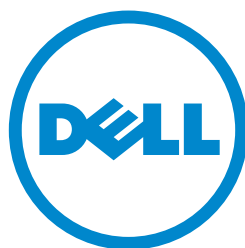# GMS 7.2 Virtual Appliance
Getting Started Guide

DELL SonicWALL

Notes, Cautions, and Warnings

NOTE: A NOTE indicates important information that helps you make better use of your system.

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

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

Overview

This Getting Started Guide contains installation procedures and configuration guidelines for deploying Dell SonicWALL GMS as a Virtual Machine in a VMware environment. The Dell SonicWALL GMS Virtual Appliance can configure, manage, and monitor the status of thousands of Dell SonicWALL Internet security appliances and non-Dell SonicWALL appliances from a central location. The Dell SonicWALL GMS Virtual Appliance provides the following benefits:

- Centralized security and network management
- Sophisticated VPN deployment and configuration
- Active device monitoring and alerts
- Intelligent reporting and activity visualization
- Centralized logging and offline management

This document contains the following sections:

Chapter 1

Before You Begin

See the following sections for information about Dell SonicWALL GMS Virtual Appliance:

- System Requirements on page 5
- Record Configuration Information on page 8

System Requirements

The Dell 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:
http://www.sonicwall.com/us/Products_Solutions.html

Before installing, review the requirements in the following sections:

GMS Virtual Appliance Supported Platforms

The elements of basic VMware structure must be implemented prior to deploying the Dell SonicWALL GMS Virtual Appliance. The Dell SonicWALL GMS Virtual Appliance runs on the following VMware platforms:

- ESXi 4.1, 5.0, 5.1, and 5.5
- ESXi 4.0 Update 1 (Build 208167 and newer)
- ESX 4.1
- ESX 4.0 Update 1 (Build 208167 and newer)
- Microsoft Hyper-V

Deployment Considerations

Consider the following before deploying the GMS Virtual Appliance:

- Dell SonicWALL GMS management is not supported on Apple MacOS.
- All modes of the application run in 64-bit mode.
- Using the Flow Server Agent role requires a minimum of:
  - Quad Core
  - 16GB of memory
  - 300 HDD

GMS Virtual Appliance Hardware Resource Requirements

Use the Capacity Calculator 2 to determine the hardware requirements for your deployment.

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

Starting with GMS 7.1 the Virtual Appliances are 64-bit, which take advantage of the additional RAM available to it. A minimum of 4GB RAM is required. However, 8GB of RAM is highly recommended for better performance of reporting modules. Read the "Capacity Planning and Performance Tuning" appendix in the *GMS Administrator's Guide*.

MySQL Requirements

Dell SonicWALL GMS automatically installs MySQL as part of the base installation package. Separately installed instances of MySQL are not supported with Dell SonicWALL GMS.

Java Requirements

Download and install the latest version of the Java 7 plug-in on any system that accesses the GMS management interface. This can be downloaded from:
www.java.com
or
http://www.oracle.com/technetwork/java/javase/downloads/index.html

Browser Requirements

Dell SonicWALL GMS uses advanced browser technologies such as HTML5 that are supported in most recent browsers. Dell SonicWALL recommends using the latest Chrome, Firefox, Internet Explorer, or Safari browsers for administration of the Dell SonicWALL GMS.

This release supports the following Web browsers:

- Google Chrome 18.0 and higher (recommended browser for dashboard real-time graphics display)
- Mozilla Firefox 16.0 and higher
- Microsoft Internet Explorer 8.0 and higher (do not use compatibility mode)

Note Internet Explorer version 10.0 in Metro interfaces of Windows 8 is currently not supported.

Mobile device browsers are not recommended for Dell SonicWALL GMS system administration.

Network Requirements

To complete the Dell SonicWALL GMS Virtual Appliance deployment process documented in this *Getting Started Guide*, the following network requirements must be met:

- The Dell SonicWALL GMS server must have access to the Internet
- TheDell SonicWALL GMS server must have a static IP address

- The Dell SonicWALL GMS server's network connection must be able to accommodate at least 1KB/s for each device under management. For example, if Dell SonicWALL GMS is monitoring 100 Dell SonicWALL appliances, the connection must support at least 100KB/s.

Note Depending on the configuration of Dell SonicWALL log settings and the amount of traffic handled by each device, the network traffic can vary dramatically. The 1KB/s for each device is a general recommendation. Your installation requirements might vary. Refer to the Capacity Calculator 2.

Dell SonicWALL Appliance and Firmware Support

Dell SonicWALL Platforms	Dell SonicWALL Firmware Version
Firewall / VPN	
SuperMassive 10000 Series	SonicOS 6.0 or newer: Note: Only partial policy management and reporting support is currently available. The following SuperMassive specific features are not supported for centralized policy management in GMS 7.2: • Multi-blade CASS • High Availability/Clustering • Support for Management Interface • Flow Reporting Configurations • Multi-blade VPN • Advanced Switching • Restart: SonicOS versus Chassis Contact your Dell SonicWALL Sales representative for more information.
SuperMassive 9000 Series	SonicOS 6.1 or newer
NSA Series	SonicOS Enhanced 5.0 or newer
TZ Series	SonicOS Enhanced 3.2 or newer SonicOS Standard 3.1 or newer
PRO Series	SonicOS Enhanced 3.2 or newer
CSM Series	SonicOS CF 2.0 or newer
Secure Remote Access	
SMB SRA Series	SonicOS SSL-VPN 2.0 or newer (management) SonicOS SSL-VPN 2.1 or newer (reporting)
E-Class SRA Series	SRA 9.0 or newer
Backup and Recovery	
CDP Series	CDP 2.3 or newer (management) CDP 5.1 or newer (reporting)
Email Security / Anti-Spam	
Email Security Series	Email Security 7.2 or newer (management only)

Note Dell SonicWALL GMS supports Dell SonicWALL firewall App Control policy management and reporting. For SonicOS firewall App Control policy management support, use a Dell SonicWALL firewall running SonicOS 5.8.1.4 or newer. And for SonicOS firewall App Control reporting support, use a Dell SonicWALL firewall running SonicOS 5.8.1.0 or newer.

Appliances running firmware newer than this GMS release can still be managed and reports can still be generated. However, the new features in the firmware release will be supported in an upcoming release of GMS

Legacy SonicWALL XPRS/XPRS2, SonicWALL SOHO2, SonicWALL Tele2, and SonicWALL Pro/Pro-VX models are not supported for SonicWALL GMS management. Appliances running SonicWALL legacy firmware including SonicOS Standard 1.x and SonicWALL legacy firmware 6.x.x.x are not supported for SonicWALL GMS management.

Non-Dell SonicWALL Appliance Support

Dell SonicWALL GMS provides monitoring support for non-Dell SonicWALL TCP/IP and SNMP-enabled devices and applications.

Record Configuration Information

Before continuing, record the following configuration information for your reference.

SMTP Server Address:	The IP address or host name of your Simple Mail Transfer Protocol (SMTP) server. For example, mail.emailprovider.com.
HTTP Web Server Port:	The number of your Web server port if customized. The default port is 80.
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.
GMS Gateway IP:	The IP address of the GMS gateway between the GMS agent and the network. This optional field is only applicable if you have a GMS gateway.
GMS Gateway Password:	The password for the GMS gateway. This optional field is only applicable if you have gateway between the GMS and the network.
Database Vendor:	Your database vendor if you are using a SQL Server database.*

Database Host/IP:	The IP address of the database host. This is not required when using the bundled database on this server.*
Database User:	The MySQL user name for the database administrator. This is not required when using the bundled database on this server.*
Database Password:	The MySQL password for the database administrator. This is not required when using the bundled database on this server.*

*This information is needed if Microsoft SQL Server is used, or in the case of a distributed deployment.

Chapter 2

Introduction to the Management Interfaces

This section describes the two Dell SonicWALL GMS management interfaces. An almost identical URL is used when accessing either the Dell SonicWALL GMS management interface or the Universal Management Host system interface, but the URL is modified to specify either "sgms" or "appliance."

See the following sections:

Overview of the Two Interfaces

The Universal Management Suite (UMS) installs two separate management interfaces:

- **Dell SonicWALL Universal Management Host (UMH) System Management Interface** – Used for system management of the host server, including registration and licensing, setting the admin password, selecting the deployment role, and configuring other system settings.

  To access the UMH system management interface on the default HTTP port using a browser on the host server, use the URL:
  http://localhost/appliance/

  From another system, access the UMH system management interface with the URL:
  http://<IP address>:<port>/appliance/

  If you are using the standard HTTP port, 80, it is not necessary to append the port number to the IP address.

- **Dell SonicWALL GMS Management Interface** – Used to access the Dell SonicWALL GMS application that runs on the Windows server. This interface is used to configure GMS management of Dell SonicWALL appliances, including creating policies, viewing reports, and monitoring networks, and for configuring GMS administrative settings. The GMS management interface is only available on systems deployed in a role that runs the Web Server service, such as the All In One or Console roles.

  Access the GMS management interface with one of the following URLs:
  http://localhost/sgms/
  or
  http://<IP address>:<port>/sgms/

Switching Between Management Interfaces

On systems deployed in the All In One or Console role, the "superadmin" user can easily switch between the UMH system management interface and the Dell SonicWALL GMS management interface. The SuperAdmin is the master administrator for the entire GMS installation.

When logged in to either interface, the superadmin can switch to the login page of the other interface by clicking **Switch** in the top right corner of the page. **Switch** is only visible for users with SuperAdmin privileges.

UMH System Interface Introduction

The Dell SonicWALL UMH system interface is used for system management of the Dell SonicWALL GMS instance, including registration and licensing, setting the admin password, configuring database settings, selecting the deployment role, and configuring other system settings.

When installing Dell SonicWALL Universal Management Suite on a host, a Web server is installed to provide the system management interface. The system interface is available by default at *http://localhost/appliance/* after restarting the system.

The login screen allows you to securely log in to the Dell SonicWALL UMH system interface using your system user ID and password.

Note   The admin account on the system interface can have a different password than the admin account for Dell SonicWALL GMS.

Management Interface Introduction

Dell SonicWALL GMS is a Web-based application for configuring, managing, monitoring and gathering reports from thousands of Dell SonicWALL Internet security appliances and non-Dell SonicWALL appliances, all from a central location. This section provides an introduction to the main elements of the Web-based management interface. This section contains the following subsections:

- Login Screen on page 11
- Dashboard on page 12
- Management Interface on page 13

Login Screen

The login screen allows you to securely log in to Dell SonicWALL GMS using your GMS application user ID and password. The Dell SonicWALL GMS management interface is available by default at *http://localhost/sgms/* after completing registration.

Dashboard

The Dashboard tab is a customizable dashboard of your Dell SonicWALL GMS deployment. The Dashboard tab provides powerful network visualization reporting, monitoring, and search filtering tools consolidated into one area of the management user interface. The Dashboard tab provides administrators with an executive summary through a **Universal Dashboard** geographic map. As depicted in the figure that follows, the Geographic View provides a scalable map that displays your GMS-managed units and servers using graphical icons, these icons provide system state information with a mouse over.

The Dashboard tab also provides administrators with a centralized location to create **Universal Scheduled Reports** for Firewall, SRA, CDP, and Email Security reporting solutions.

For more information on configuring the Universal Dashboard and Universal Scheduled Reports, refer to the "Using the Dashboard Panel" chapter in the *GMS Administrator's Guide*.

