This Getting Started Guide contains installation procedures and configuration guidelines for deploying SonicWALL Global Management System (SonicWALL GMS) on a Windows server on your network. SonicWALL GMS is a Web-based application that can configure, manage, and monitor the status of thousands of SonicWALL Internet security appliances and non-SonicWALL appliances from a central location. SonicWALL GMS 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

Note: For complete documentation, refer to the SonicWALL GMS 6.0 Administrator's Guide. This and other documentation are available at: http://www.sonicwall.com/us/Support.html

For the latest SonicWALL GMS software version downloads and documentation, login to the MySonicWALL website at: http://www.mysonicwall.com.
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong> “Before You Begin” on page 3</td>
<td>3</td>
</tr>
<tr>
<td>• “System Requirements” on page 3</td>
<td>3</td>
</tr>
<tr>
<td>• “Record Configuration Information” on page 7</td>
<td>7</td>
</tr>
<tr>
<td><strong>2</strong> “Installing and Upgrading SonicWALL GMS” on page 9</td>
<td>9</td>
</tr>
<tr>
<td>• “Installing Universal Management Suite 6.0” on page 9</td>
<td>9</td>
</tr>
<tr>
<td>• “Upgrading From an Earlier Version of SonicWALL GMS” on page 15</td>
<td>15</td>
</tr>
<tr>
<td><strong>3</strong> “Registering and Licensing SonicWALL GMS” on page 20</td>
<td>20</td>
</tr>
<tr>
<td>• “Registering / Licensing SonicWALL GMS After a Fresh Install” on page 20</td>
<td>20</td>
</tr>
<tr>
<td>• “Registering Associated Servers in a Distributed Deployment” on page 24</td>
<td>24</td>
</tr>
<tr>
<td><strong>4</strong> “Selecting the Role for a SonicWALL GMS Server” on page 26</td>
<td>26</td>
</tr>
<tr>
<td>• “Using the Role Configuration Tool” on page 27</td>
<td>27</td>
</tr>
<tr>
<td>• “Manually Configuring the System Role” on page 33</td>
<td>33</td>
</tr>
<tr>
<td><strong>5</strong> “Introduction to the Management Interfaces” on page 42</td>
<td>42</td>
</tr>
<tr>
<td>• “Overview of the Two Interfaces” on page 42</td>
<td>42</td>
</tr>
<tr>
<td>• “Switching Between Management Interfaces” on page 43</td>
<td>43</td>
</tr>
<tr>
<td>• “SonicWALL UMH System Interface Introduction” on page 44</td>
<td>44</td>
</tr>
<tr>
<td>• “SonicWALL GMS Management Interface Introduction” on page 45</td>
<td>45</td>
</tr>
<tr>
<td><strong>6</strong> “Next Steps” on page 50</td>
<td>50</td>
</tr>
</tbody>
</table>
Before You Begin

See the following sections for information about SonicWALL GMS:
• “System Requirements” on page 3
• “Record Configuration Information” on page 7

System Requirements

The SonicWALL GMS 6.0 software comes with a base license to manage either 10 nodes 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 SonicWALL GMS, review the following requirements.

Operating System Requirements

The SonicWALL GMS 6.0 release supports the following operating systems:
• Windows Server 2008 SBS 64-bit
• Windows Server 2008 Standard 32-bit and 64-bit (SP1)
• Windows Server 2003 32-bit and 64-bit (SP2)
• Windows Server 2000 (SP4)

In all instances, SonicWALL GMS runs as a 32-bit application.

Database Requirements

The SonicWALL GMS 6.0 release supports the following databases:
• MySQL 32-bit, bundled with SonicWALL Universal Management Suite
• Microsoft SQL 2000 (SP4)
• Microsoft SQL 2005 32-bit and 64-bit (SP2)
  Regarding Microsoft SQL 2005, SonicWALL GMS supports:
  • SQL Server 2005 Workgroup
  • SQL Server 2005 Standard
  • SQL Server 2005 Enterprise
  SonicWALL GMS does not support Microsoft SQL 2005 Express.

Java Requirements

Java Plug-in version 1.5 or higher is required on client machines when accessing the SonicWALL GMS application interface. SonicWALL Universal Management Suite (UMS) automatically downloads the latest Java Plug-in. SonicWALL UMS services automatically download and use the latest version of JRE 1.6. For the Web server, SonicWALL UMS uses Tomcat 6.0.20.
Browser Requirements

- Microsoft Internet Explorer 7.0 or higher
- Mozilla Firefox 2.0 or higher
- Pop-up blocker disabled

SonicWALL GMS supports SSL 3.0 / TLS 1.0 for HTTPS management of SonicWALL appliances, and for direct login to the unit from GMS. For enhanced security across a GMS network for installations that must comply with stringent regulatory compliance and account management controls as found in such standards as PCI, SOX, or HIPAA, the following browsers have SSL 3.0/TLS 1.0 as standard encryption protocols:
  - Microsoft Internet Explorer 7.0 or higher
  - Mozilla Firefox 2.0 or higher

You can set other browsers to use these protocols in their **Tools > Internet Options > Advanced** settings.

