3 Khps				All Drowfaces Rate	Auto 1-Scaling	
£1					_					
* Egress Bandwidth #	Current Ave:	810.1 kSpx	Mine: 40-3 Klape	Max: 3.5 Mpr.						r
11-14		11/08	45108	41+47	11-10	51:09	11-10	\$1.15	44144	_
nda										
								THE RECEIPTION OF THE RECEIPTION	· Auto Videaless	_
Ingress Packet Rate®	Current Ave:	2 pps	Him: 1 pps	Has: 2 ppv				Al Interfaces Rate	a last the second	
Ingress Packet Rate	Current Ave:	2 709	Mine 1 pps	Has: 2 ppy				(47 Driverhause Rans		
Ingress Packet Rate	Current Ave:	.2 pps	Him: 1 pps	Hax: 2.001				el Interfacer Rate	1	
Ingress Packet Rate #	Carrent Ave:	2 pps	Him 1 pps	Has: 2.09				jel Interfaces Rans		
Ingress Packet Rate #	Current Ave:	2 001	Him: 1 ppr	Has 2 pry				Al Interfacer Rane		
Ingress Packet Rate #	Carrent Ave:	2 mm 507 gas	Him 1 pps	Has 2 per				Al Interfacer Rans		
Ingress Packet Rate #	Carrent Ave:	2 mm 507 gas 11 -14	Him 1 pps	Har: 2 pp Har: Of pp Har: Of pp	11-04	12-08	11:18	Al Interface Rate	11-12	
Togress Packet Rate #	Current Are:	2 mm 587 gas 11-16	Han Lyre Han Lyre Han Lyre 11-14	Hare 2 per	53-64	11-68	11-18	El trachese Ravi	8.0	
Ingress Packet Rate #	Current Are:	2 pps 502 pps 11-08	Has 1 pro	Hare 2 ppp Hare Of ppp Mare Of ppp	11.64	11-08	55-18	El trachese Rave	11-12	

() 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
- Universal Scheduled Reports
- My Default Page

Universal Dashboard

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

Ceographic View	[Nodes: Total:34 Up:17 Down:10 Other:7]			
Sou il the objects of	San Francisco San Bardon Control Contr	And the second s	Mantraa Verate Proston Priser Vork Massington be	nu seons
Scheduled Tasks		T Stes		
Description	Sc Scheduled Time(Local)	Appliance Name Hits	Transferred	
Request Active Connections infr	ormation N., Dec 12, 2011 Mon [01:44 PM]	NSA 240 59F1 203,675	393 MB	
egister/Update unit with mySo	mcWA t Dec 13, 2011 Tue [00:07 AM]	E5000 6064.121 6,443	35.93 MB	
dd New Match Object: match I	foo [cr 5 Dec 8, 2011 Thur [08:47 FM]	Test 240 2,940	20.05 MB	
ave firewall prefs file	S IMMEDIATE	Test-210w Desk 1.079	7.55 MB	
ave firewall prefs file	T IMMEDIATE	PRO 1240 4260	146.1348	
ave firewall prefs file	T IMMEDIATE	the last dealer of the		
ave firewall prefs file	s IMMEDIATE			
ave frewall crefs file	E IMMEDIATE			

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.



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
- My Default Page

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 (i) about using and configuring the Universal Dashboard.

60

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
- Current Status
- Tools
- Connectivity
- Policies
- System Setup
- Security Configuration
- Logs and Reporting

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

(i) **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

(i) **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.

(i) 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.

(i) 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

Status	Status Information for Unit Node: LAB - NSA5600 (D376) Acquisition History	
Sessions	▶ Unit Setup	٠
Traffic	Unit Acquisition	
Threats	Reporting and Analytics Setup	•
URL Blocked	► Finished	
Flows		
Monitor		