Management Interface

The Dell SonicWALL GMS management interface is the main control panel for GMS. The management interface allows you to add and modify appliances, complete monitoring and reporting tasks, set policies for managed appliances, and configure settings.
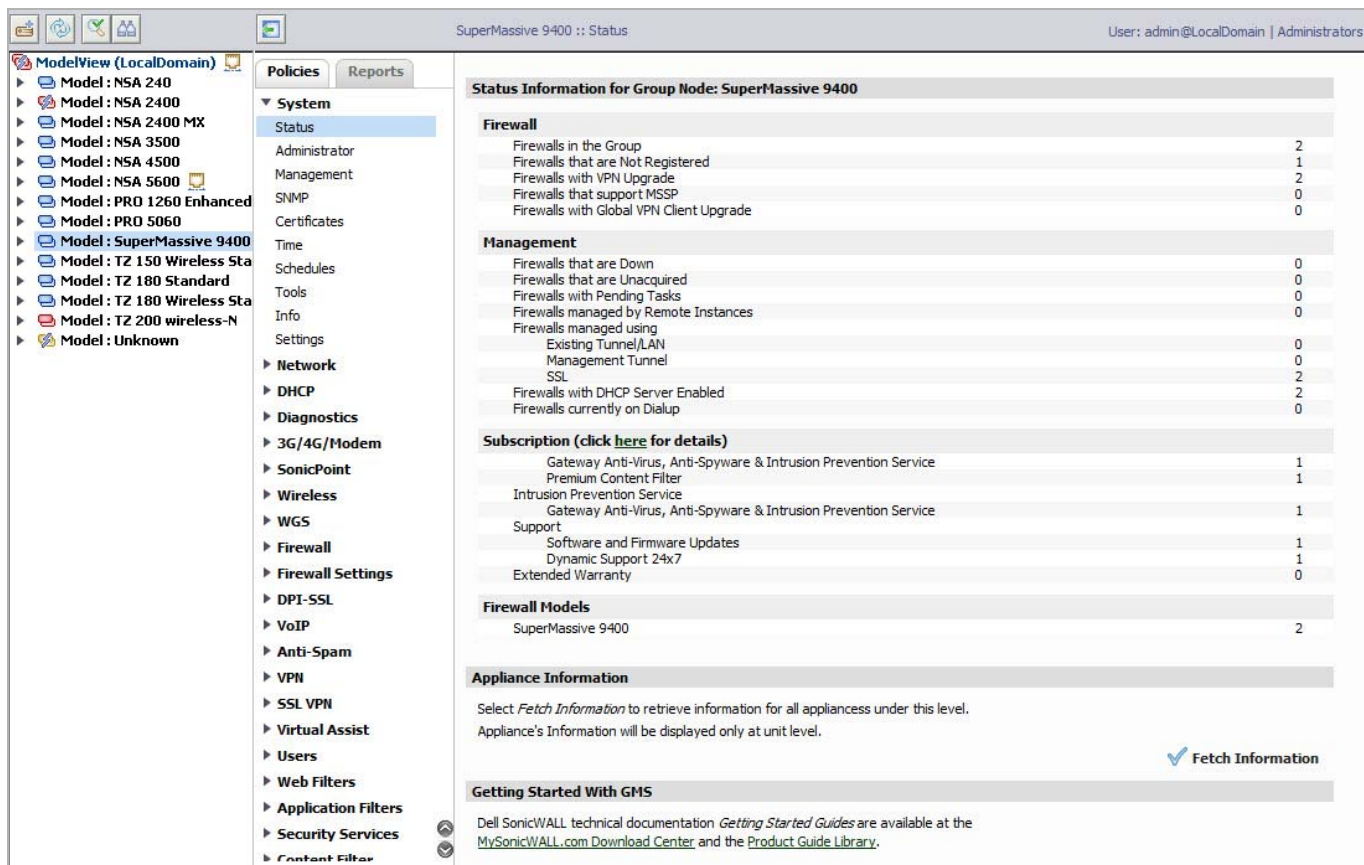
The GMS management interface features the following navigation features:

Navigation Tabs

The Dell SonicWALL GMS management interface navigation tabs are located at the top of the management interface.

The navigation tabs are: Dashboard, Firewall, SRA, CDP, ES, Monitor, and Console. The Monitor tab provides real-time monitoring at the global, group or appliance level. The Console tab provides tools to customize options found in the other Dell SonicWALL GMS tabs and manage GMS settings that affect the environment globally.

Left Pane
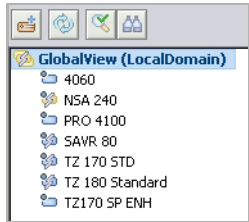
The left pane of the Dell SonicWALL GMS management interface provides a tree control that displays the current GMS view and a list of managed appliances within the current tab. The left pane is only displayed in the appliance tabs (Firewall, SRA, CDP and ES). The current category and view are indicated by a blue highlighting.

The left pane tree control provides the ability to switch between views and displays the current state of each appliance under management. A single box in the tree control indicates a node at appliance or unit level. Two boxes in the tree control indicates a node at a group level. A global node at the top of the tree control is indicated by a three-box icon. The color and additional images superimposed on these icons provide useful status information. For detailed information about appliance states, refer to Description of Managed Appliance States on page 15.

Note If there is only one appliance visible in the Left Pane, then the Left Pane automatically collapses to present a larger screen for the rest of the UI.

Center Pane
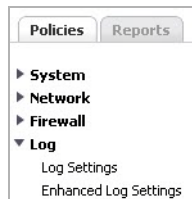
The center pane displays for the four appliance tabs (Firewall, SRA, CDP, and ES). A navigational tree control that provides access to the configuration options available based on navigational tab and left pane selections. At the top of the Center pane there are two sub-tabs: Policies and Reports. The Policies sub-tab provides policy configuration options for managed appliances. The Reports sub-tab provides reporting on the global, group, or appliance level, and is only available for Firewall, SRA, and CDP.

The current selection in the center pane is indicated by the highlighted item. For example, the figure to the left displays the current selection **Log > Log Settings**. The center pane options change based on the navigational tab and left pane selections, and selections in the center pane modify the display in the right pane. For example, the figure in the next section illustrates the contents of the right pane when the global view is selected in the left pane and **System > Status** is selected on the **Policies** tab in the center pane.

Right Pane

The right pane displays the available status or tasks based on the current selection of navigational tab, left pane and center pane options. Configurations completed in the right pane modify global, group or appliance settings. For example, the right pane image that follows displays the status and tasks available for the **Policies** navigation tab, left pane selection **GlobalView**, and center pane selection **System > Status**.

Status Information for Global Node: ModelView	
UTM	
UTMs in the System	29
UTMs that are Not Registered	6
UTMs with VPN Upgrade	25
UTMs that support MSSP	1
UTMs with Global VPN Client Upgrade	12
Management	
UTMs that are Down	8
UTMs that are Unacquired	5
UTMs with Pending Tasks	8
UTMs managed by Remote Instances	2
UTMs managed using	
Existing Tunnel/LAN	6
Management Tunnel	0
HTTPS	23
UTMs with DHCP Server Enabled	23
UTMs currently on Dialup	0
Subscription (click here for details)	
Anti-Virus	1
Content Filter List/Service	2
Extended Warranty	17
Gateway Anti-Virus	2
Intrusion Prevention Service	2
UTM Models	
NSA 240	2
NSA 3500	1
NSA 4500	1
NSA E5000	1

Description of Managed Appliance States

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

Status Icon	Description
	One blue box indicates that the appliance is operating normally. The appliance is accessible from SonicWALL GMS, and no tasks are pending or scheduled.
	Two blue boxes indicate that appliances in a group are operating normally. All appliances in the group are accessible from SonicWALL GMS and no tasks are pending or scheduled.
	Three blue boxes indicate that all appliances in the global group of this type (Firewall/SRA/CDP) are operating normally. All appliances of this type are accessible from SonicWALL GMS and no tasks are pending or scheduled.
	One blue box with a lightning flash indicates that one or more tasks are pending or running on the appliance.
	Two blue boxes with a lightning flash indicate that tasks are currently pending or running on one or more appliances within the group.
	Two blue boxes with a clock indicate that tasks are currently scheduled to execute at a future time on one or more appliances within the group.

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

Installing and Upgrading

The SonicWALL GMS Virtual Appliance is installed by deploying an OVA file to your ESX/ESXi server. Each OVA file contains all software components related to Dell SonicWALL GMS Virtual Appliance including the MySQL database, executable binary files for all GMS services, and other necessary files.

You can deploy one or both OVA files multiple times as needed for your Dell SonicWALL GMS Virtual Appliance environment. Dell SonicWALL GMS Virtual Appliance can be configured for a single server or in a distributed environment on multiple servers. In a distributed deployment, for example, you might use the 250GB file in a Summarizer role, and the 950GB file in a Database role. A distributed deployment can include one or more SonicWALL GMS Virtual Appliances, SonicWALL UMA EM5000s, or Dell SonicWALL GMS Virtual Appliance instances running on Windows Server machines.

You can deploy an OVA file by using the vSphere client that comes with ESX/ESXi. To get the vSphere client, point a browser to your ESX/ESXi server and click on **Download vSphere Client**.

Dell SonicWALL GMS Virtual Appliance can be installed as a fresh install, or as an upgrade to the latest version of GMS Virtual Appliance.

This section contains the following subsections:

- Installing with VMware vSphere on page 17
- Upgrading From an Earlier Version of Dell SonicWALL GMS on page 24

Installing with VMware vSphere

To do a fresh install of the SonicWALL GMS Virtual Appliance using the vSphere client, complete the following steps:

Step 1   Download the following OVA files from MySonicWALL to a system that is accessible to your ESX/ESXi server.

- sw_gmsvp_vm_eng_7.2.*xxxx.yyyy*.40GB.64bit.ova
- sw_gmsvp_vm_eng_7.2.*xxxx.yyyy*.250GB.64bit.ova
- sw_gmsvp_vm_eng_7.2.*xxxx.yyyy*.950GB.64bit.ova
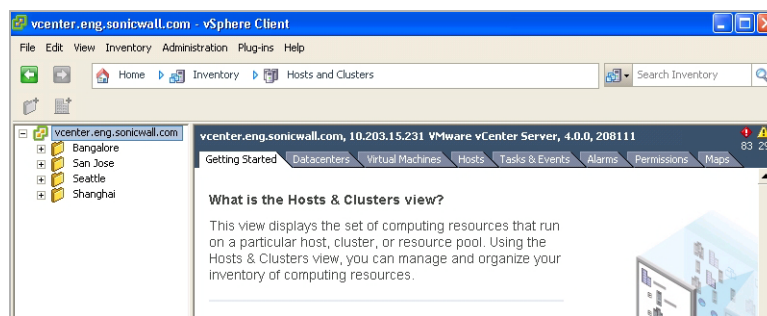
Note   Do not rename the OVA files.

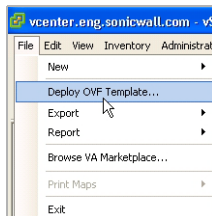The "xxxx" represent the exact version numbers

Step 2   Launch vSphere and use it to log on to your ESX/ESXi server.


Step 3   In the Home screen, navigate to a view that shows the virtual machines running on your ESX/ESXi server.


Step 4   To begin the import process, click **File** and select **Deploy OVF Template**.