---

**Note:** On Windows Server 2008, Internet Explorer 7 requires that the URL for the SonicWALL Universal Management Host is added to your trusted sites before it will display the system login page. The *Trusted Sites* list is available in **Tools > Internet Options > Security**.

---

Hardware for Single Server Deployment

- x86 Environment: Minimum 3 GHz processor dual-CPU Intel processor, 4 GB RAM, and 300 GB disk space

Hardware for a Distributed Server Deployment

**GMS Server**

- x86 Environment: Minimum 3 GHz processor single-CPU Intel processor, 2 GB RAM, and 300 GB disk space

**Database Server**

- x86 Environment: Minimum 3 GHz processor dual-CPU Intel processor, 2 GB RAM, and 300 GB disk space

---

**Note:** It is highly recommended that you install the database on a separate server.
Network Requirements

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

- The SonicWALL GMS server must have access to the Internet
- The SonicWALL GMS server must have a static IP address
- The SonicWALL GMS server’s network connection must be able to accommodate at least 1 KB/s for each device under management. For example, if SonicWALL GMS is monitoring 100 SonicWALL appliances, the connection must support at least 100 KB/s.
- You should either disable the Windows personal firewall, or enable ports for syslog, syslog forwarding, and SNMP traps. The default syslog port is UDP 514 and the default SNMP port is UDP 162. If the SonicWALL GMS system is behind a gateway or firewall, you may need to open up these ports on that device. These ports on a gateway or firewall should be opened up only when HTTPS Management is being used for remote management. The ports need not be opened up if the Existing Tunnel or GMS Management Tunnel modes are being used for management.

**Alert:** *Depending on the configuration of SonicWALL log settings and the amount of traffic handled by each device, the network traffic can vary dramatically. The 1 KB/s for each device is a general recommendation. Your installation requirements may vary.*
SonicWALL Appliance and Firmware Support

<table>
<thead>
<tr>
<th>SonicWALL Platforms</th>
<th>SonicWALL Firmware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall / UTM / VPN</td>
<td></td>
</tr>
<tr>
<td>NSA Series, E-Class NSA Series</td>
<td>SonicOS Enhanced 5.0 or newer</td>
</tr>
<tr>
<td>TZ Series</td>
<td>SonicOS Enhanced 3.2 or newer</td>
</tr>
<tr>
<td></td>
<td>SonicOS Standard 3.1 or newer</td>
</tr>
<tr>
<td>PRO Series</td>
<td>SonicOS Enhanced 3.2 or newer</td>
</tr>
<tr>
<td>SonicWALL CSM Series</td>
<td>SonicOS CF 2.0 or newer</td>
</tr>
<tr>
<td>Secure Remote Access</td>
<td></td>
</tr>
<tr>
<td>SonicWALL SMB SSL-VPN Series</td>
<td>SonicOS SSL-VPN 2.0 or newer</td>
</tr>
<tr>
<td>SonicWALL Aventail EX-Series</td>
<td>Aventail 9.0 or newer</td>
</tr>
<tr>
<td>Backup and Recovery</td>
<td></td>
</tr>
<tr>
<td>SonicWALL CDP Series</td>
<td>SonicWALL CDP 2.3 or newer for basic</td>
</tr>
<tr>
<td></td>
<td>management</td>
</tr>
<tr>
<td></td>
<td>SonicWALL CDP 5.1 or newer for</td>
</tr>
<tr>
<td></td>
<td>comprehensive Multi-Solution management</td>
</tr>
<tr>
<td>Email Security / Anti-Spam</td>
<td></td>
</tr>
<tr>
<td>SonicWALL Email Security Series</td>
<td>SonicWALL Email Security 7.2 or newer</td>
</tr>
</tbody>
</table>

Note: *Legacy SonicWALL XPRS/XPRS2, SonicWALL SOHO2, SonicWALL Tele2, and SonicWALL Pro/Pro-VX models are not supported.*

Non-SonicWALL Appliance Support

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

GMS Gateway Recommendations

A GMS gateway is a SonicWALL UTM appliance that allows for secure communication between the SonicWALL GMS server and the managed appliance(s), using VPN tunnels.
A GMS gateway is not required in all deployment scenarios, but when deployed, the GMS gateway must be a SonicWALL VPN-based network security appliance running SonicOS Enhanced firmware or another VPN device that is interoperable with SonicWALL VPN. The GMS gateway provides a VPN management tunnel for each managed appliance. The number of management tunnels depends on the number of VPNs supported by the GMS gateway appliance and may be a limiting factor.