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

										10	
Traffic											
en	Onen Time	- Artist	· Instruction	· Inc. Orberton	w Jaco Bink	w finanture	- 1e8 10	a Data 10	- Init Country	a Base Country	a fait Bast
₫ #>	10:58:42 Dec 12	Allowed	S & General DNS	Networking	a low	S General DNS	¥ 10.204.67.205	¥ 10.50.129.148	N ROT Private IP	N K2C Private IP	× 61287
a	10:58:41 Dec 12	Aloved	X @General DNS	Networking	Niew	49169 M General DNS	10.204.67.206	10.50.129.149	N NOT Private IP	N N27 Private IP	X 61286
() () () () () () () () () () () () () (10:58:41 Dec 12	Allowed	N DIS Protocol	T PROTOCOLS	Milow	49169 3 DNS Protocol	172.16.31.233	10.50.129.148	N ROT Private IP	N K2C Private IP	× 49942
A.	10:58:41 Dec 12	Allowed	N DNS Protocol	PROTOCOLS	NLow	5818 3 DNS Protocol	172.16.31.233	10.50.129.148	The Private IP	N NT Private IP	X 59050
a + •	10:58:41 Dec 12	Mowed	3 DNS Protocol	M PROTOCOLS	NLow	3 DNS Protocol	× 172.16.31.233	× 10.50.129.148	Trivate 1P	IN NOT Private IP	× 58513
a .	10:58:41 Dec 12	Alowed	M DNS Protocol	PROTOCOLS	N Low	N DNS Protocol	× 172.16.31.233	× 10.50.129.148	N Trivate IP	M Trivate IP	× 65072
a + +	10:58:41 Dec 12	Allowed	3 DNS Protocol	FROTOCOLS	NLow	3 DNS Protocol	172.16.31.233	10.50.129.148	K Trivate 1P	1 Private 1P	× 60783
<i>d</i> + •	10:58:41 Dec 12	Allowed	M DNS Protocol	PROTOCOLS	NLow	N DNS Protocol	172-16-31-233	× 10.50.129.148	IN NOT Private IP	IN THE Private IP	× 62253
a + +	10:58:41 Dec 12	X Alowed	3 DNS Protocol	M PROTOCOLS	X Low	3 DNS Protocol 6818	172.16.31.233	10.50.129.148	K Strate IP	N 122 Private IP	× 53595
<i>.</i>	10:58:41 Dec 12	X Alowed	IN DNS Protocol	M PROTOCOLS	NLow	% DNS Protocol	× 172-16-31-233	× 10.50.129.148	📧 👥 Private 3P	M Trivate IP	X 6381
<i>(</i>	10:58:41 Dec 12	Blocked by access	🕱 🖨 General UDP	× Networking	IN Low	General UDP 49202	172.16.31.233	× 17.173.254.222	IN THE Private IP	Inited States	X 1640
a 🔺 🕨	10:58:41 Dec 12	Blocked by access rule	🕱 🖨 General UDP	Ketworking	IN Low	General UDP 49202	× 172-16-31-233	× 17.173-254-222	IN NOT Private IP	📧 🔜 United States	N 1640
() (10:58:41 Dec 12	Blocked by access rule	🕱 📾 General UDP	× Networking	IN Low	General UDP 49202	× 172.16.31.233	× 17.173.254.223	IN THE Private IP	📧 📷 United States	× 1640
<i>d</i> + +	10:58:41 Dec 12	X Alowed	M General HTTPS	M Networking	N Low	3 General HTTPS 49177	X 172-16-31-233	× 52.112.67.109	📧 👥 Private IP	🕱 🎫 United States	× 53252
a + +	10:58:41 Dec 12	Mowed N	St. @ General HTTPS	Ketworking	NLow	3 General HTTPS 49177	172.16.31.233	× 104.92.130.125	K Trivate 1P	🕱 🌉 United States	3 53253
() *	10:58:41 Dec 12	Allowed	M @ General HTTPS	Ketworking	N Low	3 General HTTPS 49177	× 172-16-31-233	\$2.112.67.109	📧 🏋 Private IP	🕱 🗾 United States	33254
() * •	10:58:37 Dec 12	Allowed N	🕱 🖨 General DNS	Ketworking	IN Low	3 General DNS 49169	10.204.67.206	× 10.50.129.148	📧 👥 Private 1P	1% Trivate 1P	X 61285
() * •	10:58:07 Dec 12	X Allowed	S General DNS	Ketworking	IN Low	3 General DNS 49169	× 10.204.67.205	× 10.50.129.148	📧 😭 Private IP	📧 👥 Private IP	X 49153
a + +	0.23.33.0	W strend	*	W Halton data	No. of Concession, Name	3 General DNS	N 10.301 23.302	W 10 20 130 140	W PT Palanta III	N. 18-187 Part-rate 10	W LITER

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.

Ap	plications	Users	Web Activities Sources Destinations TI	ireats VoIP Devices Contents BWH		Greep Bys Applic	atons • 😹 💮 2
1.6	<u>×</u>	Search:					
	*		Application	Sessions	Total Packets	Total Bytes 👻	Threats
	1	14	3 🖷 General DNS	N 140	674	59.52K	0
	2	76	📧 👄 General HTTPS	n, 8	45	17.43K	0
	3	14	36 DNS Protocol	0 21	44	5.06K	0
	4	74	3 👁 General HTTPS MGHT	0 ₆ 2	24	4.49K	0
	5	14	35 🐟 Service NTP	≤ 1	10	760	0
	6	W	35 🐟 Service SHB	9 ₄ 12	12	608	0
	7	14	📧 📾 General UDP	Q 9	9	396	0
	8	X	3 👁 Service DCE EndPoint	G 6	6	304	0
	9	W	📧 👄 General HTTP	0 <u>4</u> 2	2	128	0
	10	4	31 🖷 Senice Edia	S. 1	1	48	0
	10	x	(R. ● Senies Edu	× 1	1	43	

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

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
- Real-Time Syslog
- Live Monitor

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

(i) 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.
SonicWall Support

Α

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

 \wedge

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. (i)

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

Copyright © 2018 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 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 BAY 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. Select the language based on your geographic location to see the EUPA that applies to your region.

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