Step 5   In the Source screen of the Deploy OVF Template window, enter the name of the OVA file to import in the **Deploy from a file or URL** field. To deploy from a file, click **Browse** and then select the OVA file to import. To deploy from a URL, type in the URL of the OVA file. Click **Next**.
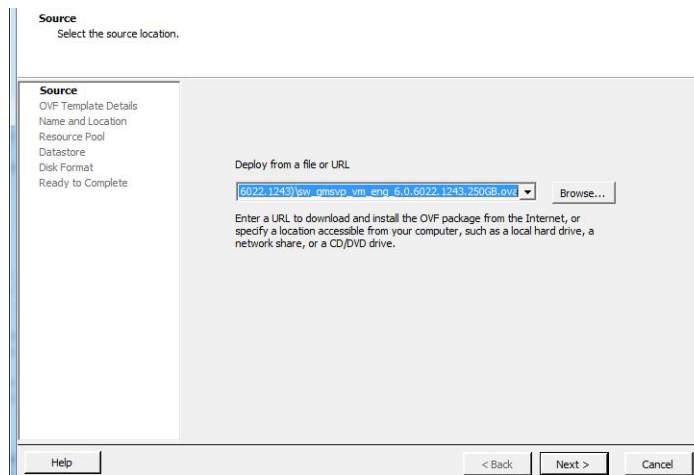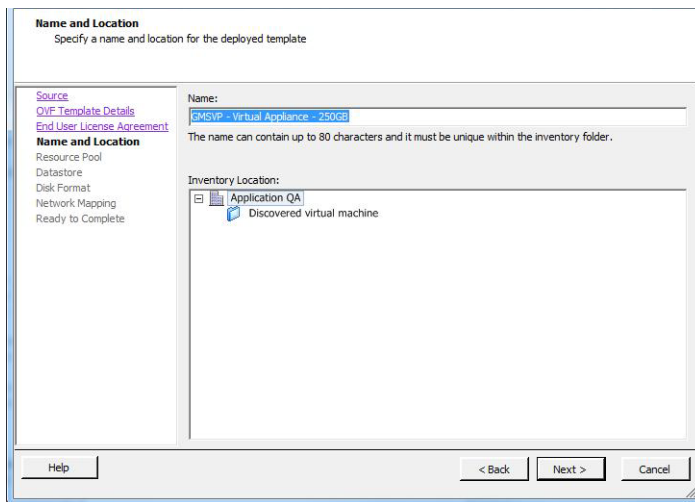
Step 6   In the OVF Template Details screen, verify the information about the selected file. To make a change, click the <u>**Source**</u> link to return to the Source screen and select a different file. To continue, click **Next**.
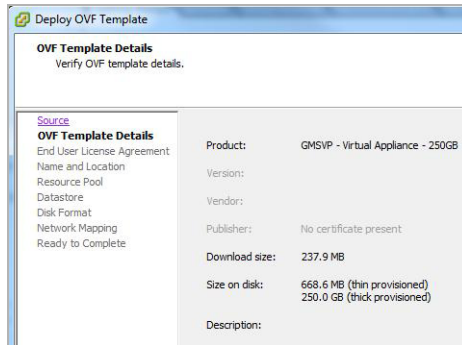
Step 7   In the End User License Agreement screen, read the agreement, click **Accept**, and then click **Next**.
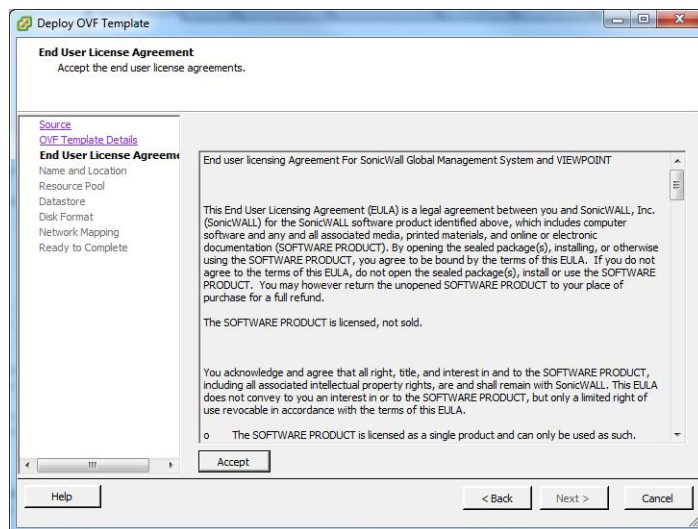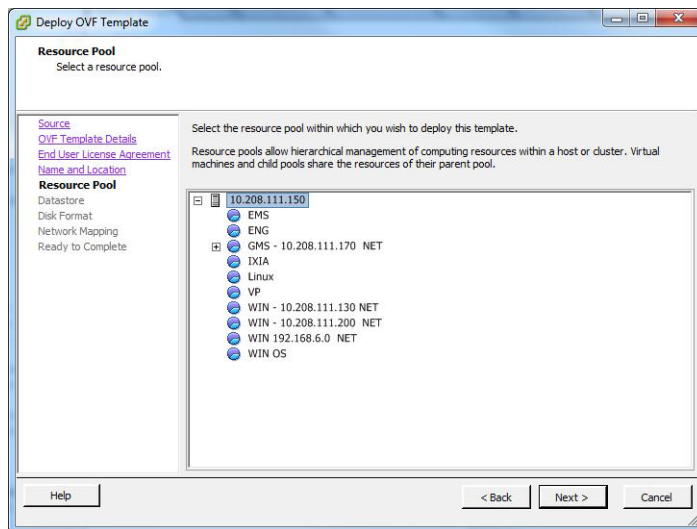

Step 8   In the Name and Location screen, enter a descriptive name for the virtual appliance into the **Name** field, and select the desired location in the **Inventory Location** field. You might wish to incorporate the role or disk size as part of the name, as in "GMS_VM_Agent_250GB." Click **Next**.

Name and Location
Specify a name and location for the deployed template

Source
OVF Template Details
End User License Agreement
Name and Location
Resource Pool
Datastore
Disk Format
Network Mapping
Ready to Complete

Name:
GMSVP - Virtual Appliance - 250GB
The name can contain up to 80 characters and it must be unique within the inventory folder.

Inventory Location:
Application QA
  Discovered virtual machine

Help   < Back   Next >   Cancel

Step 9   In the Resource Pool screen, select the resource pool within which to deploy this SonicWALL GMS Virtual Appliance and then click **Next**.

Note   When deploying a 950GB file, be sure to select a resource pool with a block size of either 4 or 8MB.

Deploy OVF Template

Resource Pool
Select a resource pool.

Source
OVF Template Details
End User License Agreement
Name and Location
Resource Pool
Datastore
Disk Format
Network Mapping
Ready to Complete

Select the resource pool within which you wish to deploy this template.

Resource pools allow hierarchical management of computing resources within a host or cluster. Virtual machines and child pools share the resources of their parent pool.

10.208.111.150
  EMS
  ENG
  GMS - 10.208.111.170 NET
  IXIA
  Linux
  VP
  WIN - 10.208.111.130 NET
  WIN - 10.208.111.200 NET
  WIN 192.168.6.0 NET
 WIN OS

Help   < Back   Next >   Cancel

Step 10 In the Datastore screen, select the datastore on which to store the files for the SonicWALL GMS Virtual Appliance and then click **Next**.
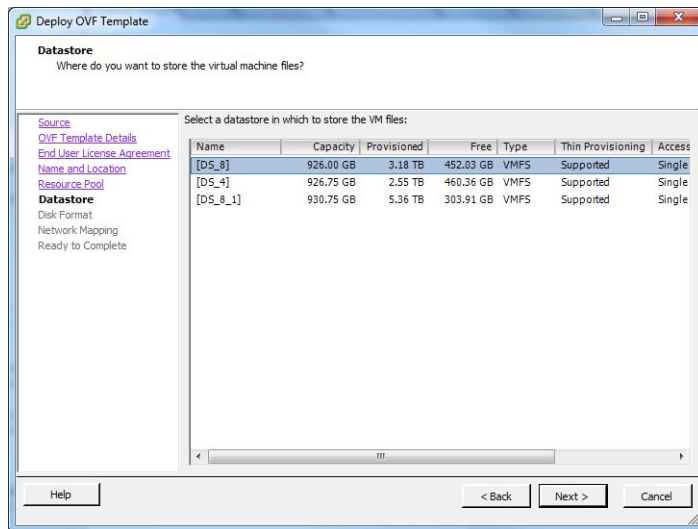
Step 11 In the Disk Format screen, select the format in which to store the virtual disks for the SonicWALL GMS Virtual Appliance. Select either **Thin provisioned format** or **Thick provisioned format**, and then click **Next**.
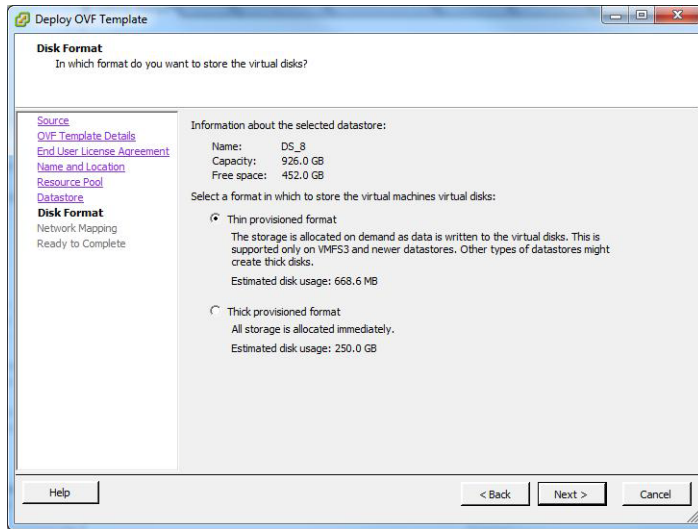
Step 12 In the Network Mapping screen, select the networks in your inventory to be used for the SonicWALL GMS Virtual Appliance, and then click **Next**.
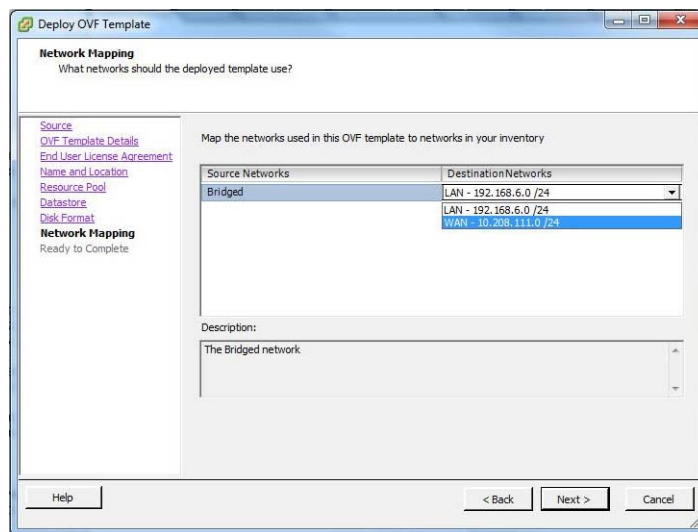
Step 13 In the Ready to Complete screen, review and verify the displayed information. To begin the deployment with these settings, click **Finish**. Otherwise, click **Back** to navigate back through the screens to make a change.
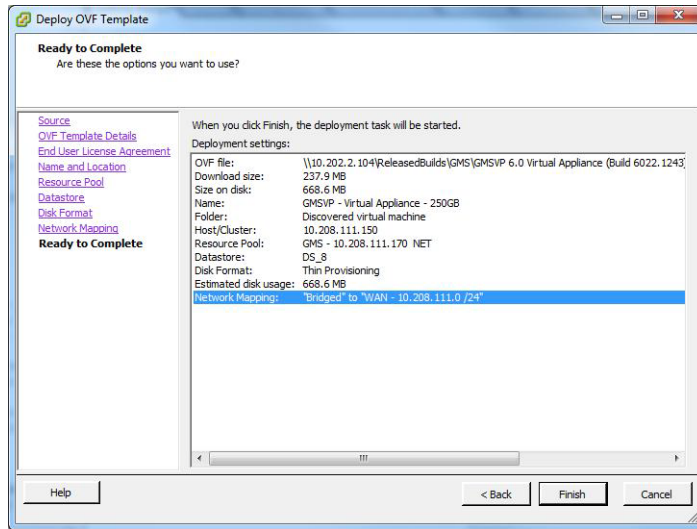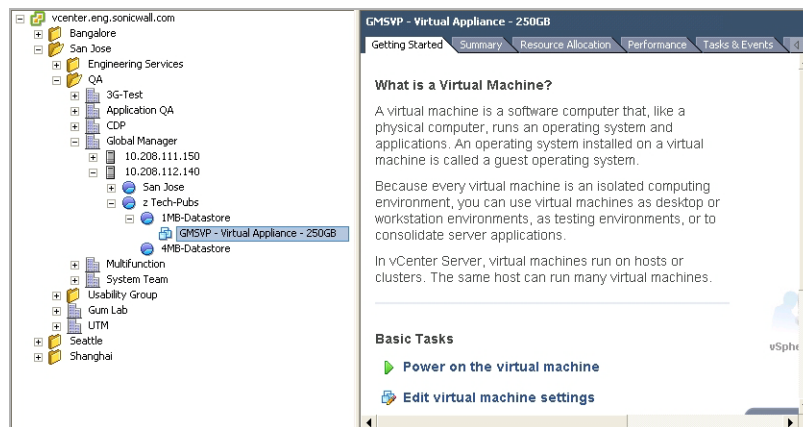

The Deploying dialog box shows the progress.

Step 14 In the Deployment Completed Successfully dialog box, click **Close**.

The name of the new SonicWALL GMS Virtual Appliance appears in the left pane of the vSphere window.

Step 15 To power on the virtual appliance and complete required host configuration, see Performing Basic Tasks and Host Configuration on page 25.

Step 16 After completing the basic tasks and host configuration, register and license SonicWALL GMS, see Registering and Licensing on page 31.