For complete information about SonicWALL GMS management methods and requirements for a GMS Gateway, see the **GMS Gateway Requirements** section in the *SonicWALL GMS Administrator’s Guide*, available on: http://www.sonicwall.com/us/Support.html

**Note:** A management VPN tunnel is only supported for SonicWALL UTM appliances, and is not supported for SonicWALL CDP or SonicWALL SSL-VPN appliances. For managing these devices, a GMS Gateway is not needed.

### Record Configuration Information

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

**SonicWALL GMS Information**

<table>
<thead>
<tr>
<th><strong>SMTP Server Address:</strong></th>
<th>The IP address or host name of your Simple Mail Transfer Protocol (SMTP) server. For example, mail.emailprovider.com.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HTTP Web Server Port:</strong></td>
<td>The number of your Web server port if customized. The default port is 80.</td>
</tr>
<tr>
<td><strong>HTTPS Web Server Port:</strong></td>
<td>The number of your secure (SSL) Web server port if customized. The default port is 443.</td>
</tr>
<tr>
<td><strong>GMS Administrator Email 1:</strong></td>
<td>The email address of a SonicWALL GMS administrator who will receive email notifications from SonicWALL GMS.</td>
</tr>
<tr>
<td><strong>GMS Administrator Email 2:</strong></td>
<td>The email address of an additional SonicWALL GMS administrator who will receive email notifications from SonicWALL GMS. This field is optional.</td>
</tr>
<tr>
<td><strong>Sender Email Address:</strong></td>
<td>The email address from which the email notifications will be sent by SonicWALL GMS.</td>
</tr>
<tr>
<td><strong>GMS Gateway IP:</strong></td>
<td>The IP address of the SonicWALL GMS gateway between the SonicWALL GMS agent and the network. This optional field is only applicable if you have a GMS gateway.</td>
</tr>
<tr>
<td><strong>GMS Gateway Password:</strong></td>
<td>The password for the SonicWALL GMS gateway. This optional field is only applicable if you have gateway between the SonicWALL GMS and the network.</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Database Vendor:</strong></td>
<td>Your database vendor if you are using a SQL Server database. Eve</td>
</tr>
<tr>
<td><strong>Database Host/IP:</strong></td>
<td>The IP address of the database host. This is not required when using the bundled database on this server.</td>
</tr>
<tr>
<td><strong>Database User:</strong></td>
<td>The MySQL user name for the database administrator. This is not required when using the bundled database on this server. Refer to “Configuring Database Settings” on page 38.</td>
</tr>
<tr>
<td><strong>Database Password:</strong></td>
<td>The MySQL password for the database administrator. This is not required when using the bundled database on this server.</td>
</tr>
</tbody>
</table>
SonicWALL GMS can be configured for a single server or in a distributed environment on multiple servers.

SonicWALL GMS 6.0 can be installed as a fresh install or as an upgrade to SonicWALL GMS 5.1. Refer to the GMS 5.1 Getting Started Guide for information on upgrading from versions earlier than 5.1. This section contains the following subsections:

- “Installing Universal Management Suite 6.0” on page 9
- “Upgrading From an Earlier Version of SonicWALL GMS” on page 15

### Installing Universal Management Suite 6.0

In SonicWALL GMS 6.0, all software components related to SonicWALL GMS and SonicWALL ViewPoint, including the MySQL database, executable binary files for all GMS services, and other necessary files, are installed using the Universal Management Suite 6.0 single-binary installer. All GMS and ViewPoint files are installed as the Universal Management Suite 6.0, but no distinction is made between GMS and ViewPoint during the installation. The initial installation phase takes just a few minutes for any type of installation, such as GMS server, ViewPoint server, database server, or any other role.

To perform a fresh install of the Universal Management Suite 6.0 from the single binary installer, perform the following steps:

1. Log on to your SonicWALL GMS management computer as **administrator** (Windows). Launch the SonicWALL Universal Management Suite 6.0 installer, by double-clicking the file `sw_gmsvp_win_eng_6.0.xxxx.xxxx.exe` (where “xxxx” represent the exact version numbers). It may take several seconds for the InstallAnywhere self-extractor to initialize.
2. In the Introduction screen, click **Next**.

![Introduction Screen](image)

3. In the License Agreement screen, select the radio button next to **I accept the terms of the License Agreement**. Click **Next**.

![License Agreement Screen](image)
4. Select the path to the folder where you would like to install the files. You can accept the default path, C:\GMSVP, type in a new path, or click the Choose button to navigate to the selected folder. When you are finished, click Next.

![Image of SonicWALL Universal Management Suite Choose Install Folder]

> Alert: Do not include spaces in the installation path.