Upgrading From an Earlier Version of Dell SonicWALL GMS

The Dell SonicWALL GMS Virtual Appliance can be upgraded from 7.1 to 7.2, but cannot be directly upgraded from GMS versions earlier than 7.1. To upgrade the GMS Virtual Appliance from a version earlier than 7.1, you need to upgrade to major versions of GMS until you reach 7.1, then you can upgrade to GMS 7.2. For the GMS Virtual Appliance deployments, upgrading can be done on the **System > Settings** page.

In a distributed environment, stop all GMS services on all GMS servers before doing an upgrade. You must upgrade all GMS servers in your deployment to the same version of GMS. For example, you cannot have some servers running version 7.1 and others running 7.2.

To upgrade, complete the following steps:

Step 1   Download the respective file from the MySonicWALL.com Software Download Center to your workstation: **sw_gmsvp_vm_eng_7.2.xxxx.yyyy.gmsvp-updater.64bit.sh** (where "xxxx" represent the exact version numbers)

Step 2   Open the GMS Virtual Appliance console.

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

Step 4   Click **Browse**, navigate to the location where you saved the previous file, and then select it.

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

Chapter 3

Performing Basic Tasks and Host Configuration

This section describes how to power on and configure basic settings on the Dell SonicWALL GMS Virtual Appliance, including virtual hardware settings and networking settings.

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

1. Power the Virtual Appliance On on page 25
2. Configure Host Settings on the Console on page 26
3. Configure Host Settings on the Appliance Management Interface on page 27

This chapter also contains information on:

- Viewing the Settings Summary on page 29
- Editing The Virtual Machine Settings on page 30

Power the Virtual Appliance On

There are multiple ways to power the Dell SonicWALL 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

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

Step 1 In vSphere, right-click the GMS Virtual Appliance in the left pane and select **Open Console** in the right-click menu.
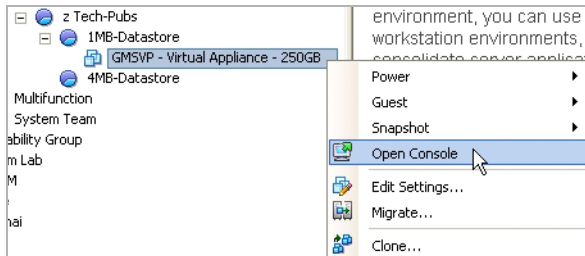
Step 2 When the console window opens, click inside the window, type *snwlcli* at the **login:** prompt and then press **Enter**. Your mouse pointer disappears when you click in the console window. To release it, press **Ctrl+Alt**.