5. In the SonicWALL Universal Management Suite Settings screen, select or type in the IP address to which the SonicWALL GMS services should bind to listen for inbound TCP, UDP, SNMP, syslog, or other packets. The installer detects and offers radio buttons for any IP addresses associated with the system. The default is your management computer IP address. To use a different IP address, select Other and type the IP address into the field. Click Next.

![Image of SonicWALL Universal Management Suite Settings]

6. To use a custom port for HTTP or HTTPS traffic to the system’s Web Server, type the port number into the HTTP Port or HTTPS Port field.
If you receive the message “Cannot bind to the port number specified. Please specify a different one,” the port you specified is in use by another program, for example, Internet Information Services (IIS). Specify a different, unused port, such as 8080.

Tip: If you specify a custom port, you will need to modify the URLs you use to access GMS by using the following format: http://localhost:<port>/ (to login from the local host) or http://<ipaddress>:<port>/ (to login from a remote location). For example, if you specified HTTP port 8080, the URL would be http://localhost:8080/ for a local host login, or http://10.0.93.20:8080/ for a remote login.

7. Click Install.
8. If you see a Windows Security Alert for Java, click Unblock.
9. The installer displays a progress bar as the files are installed. Wait a few minutes for the installer to finish installing.

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

11. The Important Registration Information screen provides the URL and credentials to use to log into the SonicWALL GMS Universal Management Host system interface after restarting your system:
   The default URL for accessing the interface from the local system is: http://localhost:80/
   The default credentials are:
   User name – admin
   Password – password
This screen also provides information about registration. To register a SonicWALL GMS installation, use the 12-character serial number that you received when you purchased this product. Click Next.

12. In the Installation Complete screen, select Yes, restart my system to restart your system immediately, or select No, I will restart my system myself to restart your system later. Click Done.

13. After restarting your system, you can access the SonicWALL UMH system interface to register the product and configure the GMS server settings on this system. Access the SonicWALL GMS UMH system interface by either clicking on the new desktop shortcut for SonicWALL Universal Management Suite 6.0 (your default Web browser will launch http://localhost/appliance/login), or by pointing your browser at http://localhost/.
14. Log in using the username **admin** and the password **password**. You will be prompted to change your password.

**Note:** *You are forced to change your password the first time you login.*

15. To register and license SonicWALL GMS, see “Registering Associated Servers in a Distributed Deployment” on page 24.

### Upgrading From an Earlier Version of SonicWALL GMS

You can use the SonicWALL UMS installer to upgrade from the 5.1 release to 6.0. To complete registration, the system must have access to the Internet and you must have a MySonicWALL account.

When upgrading a distributed deployment, upgrade and register the primary system first. This is usually the SonicWALL GMS Console system from the original deployment. All subsequent instances of SonicWALL GMS will use the primary system’s 12 character serial number when registering as components of the deployment. Each server in the distributed deployment must be upgraded and registered individually.

If the GMS Console (Web server) is set up for HTTPS management, the upgrade to GMS will preserve the HTTPS settings for the GMS Web server.

The upgrade installer checks with the SonicWALL backend to see if the SonicWALL GMS deployment has a valid support license. If it does not, then the upgrade discontinues. If the SonicWALL GMS installer detects that the SonicWALL backend site is not accessible, it prompts the user to enter an Upgrade Key. If the key is valid, it allows the upgrade to continue. If the key is invalid, the installation fails.

**Note:** *In a distributed environment, stop all GMS services on all GMS servers before performing an upgrade. You must upgrade all GMS servers in your deployment to the same version of SonicWALL GMS 6.0. You cannot have some servers running version 5.1 and others running 6.0.*

**Tip:** *It is highly recommended that you backup your database, GMS installation folders, and the <GMS installation folder>\conf\sgmsConfig.xml file on all GMS servers prior to performing the SonicWALL GMS upgrade.*

**Tip:** *If you are upgrading from 5.1 and if your database is large (greater than 40 GB), you will need to use the Pre-Upgrade Tool (available for download from MySonicWALL). If this tool is not used, the upgrade time may extend for hours and the downtime of SonicWALL GMS could be substantial. By using the Pre-Upgrade tool, the downtime can be better managed.*
To upgrade the SonicWALL GMS software, perform the following steps:

1. Log on to your SonicWALL GMS management computer as **administrator** (Windows). Launch the SonicWALL Universal Management Suite 6.0 installer, by double-clicking the file `sw_gmsvp_win_eng_6.0.xxxx.xxxx.exe` (where “xxxx” are the exact version numbers). It may take several seconds for the InstallAnywhere self-extractor to initialize.

2. In the Introduction screen, click **Next**.

3. In the License Agreement screen, select the radio button next to **I accept the terms of the License Agreement**. Click **Next**.
4. Wait while the installer prepares to install SonicWALL UMS on your system.

5. Click **Install** to upgrade your installation.

Note: You must have a valid support license to upgrade your SonicWALL GMS.

6. The Installer detects the previous installation of SonicWALL GMS. Click **Install** to proceed with the upgrade.
7. If you see a Windows Security Alert for Java, click **Unblock**.

![Windows Security Alert](image1)

8. The installer displays a progress bar as the files are installed. Wait a few minutes for the installer to finish installing.

![Installer Progress Bar](image2)

9. After the files are installed, whether or not the system has a Personal Firewall such as Windows Firewall enabled, a dialog is displayed notifying you to either disable the firewall or manually open the syslog and SNMP ports, and to ensure that these ports are open on your network gateway or firewall if you plan to use HTTPS Management.

![Manual Port Opening Dialog](image3)
mode for managing remote appliances (instead of GMS Management Tunnel or Existing Tunnel modes). Click OK. Be sure to adjust the settings as recommended.

10. The final installer screen contains the path of the installation folder, and warns you that the Universal Management Suite Web page will be launched next. Click Done.
Registering and Licensing SonicWALL GMS

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 software installations on Windows servers or to SonicWALL UMA appliances.

This section contains the following subsections:

- “Registering / Licensing SonicWALL GMS After a Fresh Install” on page 20
- “Registering Associated Servers in a Distributed Deployment” on page 24

Registering / Licensing SonicWALL GMS After a Fresh Install

SonicWALL GMS registration is performed using the SonicWALL Universal Management Host (UMH) system interface. When installing SonicWALL Universal Management Suite 6.0 on a server, or host, a Web server is installed to provide the UMH system interface. The system interface is available by default at http://localhost/ after restarting the system.

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

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

The License Manager provides a way to register the product as either SonicWALL GMS or SonicWALL ViewPoint. Your choice determines the remaining installation process after registration and licensing are completed. In this guide, SonicWALL GMS registration is described.

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

1. Double-click the SonicWALL Universal Management Suite 6.0 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) in "Installing Universal Management Suite 6.0" on page 9, modify the URL as follows: \texttt{http://localhost:<port>/}. For example, if you specified port 8080, the URL would be \texttt{http://localhost:8080/}.

2. On the Universal Management Host Login page, type \texttt{admin} in the User field, and \texttt{password} in the Password field and then click Submit.

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.

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.
Optionally, you can select the **Perform this check after 30 days** checkbox 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.

![Windows Firewall - Alert!]

<table>
<thead>
<tr>
<th>Windows Firewall - Alert!</th>
</tr>
</thead>
<tbody>
<tr>
<td>Please check Windows Firewall settings on the GM15/ViewPoint Server.</td>
</tr>
<tr>
<td>If Windows Firewall is enabled on your server, Syslog and SNMP packets will not be collected by the product, which will affect the Management, Alerting and Reporting functionalities of the product.</td>
</tr>
<tr>
<td>Please open ‘Windows Firewall’ in Control Panel to check the status of Windows Firewall. Make sure you have either disabled Windows Firewall software on the Server, or unblocked Syslog (typically UDP 514) and SNMP (UDP 162) packets.</td>
</tr>
<tr>
<td>Click OK only after you have undertaken these steps.</td>
</tr>
<tr>
<td>□ Perform this check after 30 days.</td>
</tr>
<tr>
<td>OK</td>
</tr>
</tbody>
</table>

5. 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 the **Register** button in the top, right corner.
6. 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 here in the sentence. **If you do not have a mySonicWall account, please click here to create one.**

7. 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 SonicWALL GMS that you are registering in a multi-server deployment, the Serial Number and Authentication Code you received from your SonicWALL sales representative is entered here. As you add more instances of SonicWALL GMS on Windows Server systems to the distributed deployment, use the same serial number used for the installation of the first GMS Windows Software or 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 24.

8. 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 SonicWALL GMS that you have registered in a multi-server deployment, the Friendly Name for this system will also be used as the name for the distributed deployment.** See “Registering Associated Servers in a Distributed Deployment” on page 24.

9. Click **Submit**.

10. The License Management page displays a completion screen. Click **Continue**.

   ![License Management](image)

   The License Management page displays license summary information.

   ![License Management](image)

11. After registration, the next step is to select the role for this GMS server. Continue with the procedure described in “Selecting the Role for a SonicWALL GMS Server” on page 26.

**Registering Associated Servers in a Distributed Deployment**

When you have a distributed SonicWALL GMS deployment involving more than one SonicWALL UMA EM5000 appliance or software instance of SonicWALL GMS, you can associate these components during the registration process. A MySonicWALL account is required. In a distributed deployment, 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 SonicWALL GMS when registering each subsequent server in the distributed deployment.