Step 3 The console might display warning messages that can be ignored, and then displays a second **Login:** prompt. Type *admin* at the **Login:** prompt and press **Enter**, and then type *password* at the **Password:** prompt and press **Enter**. The "SNWLCLI>" prompt is displayed.
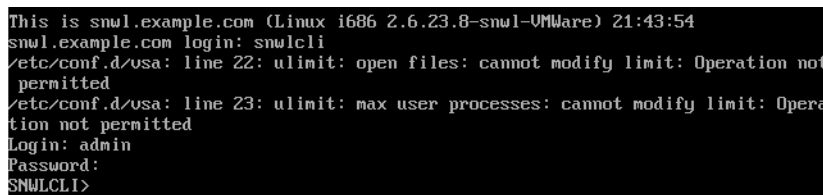
Step 4 Configure the local IP address for the virtual appliance by typing the following command, substituting your IP address and subnet mask for the values shown here:

```
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.

Step 5 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.

Step 6 Type *exit* to exit the CLI, and 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 change the admin password and configure host name, network, and time settings in the appliance management interface. The password is changed during the login process, and the Host Configuration Tool changes the other settings.

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

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

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

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

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

Step 1 Launch a browser and enter the URL of the virtual appliance, such as:

http://10.208.112.175

Step 2 On the appliance interface login page, type in the default credentials and then click **Submit** to log in.

The default credentials are:

User—*admin*

Password—*password*

Step 3 The first time you log in to the appliance, you must change the password. The login page re-displays with the default login credentials pre-populated. Enter a new password for the admin account in the **New Password** field, and enter it again in the **Confirm New Password** field. Click **Submit**.

Note The new password must be at least seven characters.

Be sure to save or write this password down in a secure location, as it is encrypted and is difficult to recover if you forget it.

Step 4   The Host Configuration Tool wizard starts automatically. In the Introduction screen, click **Next**.

Step 5   In the Network Settings screen, configure the following network settings for the GMS Virtual Appliance, and then click **Next**:

- **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

Step 6   In the Time Settings screen, select values for the following system settings on the virtual appliance, and then click **Next**:

- **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

Step 7   In the Summary screen, verify the settings. Click **Back** to make changes on a previous screen, or click **Apply** to accept the settings.

Step 8   A dialog box warns you that the virtual appliance is rebooting. Click **OK**.
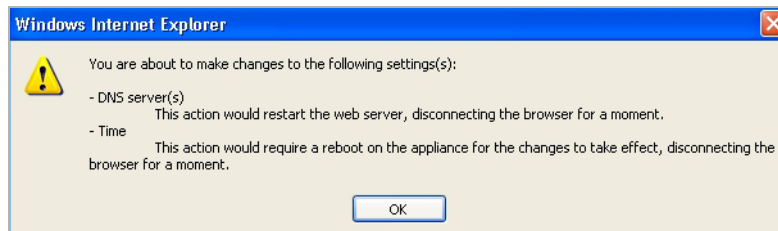
Step 9   Wait for the settings to be applied, possibly for a few minutes. The screen displays a progress bar until it finishes, and then displays the status.

Note If you modified the DNS settings, the services on the appliance restarts when the changes are applied, causing a momentary connectivity loss to the Web server. Your browser is redirected to the appliance management interface login page.

If you modified the Time settings, the virtual appliance will reboot. Use your browser to reconnect to the appliance management interface.

Viewing the Settings Summary

When the Dell SonicWALL 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 the Power On and Edit Settings.

When using vSphere with vCenter Server, the Migrate and Clone commands are also available.

Editing The Virtual Machine Settings

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

To edit virtual machine settings:

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

Step 2   In the Virtual Machine Properties window, the **Hardware** tab displays the settings for memory, CPU, hard disk, and other hardware. Click on the row in the table to access the editable settings in the right pane.
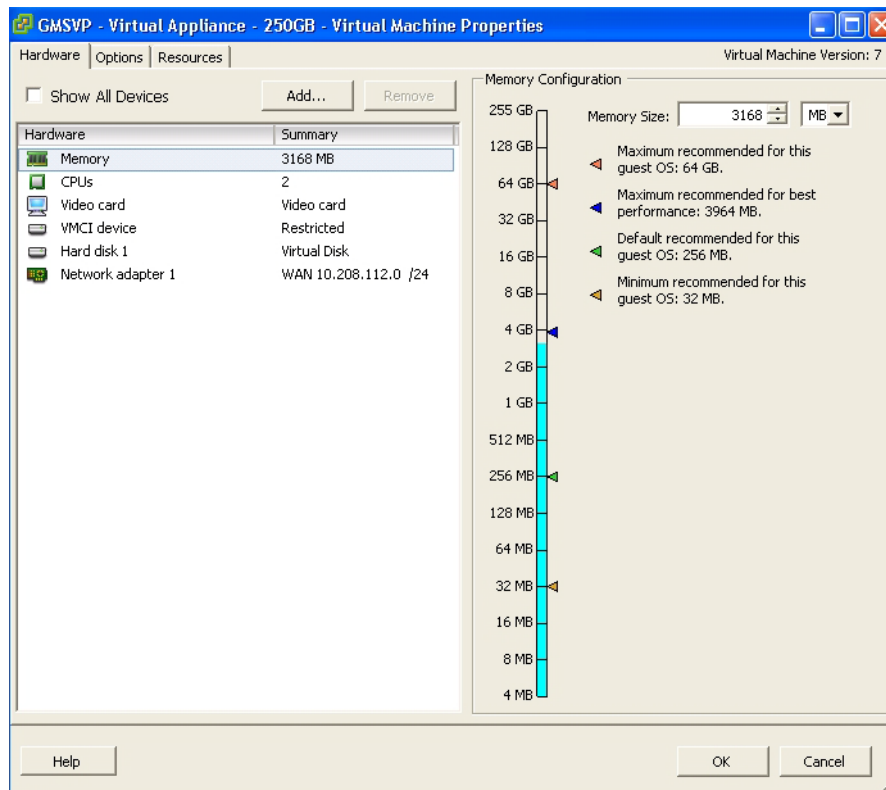
Step 3   Click the **Options** tab to view and edit the GMS Virtual Appliance name, location (datastore), guest power management (for standby), and other settings.

Step 4   Click the **Resources** tab to view and edit the resource allocation settings.

Step 5   When finished, click **OK**.

Chapter 4

Registering and Licensing

All instances of SonicWALL GMS must be registered and licensed before use. This requirement applies to both single server deployments or distributed deployments on multiple servers, to fresh or upgraded installations, and to Virtual Appliance installations on Windows servers or to SonicWALL UMA appliances.

This section contains the following subsections:

Registering / Licensing After a Fresh Install

Dell SonicWALL GMS registration is completed using the Universal Management Host (UMH) system interface. When installing the Universal Management Suite on a server, or host, a Web server is installed to provide the UMH system interface. The system interface is available by default after restarting the system at: *http://localhost/*

To complete registration, the system must have access to the Internet and you must have a MySonicWALL account. The Dell SonicWALL License Manager, available on the **System > Licenses** page of the UMH system interface, allows you to log in and enter your registration information on MySonicWALL.

Note MySonicWALL registration information is not sold or shared with any other company.

To register and license Dell SonicWALL GMS on this server, complete the following steps:

Step 1 Double-click the Universal Management Suite desktop icon or open a Web browser and enter *http://localhost/* to launch the UMH system interface.

Note If you specified a custom port (a port other than the default port 80), modify the URL as follows: http://localhost:*<port>*/.

For example, if you specified port 8080, the URL would be: http://localhost:8080/.

Step 2 The login page loads by default in English, type *admin* in the **User** field, and *password* in the **Password** field and then click **Submit**. GMS includes language support for English, Japanese, Simplified Chinese, Traditional Chinese. Click the language of your choice at the bottom of this page.

Step 3 The Login page reloads to force a password change. Type a new password into both the **New Password** and **Confirm New Password** fields, and then click **Submit**.

Step 4 If the software detects that the Windows Firewall is enabled on the system, a warning dialog box is displayed on top of the **System > Status** page. To receive syslog and SNMP packets, either disable the Windows Firewall or configure it to open these ports (default syslog port is UDP 514 and default SNMP port is UDP 162). When ready, click **OK**.

Step 5 Optionally, you can select **Perform this check after 30 days** if you do not plan to disable the Windows Firewall immediately, and do not wish to see this warning every time you login. The check for Windows Firewall cannot be disabled completely, and if you leave it running you will see this alert after the 30-day delay. You can repeat the delay as many times as needed.

Step 6 On the **System > Status** page, the **Registration Pending** notification across the top of the screen indicates that the system is not registered, the Serial Number status is **UNKNOWN**, and the License status displays **Not Licensed**. To begin registration, click **Register** in the top, right corner.

Step 7 On the License Management page, type your MySonicWALL user name and password into the appropriate fields and then click **Submit**.

Note If you do not have a MySonicWALL account, you must create one before continuing. Click the link to create a MySonicWALL account.

Step 8 On the second License Management page, type your 12-character software serial number into the **Serial Number** field and your authentication code into the **Authentication Code** field.

Note If this is the first Dell SonicWALL GMS Virtual Appliance that you are registering in a multi-server deployment, the Serial Number and Authentication Code you received from your Dell SonicWALL sales representative is entered here. As you add more instances of Dell SonicWALL GMS Virtual Appliance on Windows Server systems to the distributed deployment, use the same serial number used for the installation of the first GMS Windows Software or Dell SonicWALL UMA appliance. You can use the GMS Windows serial number to register associated servers if it is a full-retail GMS serial number, but not a Demo or Free Trial GMS serial number. See Registering Associated Servers in a Distributed Deployment on page 33.

Step 9 Type a friendly name for the system into the **Friendly Name** field. The friendly name is displayed on MySonicWALL to more easily identify the installation on this system.

Note If this is the first Dell SonicWALL GMS Virtual Appliance that you have registered in a multi-server deployment, the Friendly Name for this system is also used as the name for the distributed deployment. See Registering Associated Servers in a Distributed Deployment on page 33.

Step 10 Click **Submit**.

Step 11 The License Management page displays a completion screen. Click **Continue**. The license summary information displays.

Step 12 After registration, the next step is to select the role for this GMS server. Continue with the procedure described in Using the Role Configuration Tool on page 36.

Registering Associated Servers in a Distributed Deployment

When you have a distributed Dell SonicWALL GMS deployment involving more than one Dell SonicWALL UMA EM5000 appliance or Virtual Appliance instance of GMS, you can associate these components during the registration process. A MySonicWALL account is required. In a distributed deployment, Dell SonicWALL GMS must be registered and licensed on each server and associated with the initially registered instance of GMS. This is accomplished by entering the serial number of the primary instance of Dell SonicWALL GMS when registering each subsequent server in the distributed deployment.

When the primary instance of Dell SonicWALL GMS is a Dell SonicWALL UMA EM5000 appliance, you can download the UMS installer from MySonicWALL, so that you can install UMS on Windows systems to be used in the distributed deployment. When registering the Virtual Appliance instances of Dell SonicWALL GMS, use the serial number of the Dell SonicWALL UMA appliance.

Note The base 10-node or 25-node management license is not automatically increased when additional servers are associated with an existing Dell SonicWALL GMS deployment. You can purchase additional node licenses on MySonicWALL.

To register a Dell SonicWALL GMS instance as an associated server in an existing GMS deployment, complete the following steps:

Step 1   In a browser, log in to the system management interface and click **Register**.

Step 2   On the License Management page, enter the same MySonicWALL user name and password that you used when registering the primary instance of GMS into the appropriate fields and then click **Submit**.

Step 3   On the second License Management page, do one of the following:

- Type the 12 character serial number of the primary GMS into the **Serial Number** field and type the authentication code of the primary GMS into the **Authentication Code** field. The primary GMS must already be registered.
- If adding a UMA EM5000 appliance as a secondary member of a distributed deployment, the License Manager automatically populates the **Serial Number** field. You have the opportunity to add this unit to the existing deployment in a later step.
- If you have an eight character serial number because you upgraded this distributed deployment from a previous version of GMS, click the **Click here if you have an 8 character Serial Number** link and enter the eight character serial number of the primary GMS.

Step 4   Type a descriptive name for the system into the **Friendly Name** field. Click **Submit.**

Step 5   In the License Management completion screen, click **Continue**.

Step 6   After registration, the next step is to select the role for this GMS server. Continue with the procedure described in Configuring UMH Deployment Options on page 35.

Chapter 5

Configuring UMH Deployment Options

The role that you assign to your Dell SonicWALL GMS defines the Universal Management Suite services that it provides. The Dell SonicWALL GMS uses these services to do management, monitoring, and reporting tasks.

Your Dell SonicWALL GMS can be deployed in any of the following roles:

- All in One
- Database Only
- Console
- Agent
- Monitor
- Syslog Collector
- Flow Server
- All in One - Flow Server (Demo Mode Only)

Deployment Considerations

- In the UMH system interface, clicking **Details** in the same row as a role provides a list of the services that run on a system in that role, and information about using the role.
- As the number of managed appliances increases, a more distributed deployment provides better performance. To manage large numbers of Dell SonicWALL appliances, you can use several Dell SonicWALL GMS instances operating in different roles in a distributed deployment. These instances can run on Windows Server machines or on Dell SonicWALL UMA appliances.