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

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

1. In a browser, Log into the system management interface and click the Register button.
2. On the License Management page, enter the same MySonicWALL user name and password that you used when registering the primary instance of SonicWALL GMS into the appropriate fields and then click Submit.
3. On the second License Management page, do one of the following:
   - Type the 12 character serial number of the primary SonicWALL GMS into the Serial Number field and type the authentication code of the primary SonicWALL GMS into the Authentication Code field. The primary SonicWALL GMS must already be registered.
   - If adding a SonicWALL UMA EM5000 as a secondary member of a distributed deployment, the License Manager automatically populates the Serial Number field. You will have the opportunity to add this unit to the existing deployment in a later step.
   - If you have an 8 character serial number because you upgraded this distributed deployment from a previous version of SonicWALL GMS (such as from 5.0 to 5.1 and then to 6.0), click the Click here if you have an 8 character Serial Number link and enter the 8 character serial number of the primary SonicWALL GMS.
4. Type a descriptive name for the system into the Friendly Name field and then click Submit.
5. In the License Management completion screen, click Continue.
6. After registration, the next step is to select the role for this GMS server. Continue with the procedure described in “Selecting the Role for a SonicWALL GMS Server” on page 26.
Selecting the Role for a SonicWALL GMS Server

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

Your SonicWALL GMS can be deployed in any of the following roles:
- All in One
- Database Only
- Console
- Agent
- Monitor
- Syslog Collector

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 SonicWALL appliances, you can use several SonicWALL GMS instances operating in different roles in a distributed deployment. These instances can run on Windows Server machines or on 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 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 perform the configuration tasks and other tasks of the Agent that went down.

Note: 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 the Include Database (MYSQL) checkbox if configuring the system with any other role
- By setting up a compatible database on another machine and providing that IP address when prompted
The initial **Deployment > Role** page is shown below:

Using the Role Configuration Tool

The Role Configuration Tool is a wizard that guides you through the process of defining the deployment role for SonicWALL GMS. Your system must be registered and licensed for 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 SonicWALL 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, perform the following steps:

1. Log into the appliance management interface and navigate to the **System > Status** page.
2. Click the **Click here** link at the top of the page.
3. In the Introduction page of the Role Configuration Tool, click **Next**.

![Role Configuration Tool Introduction](image)

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

![Role Configuration Tool Setup Type](image)

**Note:** *If you selected Yes, skip step 5 and proceed to step 6.*
5. In the Deployment Type page, select **Yes** if this system will be the only SonicWALL GMS server in the deployment, or select **No** if there will be multiple GMS servers. Click **Next**.

![Deployment Type Page](image1)

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

   The list of roles on this page will vary depending on your previous selections such as whether this system is part of an existing SonicWALL 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.

![Role Configuration Page](image2)
7. In the Database Configuration page, enter the database parameters that are required for the selected role. The database fields will vary depending on your previous selections.

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

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
- The Include Database (MYSQL) checkbox 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 SonicWALL 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.

8. When finished entering the database parameters, click **Next**.

9. 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
   
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.
10. In the **Syslog Server Port** field, type in the port used for receiving syslog messages or accept the default of 514.

11. 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**.

12. Click **Next**.

13. 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.

14. 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.
15. Click **Close** to exit the Role Configuration Tool.

Manually Configuring the System Role

You can configure the role of the SonicWALL GMS system without using the Role Configuration Tool.

All role configuration is performed in the UMH system interface, available at the URL: **http://<IP address>[:<port>]/appliance/**

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

- “Configuring the All In One Role” on page 34
- “Configuring the Database Only Role” on page 34
- “Configuring the Console Role” on page 35
- “Configuring the Agent Role” on page 36
- “Configuring the Monitor Role” on page 37
- “Configuring the Syslog Collector Role” on page 38
- “Configuring Database Settings” on page 38
- “Configuring Deployment Settings” on page 40
Configuring the All In One Role

All In One deployments are ideal for managing a small number of SonicWALL appliances or for test environments. However, 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.

The All In One role provides all nine services utilized by SonicWALL GMS:

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

To deploy your SonicWALL GMS server in the All In One role, perform the following steps:

1. Log into your UMH system interface by pointing your browser at the URL: http://localhost/
2. On the Deployment > Role page under Host Role Configuration, select the All In One radio button.
3. If this SonicWALL GMS server will connect to managed appliances through a GMS gateway, type the gateway IP address into the GMS Gateway IP field. To determine if a GMS gateway is required, see the GMS Gateway Recommendations section, on page 6.
4. If a GMS gateway will be used, type the password into both the GMS Gateway Password and Confirm GMS Gateway Password fields.
5. If this 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.
6. Configure the database settings as described in the Configuring Database Settings section, on page 38.
7. Configure the Web port settings as described in the Configuring Web Port Settings section, on page 40.
8. To apply your changes, click Update. To change the settings on this page back to the defaults, click Reset.

Configuring the Database Only Role

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

SonicWALL GMS can use a MySQL database installed on a SonicWALL UMA EM5000 appliance or on a server, or a Microsoft SQL Server database installed on a server. Only the MySQL database included in the installer is supported. If upgrading from a SonicWALL GMS 5.0 installation that used the SonicWALL MySQL installer, SonicWALL GMS 6.0 will continue to support that MySQL installation.