- You can include the MySQL database installation with any role. The All In One or Database Only roles automatically include the MySQL database. Only one server in a Dell SonicWALL GMS deployment should have the MySQL database included in its role.
- You can scale your deployment to handle more units and more reporting by adding more systems in the Agent role. Agents provide built-in redundancy capability, meaning that if an Agent goes down, other Agents can do the configuration tasks and other tasks of the Agent that went down.
- When configuring the role for the first appliance in a distributed deployment, you should either include the database or be prepared to provide the IP address of an existing database server.

  You can meet this database objective in one of the following ways:

  – By selecting a role that includes the database automatically, such as All In One or Database Only

  – By selecting **Include Database (MYSQL)** if configuring the system with any other role

  – By setting up a compatible database on another machine and providing that IP address when prompted

Using the Role Configuration Tool

The Role Configuration Tool is a wizard that guides you through the process of defining the deployment role for Dell SonicWALL GMS. Your system must be registered and licensed for Dell SonicWALL GMS to run the Role Configuration Tool.

There are two ways to access the Role Configuration Tool:

- After the appliance is registered and licensed for GMS, the **System** > **Status** page of the appliance management interface provides a link to the wizard.
- The **Wizards** button in the top right corner of the page provides access to the Role Configuration Tool.

To use the Role Configuration Tool, complete the following steps:

Step 1   Log in to the appliance management interface and navigate to the **System > Status** page.

Step 2   Click the **Click here** link at the top of the page.

Step 3   In the Introduction page of the Role Configuration Tool, click **Next**.

Step 4   In the Setup Type page, select **Yes** if you are adding this system to an existing GMS deployment. Selecting Yes indicates to the wizard that there is an existing GMS database on another server. Select **No** if this system is part of a new GMS deployment or is the only system in your GMS deployment. Click **Next**.

If you selected Yes, skip step 5 and proceed to step 6.

Step 5   In the Deployment Type page, select **Yes** if this system is the only GMS server in the deployment, or select **No** if there are multiple GMS servers. Click **Next**.

Step 6   In the Role Configuration page, select the desired role for this system and select **Include Database (MYSQL)** if you want to configure a GMS database on this system. Click **Next**.

Step 7   The list of roles on this page varies depending on your previous selections such as whether this system is part of an existing GMS deployment and if it is a single-server or part of a multi-server deployment. Neither the Database Only nor the Include Database (MYSQL) options are available if this system is part of an existing deployment.

Step 8   In the Database Configuration page, enter the database parameters that are required for the selected role. The database fields varies depending on your previous selections.

Step 9   Certain fields are prepopulated if you made a choice of role that automatically includes the MySQL database or if you chose **Include Database (MYSQL)**.

Step 10 For a MySQL instance, additional fields are available for configuring the database administrator credentials. The **Administrator Credentials** fields are only displayed and editable in the following circumstances:

- The **Database Type** is **MySQL**
- **Include Database (MYSQL)** is selected either manually or automatically for the chosen role
- The **Database Host** field is set to **localhost** and is not editable

When these conditions are met, the administrator password is required to create a regular access user account for the GMS application.

If you selected a role that does not include the MySQL database, you have the option of configuring the use of a SQL Server database in this screen.

Note the following when selecting values for these fields:

- **Database User** – Do not use any special characters, and do not use 'sa', 'root', or 'admin'.
- **Database Password** – Do not use any special characters.
- **Admin Login** – If using MySQL, the default Admin Login is 'root'. This cannot be changed.
- **Admin Password** – Do not use any special characters.

Step 11 When finished entering the database parameters, click **Next**.

Step 12 In the Other Configuration page, the fields vary depending on the selected role, as follows:

- **Gateway Parameters** – Required for All in One, Console, and Agent roles
- **Syslog Server Parameters** - Required for All in One, Console, Agent, and Syslog Collector roles
- **SMTP Parameters** - Required for All in One and Console roles

Step 13 Enter the **GMS Gateway IP** address and connection password, if you are using a GMS gateway. Leave these fields empty if you are using HTTP/HTTPS to connect to the managed appliances.

Step 14 In the **Syslog Server Port** field, type in the port used for receiving syslog messages or accept the default of 514.

Step 15 For access to email on this system, including the ability to send email alerts, type the mail server IP address into the **SMTP Server** field and enter valid email addresses for the **Sender Address** and **Administrator Address**. Click **Next**.

Step 16 In the Summary page, verify that all parameters are correct. Click **Back** to make changes on a previous screen, or click **Apply** to accept the settings.

Step 17 Wait for the settings to be applied. The screen displays a progress bar until it finishes, and then displays the status. This phase can take up to 10 minutes, especially if the database was included in the deployment.

Step 18 Click **Close** to exit the Role Configuration Tool.

Manually Configuring the System Role

You can configure the role of the Dell SonicWALL GMS system without using the Role Configuration Tool. All role configuration is completed in the UMH system interface, available at the URL: http://<I*P address*>:<*port*>/appliance/

Note Dell SonicWALL recommends that you use a multi-system distributed deployment in production environments, with the database on a dedicated server and the other services on one or more systems. When only one other system is deployed, the Console role should be assigned to it.

Refer to the following sections for instructions on manually configuring the system role:

Configuring the All In One Role

The All In One role is used for demonstrating functionality in test environments, it should not be used in production environments.
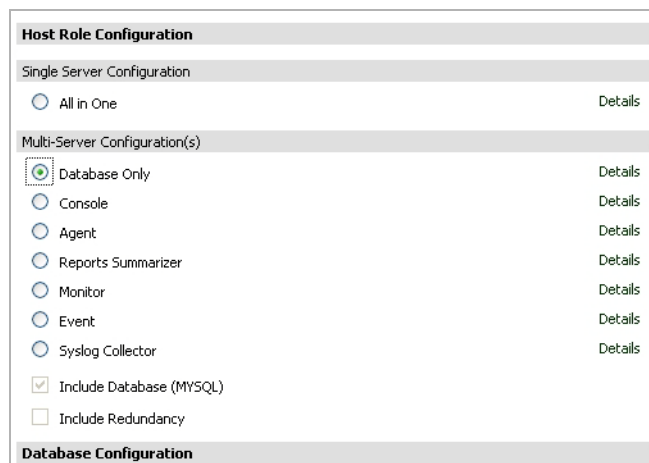
The All In One role provides all services utilized by Dell SonicWALL GMS:

- Syslog Collector
- Reports Scheduler
- Update Manager
- Reports Summarizer
- SNMP Manager
- Scheduler
- Monitoring Manager
- Web Server
- Database
- Flow Server

To Configure the Gateway settings for this role, refer to Configuring the Gateway on page 45.

Configuring the Database Only Role

The Database Only role is used in a multi-server Dell SonicWALL GMS deployment. In this role, the server is configured to run only the database service. Dell SonicWALL recommends that one of the servers in a multi-server GMS deployment is assigned a Database Only role.

Only the Universal Management Suite Database service runs on a Database Only system.

The MySQL database engine is pre-installed along with the Dell SonicWALL GMS installation. Dell SonicWALL GMS can also use a MySQL database or a Microsoft SQL Server database installed on a server. Only the MySQL database included in the installer is supported. On the **Deployment > Role** page in the Dell SonicWALL GMS Virtual Appliance appliance management interface, you can configure your Dell SonicWALL GMS systems to use either a MySQL or a SQL Server database.

To deploy your Dell SonicWALL GMS Virtual Appliance in the Database Only role, complete the steps described in the Configuring Database Settings on page 47.

Configuring the Console Role

The Console role is used in a multi-server, distributed Dell SonicWALL GMS deployment. In this role, the Dell SonicWALL GMS installation runs all Universal Management Suite services except for the Database service. In this scenario, the Database role is assigned to a separate appliance or server.

In the Console role, the Dell SonicWALL GMS Virtual Appliance behaves as an Agent, and also provides the following functions:

* Provides Web user interface for the Dell SonicWALL GMS application
* Emails Scheduled Reports
* Performs Event Management tasks
* Performs various periodic checks, such as checking for new appliances that can be managed, checking for new firmware versions of managed appliances, and similar functions

To Configure the Gateway settings for this role, refer to Configuring the Gateway on page 45.

Configuring the Agent Role

The Agent role can be used in a distributed deployment of Dell SonicWALL GMS. The primary functions of this role include the following:

- Manages units by acquiring them, pushing configuration tasks to the units and tracking their up/down status
- Performs monitoring based on ICMP probes, TCP probes, and SNMP OID retrievals
- Collects and stores syslog messages
- Performs report summarization

The following Universal Management Suite services run on an Agent system:

- Syslog Collector
- Reports Summarizer
- SNMP Manager
- Scheduler
- Monitoring Manager

To Configure the Gateway settings for this role, refer to Configuring the Gateway on page 45.

Configuring the Reports Summarizer Role

The Reports Summarizer role is used to dedicate a server for doing only summarization of reports in a multi-server Dell SonicWALL GMS deployment. Syslogs collected by the Syslog Collector service are consumed by the Reports Summarizer service to create generate reports. In such a deployment, it is essential that the Syslog Collectors running on various GMS Servers write syslogs to folders that are accessible by Reports Summarizer systems.

The following services run on a Summarizer system:

- Dell SonicWALL Universal Management Suite - Reports Summarizer
- Dell SonicWALL Universal Management Suite - Web Service Server

To deploy your Dell SonicWALL GMS Virtual Appliance in the Reports Summarizer role, complete the following steps in the appliance management interface:

Step 1   Navigate to the **Deployment > Role** page. Under **Host Role Configuration**, select **Reports Summarizer**.

Multi-Server Configuration(s)	
○ Database Only	Details
○ Console	Details
○ Agent	Details
⦿ Reports Summarizer	Details

Step 2   To include the MySQL database on this system, select **Include Database (MYSQL)**. To use a MySQL or Microsoft SQL Server database on another system, do not select this checkbox.

Step 3   Configure the database settings as described in the Configuring Database Settings on page 47.

Step 4   Configure the Web port settings as described in the *Configuring Web Port Settings* section, on page 48.

Step 5   To apply your changes, click **Update**.
To change the settings on this page back to the defaults, click **Reset**.

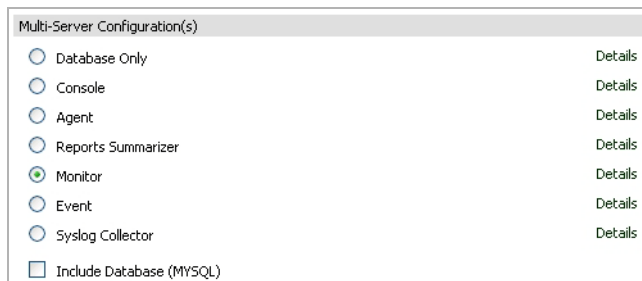# Configuring the Monitor Role

The Monitor role is used to dedicate the Dell SonicWALL GMS installation to monitoring appliances and applications in a multi-server GMS deployment. The monitoring is based on ICMP probes, TCP probes, and SNMP OID retrievals.

Only the Universal Management Suite Monitoring Manager service runs on a Monitor system.

To deploy your Dell SonicWALL GMS Virtual Appliance in the Monitor role, complete the following steps in the appliance management interface:

Step 1   Navigate to the **Deployment > Role** page. Under **Host Role Configuration**, select **Monitor**.

Step 2   To include the MySQL database on this system, select **Include Database (MYSQL)**. To use a MySQL or Microsoft SQL Server database on another system, do not select this checkbox.

Step 3   Configure the database settings as described in the Configuring Database Settings on page 47.

Step 4   Configure the Web port settings as described in the Configuring Web Port Settings on page 48.

Step 5   To apply your changes, click **Update**.
To change the settings on this page back to the defaults, click **Reset**.

Configuring the Event Role

The Event, or Event Management, role of a GMS Server is used to dedicate a server for doing only event-based alerting of appliances and applications in a multi-server Dell SonicWALL GMS Virtual Appliance deployment.

The following services run on an Event Management system:

- Dell SonicWALL Universal Management Suite - Event Manager
- Dell SonicWALL Universal Management Suite - Web Service Server

To deploy your Dell SonicWALL GMS Virtual Appliance in the Event role, complete the following steps in the appliance management interface:

Step 1   Navigate to the **Deployment > Role** page. Under **Host Role Configuration**, select **Event**.

Step 2   To include the MySQL database on this system, select **Include Database (MYSQL)**. To use a MySQL or Microsoft SQL Server database on another system, do not select this checkbox.