On the Deployment > Role page in the UMH system interface, you can configure your SonicWALL GMS systems to use either a MySQL or a SQL Server database.

To deploy your SonicWALL GMS in the Database Only role, perform the steps described in the Configuring Database Settings section, on page 38.

**Configuring the Console Role**

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

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

- Provides Web user interface for the 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 deploy your SonicWALL GMS server in the Console role, perform the following steps:

1. Log into your UMH system interface and navigate to the Deployment > Role page.
2. Under Host Role Configuration, select the Console radio button.
3. If this SonicWALL GMS server will connect to managed appliances through a GMS gateway, type the gateway IP address into the GMS Gateway IP field. To determine if a GMS gateway is required, see the GMS Gateway Recommendations section, on page 6.
4. If a GMS gateway will be used, type the password into both the GMS Gateway Password and Confirm GMS Gateway Password fields.
5. If this 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.

6. To use a MySQL or Microsoft SQL Server database on another system, do not select the **Include Database (MYSQL)** checkbox. To include the MySQL database on this system (not recommended), select this checkbox (for this configuration, select the All In One role instead of the Console role).

7. Configure the database settings as described in the *Configuring Database Settings* section, on page 38.

8. Configure the Web port settings as described in the *Configuring Web Port Settings* section, on page 40.

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

**Configuring the Agent Role**

The Agent role can be used in a distributed deployment of 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 SonicWALL Universal Management Suite services run on an Agent system:

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

To deploy your SonicWALL GMS server in the Agent role, perform the following steps in the UMH system interface:

1. Navigate to the **Deployment > Role** page. Under **Host Role Configuration**, select the **Agent** radio button.

2. If this SonicWALL GMS server will connect to managed appliances through a GMS gateway, type the gateway IP address into the **GMS Gateway IP** field. To determine if a GMS gateway is required, see the *GMS Gateway Recommendations* section, on page 6.
3. If a GMS gateway will be used, type the password into both the **GMS Gateway Password** and **Confirm GMS Gateway Password** fields.

4. If this 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.

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

6. Configure the database settings as described in the **Configuring Database Settings** section, on page 38.

7. Configure the Web port settings as described in the **Configuring Web Port Settings** section, on page 40.

8. 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 SonicWALL GMS server to monitoring appliances and applications in a multi-server SonicWALL GMS deployment. The monitoring is based on ICMP probes, TCP probes and SNMP OID retrievals.

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

To deploy your SonicWALL GMS server in the Monitor role, perform the following steps in the UMH system interface:

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

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

3. Configure the database settings as described in the **Configuring Database Settings** section, on page 38.

4. Configure the Web port settings as described in the **Configuring Web Port Settings** section, on page 40.

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

The syslog messages are used by the Reports Summarizer service running on another SonicWALL GMS server or 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 SonicWALL Universal Management Suite Syslog Collector service runs on a Syslog Collector system.

To deploy your SonicWALL GMS server in the Syslog Collector role, perform the following steps in the UMH system interface:

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

2. If this 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.

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

4. Configure the database settings as described in the Configuring Database Settings section, on page 38.

5. Configure the Web port settings as described in the Configuring Web Port Settings section, on page 40.

6. 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 the Include Database (MYSQL) checkbox 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. SonicWALL GMS can use either a MySQL or a SQL Server database.
Note: If this appliance will connect to a SQL Server system with a non-default instance name, then the entries will be different than described in this section. Refer to the SonicWALL GMS Administrator's Guide for configuration instructions.

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

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

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

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.

4. In the Database Host field, type in the IP address of the database server or accept the default, localhost, if this SonicWALL GMS 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.

5. To use a different user name when SonicWALL GMS accesses the database, type the user name into the Database User field. The default user name is “sa”.

6. Type the password that SonicWALL GMS will use to access the database into both the Database Password and Confirm Database Password fields.

7. Under Administrator Credentials, type the password for the administrator (root) account into both the Admin Password and Confirm Admin Password fields.
Note that the Administrator Credentials fields are only displayed and editable in the following circumstances:

- The Database Type is MySQL
- The Include Database (MYSQL) checkbox 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 SonicWALL GMS application.

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

---

Note: It may take 10 or 15 minutes for a database installation to complete. The database installation creates a minimal GMS database. To change database sizes, you may 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 SonicWALL GMS maintenance plans, refer to the 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 40
- “Configuring SMTP Settings” on page 41

Configuring Web Port Settings

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

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

   ![Web Port Configuration](image)

2. To use a different port for HTTPS access to the SonicWALL GMS server, type the port number into the HTTPS Port field. The default port is 443.
3. Click **Update** to apply the Web port settings.