Step 3   Configure the database settings as described in the Configuring Database Settings on page 47.

Step 4   Configure the Web port settings as described in the Configuring Web Port Settings on page 48.

Step 5   To apply your changes, click **Update**.
To change the settings on this page back to the defaults, click **Reset**.

Configuring the Syslog Collector Role

The Syslog Collector role can be assigned to a Dell SonicWALL GMS server in a multi-server deployment of GMS. In this role, the Dell SonicWALL GMS server is dedicated to collecting syslog messages on the configured port (by default, port 514). The syslog messages are stored in the Dell SonicWALL GMS server file system.

The syslog messages are used by the Reports Summarizer service running on another Dell SonicWALL GMS server or Dell SonicWALL UMA EM5000 in the distributed deployment. The folder where the Syslog Collector server stores the syslog messages must be accessible by the server running the Reports Summarizer service.

Only the Universal Management Suite Syslog Collector service runs on a Syslog Collector system.

To deploy your Dell SonicWALL GMS Virtual Appliance server in the Syslog Collector role, complete the following steps in the UMH system interface:

Step 1   Navigate to the **Deployment > Role** page. Under **Host Role Configuration**, select **Syslog Collector**.

Step 2   If this Dell SonicWALL GMS server listens for syslog messages on a non-standard port, type the port number into the **Syslog Server Port** field. The default port is 514.

Step 3   To include the MySQL database on this system, select **Include Database (MYSQL)**. To use a MySQL or Microsoft SQL Server database on another system, do not select this checkbox.

Step 4   Configure the database settings as described in the Configuring Database Settings on page 47.

Step 5   Configure the Web port settings as described in the Configuring Web Port Settings on page 48.

Step 6   To apply your changes, click **Update**.
To change the settings on this page back to the defaults, click **Reset**.

Configuring the Flow Server Role

The Flow Server role can be used in a distributed deployment of Dell SonicWALL GMS. The primary functions of this role include the following:

• Collect and stores flows from the firewalls
• Performs report summarization

The following Universal Management Suite services run on an Agent system:

• Dell SonicWALL Universal Management Suite - Flow Server

The single service that runs in this role is Dell SonicWALL Universal Management Suite - Flow Server. The flows are collected and stored in internal databases. To be able to create reports out of these flows, you need to have a GMS server in this deployment with a minimum version of 7.1 and a role of "Console" or "All in One," and so on. You also need to make sure that the following ports are open:

- UDP 2055
- UDP 5055
- TCP 9063
- TCP 9064
- TCP 9065
- TCP 9066
- TCP 9067

To deploy your Dell SonicWALL GMS Virtual Appliance in the Flow Server role, complete the following steps in the appliance management interface:

Step 1 Navigate to the **Deployment > Role** page. Under **Host Role Configuration**, select **Flow Server**.

Step 2 Configure the database settings as described in the Configuring Database Settings on page 47.

Step 3 Configure the Web port settings as described in the Configuring Web Port Settings on page 48.

Step 4 To apply your changes, click **Update**.
To change the settings on this page back to the defaults, click **Reset**.

Configuring the All in One-Flow Server (Demo Mode Only).

The All In One-Flow Server role is used for demonstrating Flow Server functionality in test environments, it should not be used in production environments. This role configuration is available for the GMS Virtual Appliance only.

Following services run on an All in One-Flow Server Management system:

- Dell SonicWALL Universal Management Suite - Database
- Dell SonicWALL Universal Management Suite - Event Manager
- Dell SonicWALL Universal Management Suite - Flow Server
- Dell SonicWALL Universal Management Suite - Monitoring Manager
- Dell SonicWALL Universal Management Suite - Reports Database
- Dell SonicWALL Universal Management Suite - Reports Scheduler
- Dell SonicWALL Universal Management Suite - Reports Summarizer
- Dell SonicWALL Universal Management Suite - Scheduler
- Dell SonicWALL Universal Management Suite - Syslog Collector
- Dell SonicWALL Universal Management Suite - Update Manager
- Dell SonicWALL Universal Management Suite - Web Server
- Dell SonicWALL Universal Management Suite - Web Services

To Configure the Gateway settings for this role, refer to Configuring the Gateway on page 45.

Configuring the Gateway

After choosing a role, select a gateway to configure:

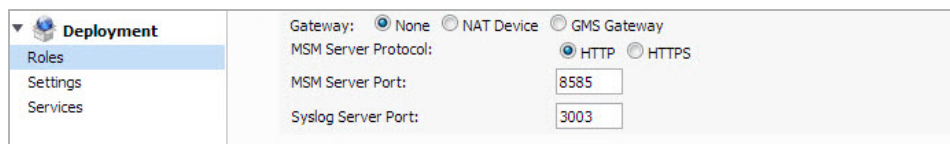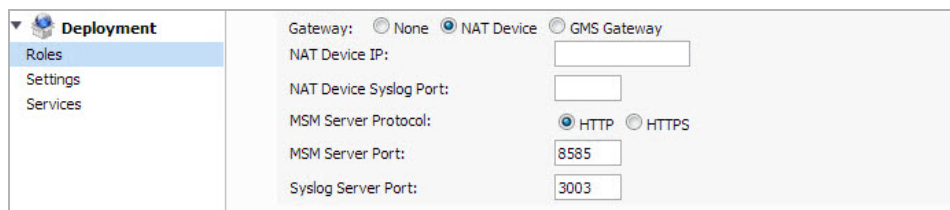- None on page 45
- NAT Device on page 45
- GMS Gateway on page 46

None

No gateway is specified.

If you do not wish to configure a gateway, complete the following steps:

Step 1   Click **None**.

Step 2   Select **HTTP** or **HTTPS** for the MSM Server Protocol.

Step 3   Click the **MSM Server Port** text-field, then enter the MSM Server port number.
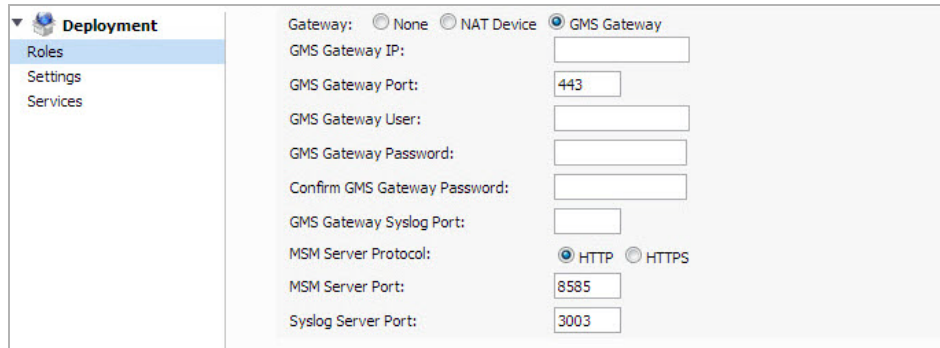
Step 4   Click the **Syslog Server Port** text-field, then enter the Syslog Server port number.

Step 5   To apply your changes, click **Update**. To change the settings on this page back to the defaults, click **Reset**.

NAT Device

Use this option when a NAT device is configured as the gateway. The GMS appliance does not have to log in to the unit for any reason and all NAT configurations are taken care of by the network Administrator directly through the device's management interface.

To configure the NAT device, complete the following steps:

Step 1   Select **NAT Device**.

Step 2   Click the **NAT Device IP** text-field, then enter the NAT Device IP address.

Step 3   Click the **NAT Device Syslog Port** text-field, then enter the NAT Device Syslog port number. This is the Syslog port used for Syslogs sent from the managed units.

Step 4   Select **HTTP** or **HTTPS** for the MSM Server Protocol.

Step 5   Click the **MSM Server Port** text-field, then enter the MSM Server port number.

Step 6   Click the **Syslog Server Port** text-field, then enter the Syslog Server port number.

Step 7   To apply your changes, click **Update**. To change the settings on this page back to the defaults, click **Reset**.

GMS Gateway

Use this option when a Dell SonicWALL device is acting as a Gateway. Using a Dell SonicWALL appliance is recommended, but can be setup as a NAT Device if all units are managed using an SSL tunnel. To configure the GMS Gateway, complete the following steps:

Step 1   Click **GMS Gateway**.

Step 2   If the Dell SonicWALL GMS connects to managed appliances through a GMS gateway, click the **GMS Gateway IP** text-field, then enter the internal IP address of the device.
If you change the GMS gateway IP address or password, you must also change the settings on this page. To determine if a GMS Gateway is required, see the *Dell SonicWALL Getting Started Guide* for your product

Step 3   Click the **GMS Gateway Port** text-field, then enter the management port used to sign into the device.

Step 4   Click the **GMS Gateway User** text-field, then enter the username used to sign into the device.

Step 5   Click the **GMS Gateway Password** text-field, then enter the password used to sign into the device.

Step 6   Confirm the GMS Gateway Password you entered.

Step 7   Click the **GMS Gateway Syslog Port** text-field, then enter the Syslog port used for syslogs sent from the managed units.

Step 8   Select **HTTP** or **HTTPS** for the MSM Server Protocol.

Step 9   Click the **MSM Server Port** text-field, then enter the MSM Server port number.

Step 10   Click the **Syslog Server Port** text-field, then enter the Syslog Server port number.

Step 11   To apply your changes, click **Update**. To change the settings on this page back to the defaults, click **Reset**.

Configuring Database Settings

Database settings configuration is largely the same for any role when you choose to include the database on that server. For roles that automatically include the default MySQL database, such as All In One or Database Only, the Database Type, Database Host, and Database Port fields are not editable. This is also the case for any role when **Include Database (MYSQL)** is selected. The Administrator Credentials fields are displayed only if the role has been defined to include the installation of the MySQL database. These are not available when a SQL Server database is selected.

This section describes the options for configuring the database settings for either the MySQL database or the Microsoft SQL Server database. Dell SonicWALL GMS can use either a MySQL or a SQL Server database.

> **Note** If this appliance connects to a SQL Server system with a non-default instance name, then the entries are different than described in this section. Refer to the *Dell SonicWALL GMS Administrator's Guide* for configuration instructions.

To configure the database settings for any role, complete the following steps in the UMH system interface:

Step 1 Navigate to the **Deployment > Role** page and select the role for this server.

Step 2 To run the MySQL database on this GMS server, select **Include Database (MYSQL)**. To use a MySQL or Microsoft SQL Server database on another system, do not select this checkbox.

Step 3 Under **Database Configuration**, if **Include Database (MYSQL)** was not selected in the previous step, select either **MYSQL** or **SQL Server** from the **Database Type** drop-down list. This field is not editable if you previously selected **Include Database (MYSQL)** or if the selected role is All In One or Database Only.

Step 4 In the **Database Host** field, type in the IP address of the database server or accept the default, **localhost**, if this Dell SonicWALL GMS Virtual Appliance server includes the database. This field is not editable if you previously selected **Include Database (MYSQL)** or if the selected role is All In One or Database Only.

Step 5 To use a different user name when GMS accesses the database, type the user name into the **Database User** field. The default user name is "sa".

Step 6 Type the password that GMS uses to access the database into both the **Database Password** and **Confirm Database Password** fields.

Step 7 Under **Administrator Credentials**, type the password for the administrator (root) account into both the **Admin Password** and **Confirm Admin Password** fields.

Step 8 Note that the **Administrator Credentials** fields are only displayed and editable in the following circumstances:

- The **Database Type** is **MySQL**
- **Include Database (MYSQL)** is selected either manually or automatically for the chosen role
- The **Database Host** field is set to **localhost** and is not editable

When these conditions are met, the administrator password is required to create a regular access user account for the GMS application.

Step 9 To apply your changes, click **Update**.
To change the settings on this page back to the defaults, click **Reset**.

Note It could take 10 or 15 minutes for a database installation to complete. The database installation creates a minimal GMS database. To change database sizes, you might need to use database tools such as MySQL Server Enterprise Manager.

Tip For optimal performance, you need to configure database maintenance plans. For information on configuring Dell SonicWALL GMS maintenance plans, refer to the *Dell SonicWALL GMS Administrator's Guide.*

Configuring Deployment Settings

The following sections describes the settings available on the **Deployment > Settings** page of the system interface:

- Configuring Web Port Settings on page 48
- Configuring SMTP Settings on page 49
- Configuring SSL Certificate Access on page 50

Configuring Web Port Settings

Web port settings configuration is largely the same on any role. To change the Web port settings, complete the following steps:

Step 1 On the **Deployment > Settings** page under **Web Port Configuration**, to use a different port for HTTP access to the Dell SonicWALL GMS Virtual Appliance server, type the port number into the **HTTP Port** field. The default port is 80.

Web Server Settings

HTTP port:	85
HTTPS port:	8445
Enable HTTPS redirection:	☐
Public IP:	10.203.23.74

Update   Reset

Step 2 To use a different port for HTTPS access to the Dell SonicWALL GMS Virtual Appliance server, type the port number into the **HTTPS Port** field. The default port is 443.

Step 3 To enable HTTPS redirection, click **Enable HTTPS redirection**.

Step 4 Click **Enable HTTPS Redirection** to redirect HTTP to HTTPS when accessing the GMS management interface.

Step 5 In the **Public IP** text-field, enter the public IP or FQDN of the outside web services.

Step 6 Click **Update** to apply the Web port settings.

Note Changing the Web port settings causes the system to restart.

Step 7   After the appliance restarts, use the new port to access the appliance management interface. For example:

- If you changed the HTTP port to 8080, use the URL:
  http://<*IP Address*>:8080/appliance/
- If you changed the HTTPS port to 4430, use the URL:
  http://<*IP Address*>:4430/appliance/

Configuring SMTP Settings

The SMTP settings are used for sending email alerts to the Dell SonicWALL UMH system administrator.

If the Mail Server settings are not configured correctly, you will not receive important email notifications, such as:

- System alerts for your Dell SonicWALL GMS deployment performance
- Availability of product updates, hot fixes, or patches
- Availability of firmware upgrades for managed appliances
- Alerts on your managed appliances' status
- Scheduled Reports

To configure the SMTP settings, complete the following steps:

Step 1   On the **Deployment > Settings** page under **SMTP Configuration**, enter the IP address of the SMTP server into the **SMTP server** field.

Step 2   If the SMTP server in your deployment is set to use authentication, click **Use Authentication**. This option is necessary for all outgoing GMS emails to properly send to the intended recipients. Enter the username in the **User** field, and enter/confirm the password in the **Password** and **Confirm Password** fields. This is the username/password that is used to authenticate against the SMTP server.

Step 3   In the **Sender address** field, enter the email address that appears as the 'From' address when email alerts are sent to the administrator.

Step 4   In the **Administrator address** field, enter a valid email address for the administrator who receives email alerts.
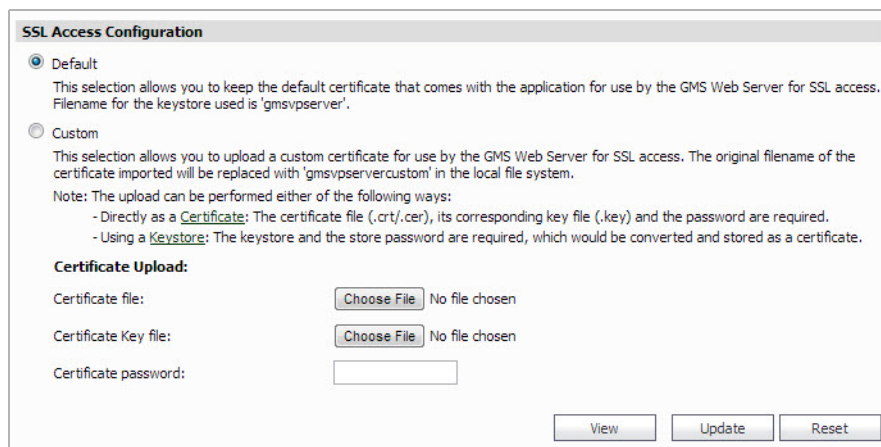
Step 5   In the **Email send timeout** field, enter a timeout interval (in minutes). If the server does not respond within the specified interval, the Email send action is stopped and an error is reported.

Step 6   Click **Test Connectivity** to verify your SMTP server configuration settings.

Step 7   Click **Update** to apply the SMTP settings.

Configuring SSL Certificate Access

Most Dell SonicWALL GMS Virtual Appliance deployments use the default certificate accompanied with your GMS Web Server. You can also choose to use a custom certificate and a respective unique password for your Dell SonicWALL GMS Virtual Appliance deployment as shown in the following image. The SSL Access Configuration section allows you to configure and upload a custom Keystore/Certificate file for SSL access to the GMS appliance, or select the default local keystore

To configure SSL access:

Step 1   Navigate to the **Deployment > Settings** page under **SSL Access Configuration** section.

Step 2   Select **Default** to keep, or revert to, the default settings, where the default GMS Web Server certificate with 'gmsvpserverks' keystore is used.

Step 3   Select **Custom** to upload a custom certificate for GMS SSL access.

Step 4   In the **Certificate file** field, click **Choose File** to select your certificate file.

Step 5   In the **Certificate Key file** field, click **Choose File** to select your certificate key file.

Step 6   Type the password for the certificate into the **Certificate password** field.

Step 7   Click **View** to display details about your certificate.

Step 8   Click **Update** to submit your changes.

Controlling Deployment Services

The **Deployment > Services** page provides a list of the services that are running on your system as part of Dell SonicWALL GMS Virtual Appliance. It also provides a way to stop or start any of the services.

Host Role	
Host Role: All in One	Details

Host Services	
☐ **Service Name**	**Current State**
☐ SonicWALL Universal Management Suite - Update Manager	Started (Enabled)
☐ SonicWALL Universal Management Suite - Syslog Collector	Started (Enabled)
☐ SonicWALL Universal Management Suite - Web Server	Started (Enabled)
☐ SonicWALL Universal Management Suite - Monitoring Manager	Started (Enabled)
☐ SonicWALL Universal Management Suite - Scheduler	Started (Enabled)
☐ SonicWALL Universal Management Suite - Event Manager	Started (Enabled)
☐ SonicWALL Universal Management Suite - Reports Scheduler	Started (Enabled)
☐ SonicWALL Universal Management Suite - Reports Summarizer	Started (Enabled)
☐ SonicWALL Universal Management Suite - Database	Started (Enabled)

[Disable/Stop] [Enable/Start] [Restart]

To stop a service that is currently Enabled, select the checkbox for that service and then click **Disable/Stop**.

To start a service that is currently Disabled, select the checkbox for that service and then click **Enable/Start**.

To restart a service that is either Enabled or Disabled, select the checkbox for that service and then click **Restart**.

Chapter 6

Provisioning and Adding Units

After installation, registration, and role configuration, the next steps in setting up your Dell SonicWALL GMS Virtual Appliance are provisioning Dell SonicWALL appliances to support GMS and adding them to the Dell SonicWALL GMS Virtual Appliance. All Dell SonicWALL appliances must be provisioned before adding them to the Dell SonicWALL GMS Virtual Appliance. Make sure the provisioned Dell SonicWALL appliances have a valid GMS license— one GMS license for each Dell SonicWALL appliance.

This chapter contains the following sections:

Provisioning a Dell SonicWALL Firewall Appliance

To provision a Dell SonicWALL firewall appliance to support GMS, complete the following steps:

Step 1   Log in to the firewall appliance. Navigate to the **Log > Syslog** page.

Step 2   In Syslog Servers, click **Add**.

Step 3   Enter the GMS IP address to start sending syslogs. The GMS service should be activated. Set the log in UTC format and log category.
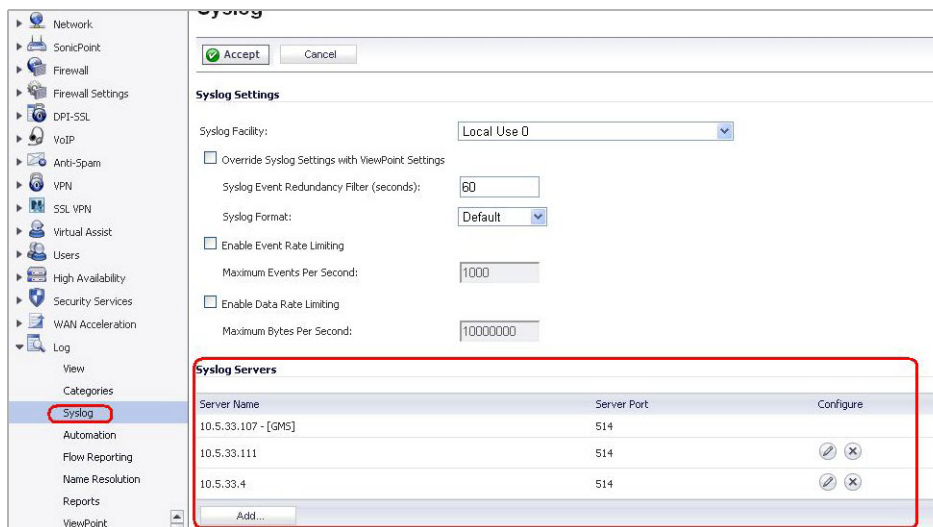
Step 4   Navigate to the **System > Time** page, and enable **Display UTC in logs (instead of local time)**.
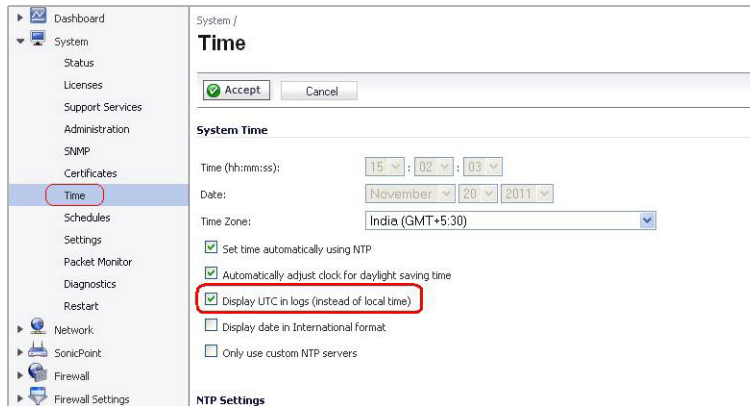
Provisioning a Dell SonicWALL SRA SMB Appliance

To provision a Dell SonicWALL SRA SMB appliance for Dell SonicWALL GMS Virtual Appliance complete the following steps:
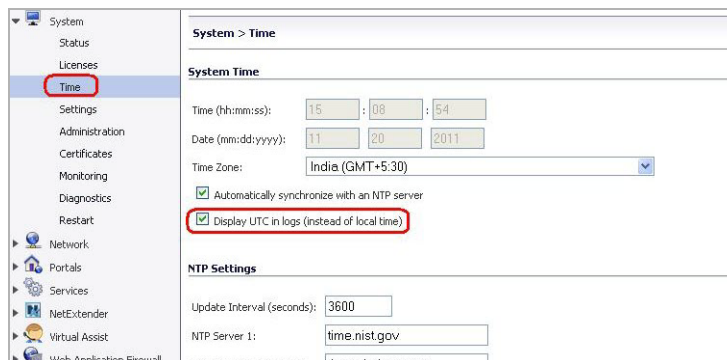
Step 1   Log in to the SRA SMB appliance. Navigate to the **Log > Analyzer** page.

Step 2   In Analyzer Settings, click **Enable Analyzer**.

Step 3   Click **Add** to add the GMS IP address, this starts sending syslogs.

Step 4   Navigate to the **System > Time** page, and enable **Display UTC in logs (instead of local time)**.

Provisioning a Dell SonicWALL E-Class SRA Series Appliance

Currently there is no GMS settings implementation in Dell SonicWALL E-Class SRA series appliances. To add GMS reporting support, use the **Additional ViewPoint** settings in the **General Settings > Configure Centralized Management** screen, and enter the GMS IP address and port number to start sending syslog.

Provisioning a Dell SonicWALL CDP Appliance

Currently there is no GMS settings implementation in Dell SonicWALL CDP appliances. To add GMS reporting support, use the **GMS** settings in the **Settings > SMB** screen. In Active Report, select **Enable**, and enter the GMS IP address and port number to start sending CDP syslog.
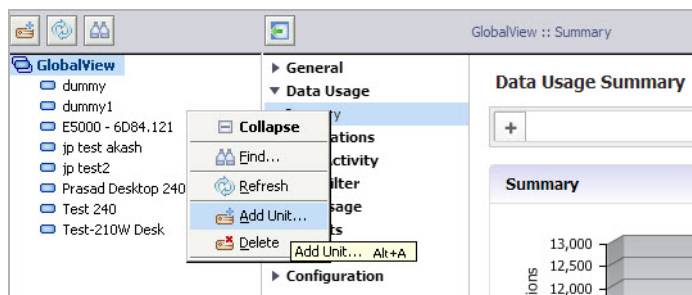
Adding Dell SonicWALL Appliances

This section describes how to add Dell SonicWALL appliances to the GMS. Dell SonicWALL GMS Virtual Appliance checks with the Dell SonicWALL licensing server when you add an appliance, so it is important that Dell SonicWALL GMS Virtual Appliance has Internet access to the server. Dell SonicWALL GMS Virtual Appliance can communicate with Dell SonicWALL appliances through HTTP or HTTPS.

To add a Dell SonicWALL appliance using the Dell SonicWALL GMS Virtual Appliance management interface, complete the following steps:

Step 1   Click the appliance tab that corresponds to the type of appliance that you want to add:

- **Firewall**
- **SRA**
- **CDP**

Step 2   Expand the Dell SonicWALL GMS Virtual Appliance tree and select the group to which you are adding the Dell SonicWALL appliance. Then, right-click the group and select **Add Unit** from the pop-up menu. To not specify a group, right-click an open area in the left pane (TreeControl pane) of the Dell SonicWALL GMS Virtual Appliance management interface and select **Add Unit** or click the **Add Unit i**con in the tool bar.

The Add Unit dialog box appears:

Step 3 Enter a descriptive name for the Dell SonicWALL appliance in the **Unit Name** field. Do not enter the single quote character (') in the Unit Name field.

Step 4 Enter the serial number of the Dell SonicWALL appliance in the **Serial Number** field.

Step 5 For the **Managed Address**, choose whether to **Determine automatically**, or S**pecify manually**. Most deployments are able to determine the IP address automatically. If you choose to specify the IP address manually, an option to **Make manual address sticky** is available. This retains the Manual Mode and the specified IP address is not overwritten.

Step 6 Enter the Administrator login name for the Dell SonicWALL appliance in the **Login Name** field. The Administrator of the appliance can also enter a Local User or a Remote User name (as configured on the Firewall) for GMS Management. If using Local User or Remote User names, they must be included in the user list created on the Firewall.

Step 7 Enter the password used to access the Dell SonicWALL appliance in the **Password** field.

Step 8 For **Management Mode**, select from the following:

- If the Dell SonicWALL appliance is managed through an existing VPN tunnel or over a private network, select **Using Existing Tunnel or LAN**.
- If the Dell SonicWALL appliance is managed through a dedicated management VPN tunnel, select **Using Management Tunnel**.
- If the Dell SonicWALL appliance is managed using SSL, select **Using SSL (default)**.

Step 9 Enter the IP address of the managed appliance in the **Management Port** field (default port is HTTPS: 443). The Dell SonicWALL appliance is connected with HTTPS by default.

Step 10 For VPN tunnel management, enter a 16-character encryption key in the **SA Encryption Key** field. The key must be exactly 16 characters long and composed of hexadecimal characters. Valid hexadecimal characters are "0" to "9", and "a" to "f" (such as, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). For example, a valid key would be: *1234567890abcdef*

Note This key must match the encryption key of the SonicWALL appliance. You can set the key on the appliance by logging directly into it.

Step 11 For VPN tunnel management, enter a 32-character authentication key in the **SA Authentication Key** field. The key must be exactly 32 characters long and composed of hexadecimal characters. For example, a valid key would be:
1234567890abcdef1234567890abcdef

> Note This key must match the authentication key of the SonicWALL appliance.

Step 12 Select the IP address of the GMS agent server that manages the Dell SonicWALL appliance from the **Agent IP Address** drop-down.

> Note If GMS is configured in a multi-tier distributed environment, you must select the GMS Agent whose IP address matches the IP address that you specified when configuring the SonicWALL appliance for GMS management.
>
> If GMS is in a single-server environment, the IP address of the GMS agent server already appears in the field.

Step 13 If the GMS is configured in a multi-tier distributed environment, enter the IP address of the backup GMS server in the **Standby Agent IP** field. The backup server automatically manages the SonicWALL appliance in the event of a primary server failure. Any Agent can be configured as the backup. If the GMS is deployed in a single server environment, leave this field blank.

Step 14 Click **OK**. The new Dell SonicWALL appliance appears in the GMS management interface. It has a yellow icon that indicates it has not yet been successfully acquired. GMS then attempts to set up an HTTPS connection to access the appliance. GMS then reads the appliance configuration and acquires the Dell SonicWALL appliance for reporting. This takes a few minutes. After the Dell SonicWALL appliance is successfully acquired, its icon turns blue, its configuration settings are displayed at the unit level, and its settings are saved to the database.

Chapter 7

Support

Related Technical Documentation

Dell SonicWALL GMS reference documentation is available at the Dell SonicWALL Technical Documentation Online Library:
https://support.software.dell.com.

Dell SonicWALL GMS video training is available from the GMS Development Team:
http://software.sonicwall.com/gmsvp/Dev-Training/

The Dell SonicWALL GMS 7.2 documentation set includes the following:

- Dell SonicWALL GMS 7.2 Release Notes
- Dell SonicWALL GMS 7.2 Software Getting Started Guide
- Dell SonicWALL GMS 7.2 Virtual Appliance Getting Started Guide
- Dell SonicWALL UMA EM5000 Getting Started Guide
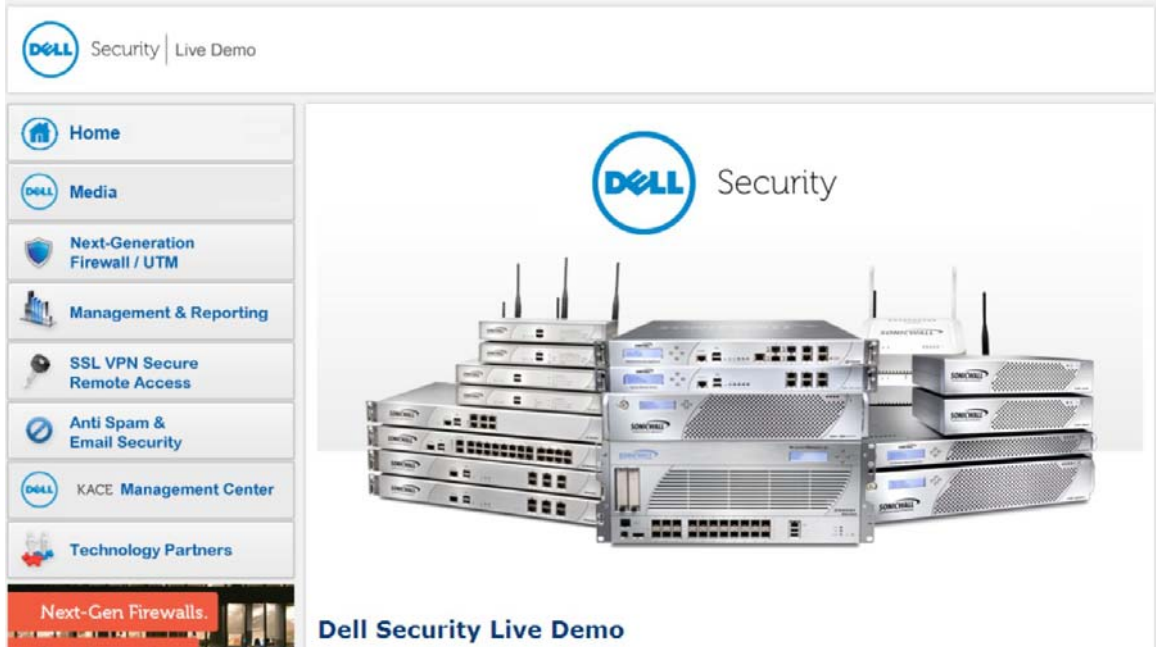- Dell SonicWALL GMS 7.2 Administrator's Guide

Dell SonicWALL Live Product Demos

Get the most out of your Dell SonicWALL GMS with the complete line of Dell SonicWALL products. The Dell SonicWALL Live Demo Site provides free test drives of Dell SonicWALL security products and services through interactive live product installations:

- UTM/Firewall/VPN
- Continuous Data Protection
- SSL VPN Secure Remote Access
- Content Filtering
- Email Security
- GMS and Analyzer

For further information, visit:

http://livedemo.sonicwall.com/