**Note:** *Changing the Web port settings will cause the system to restart.*

4. 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 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 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, perform the following steps:

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

2. In the **Sender address** field, enter the email address that will appear as the ‘From’ address when email alerts are sent to the administrator.

3. In the **Administrator address** field, enter a valid email address for the administrator who will receive email alerts.

4. Click **Update** to apply the SMTP settings.
Introduction to the Management Interfaces

This section describes the two SonicWALL GMS management interfaces. An almost identical URL is used when accessing either the 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” on page 42
- “Switching Between Management Interfaces” on page 43
- “SonicWALL UMH System Interface Introduction” on page 44
- “SonicWALL GMS Management Interface Introduction” on page 45

Overview of the Two Interfaces

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

- **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.
• **SonicWALL GMS Management Interface** – Used to access the SonicWALL GMS application that runs on the Windows server. This interface is used to configure GMS management of 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/
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 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 the **Switch** button in the top right corner of the page. The **Switch** button is only visible for users with SuperAdmin privileges.
SonicWALL UMH System Interface Introduction

The SonicWALL UMH system interface is used for system management of the 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 SonicWALL Universal Management Suite 6.0 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 login to the 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 SonicWALL GMS.*
SonicWALL GMS Management Interface Introduction

SonicWALL GMS is a Web-based application for configuring, managing, monitoring and gathering reports from thousands of SonicWALL Internet security appliances and non-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 45
- “SonicToday” on page 45
- “Live Monitoring” on page 45
- “Multi-Solution Management” on page 46
- “Management Interface” on page 46

Login Screen

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

SonicToday

After login is completed, users will land at the SonicToday tab of the main default page. Using RSS and AJAX technology, SonicToday is a tab intended to work as a customizable dashboard to monitor the latest happenings with this SonicWALL GMS 6.0 deployment, the network, the IT and Security World, as well as the rest of the world.

Live Monitoring

The Live Monitoring feature provides users with the ability to monitor an entire network through the correlation of syslog messages received from appliances throughout a deployment. The collected syslogs are filtered with user-defined rules to become alerts. By viewing alerts in the Live Monitoring screen, users can monitor a network, analyze traffic based on protocols, Web usage and productivity, and detect viruses and attacks in the network.
Multi-Solution Management

The Multi-Solution Management feature in SonicWALL GMS provides next generation management capability by allowing administrators to manage multiple appliance types—UTM, CDP, SSL VPN, EX-Series SSL VPN, and Email Security—through their respective Web user interfaces over HTTP and HTTPS. Multi-Solution Management enables GMS Core Management functionality through the GMS user interface. Functions such as creating tasks, posting policies, scheduling tasks, and more are easily completed across multiple appliances at Unit Node and Group Node levels.

Management Interface

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

The SonicWALL GMS management interface has four main sections:

- “Navigation Tabs” on page 47
- “Left Pane” on page 47
- “Center Pane” on page 49
- “Right Pane” on page 49
Navigation Tabs

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

![SonicWALL GMS management interface navigation tabs]

The seven navigation tabs are SonicToday, UTM, SSL-VPN, 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 SonicWALL GMS tabs and to manage SonicWALL GMS settings and manage SonicWALL GMS settings that affect the environment globally.

Left Pane

The left pane of the 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 for the four appliance tabs: UTM, SSL-VPN, 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 48.

---

Note: If there is only one appliance visible in the Left Pane, then the Left Pane will automatically collapse to present a larger screen for the rest of the UI.
### 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 SonicWALL GMS management interface.

<table>
<thead>
<tr>
<th>Appliance Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![One blue box]</td>
<td>One blue box indicates that the appliance is operating normally. The appliance is accessible from the SonicWALL GMS, and no tasks are pending or scheduled.</td>
</tr>
<tr>
<td>![Two blue boxes]</td>
<td>Two blue boxes indicate that appliances in a group are operating normally. All appliances in the group are accessible from the SonicWALL GMS and no tasks are pending or scheduled.</td>
</tr>
<tr>
<td>![One blue box with a lightning flash]</td>
<td>One blue box with a lightning flash indicates that one or more tasks are pending or running on the appliance.</td>
</tr>
<tr>
<td>![Two blue boxes with a lightning flash]</td>
<td>Two blue boxes with a lightning flash indicate that tasks are currently pending or running on one or more appliances within the group.</td>
</tr>
<tr>
<td>![Two blue boxes with a clock]</td>
<td>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.</td>
</tr>
<tr>
<td>![One blue box with a clock]</td>
<td>One blue box with a clock indicates that one or more tasks are scheduled on the appliance.</td>
</tr>
<tr>
<td>![One yellow box]</td>
<td>One yellow box indicates that the appliance has been added to SonicWALL GMS (provisioned) but not yet acquired.</td>
</tr>
<tr>
<td>![Two yellow boxes]</td>
<td>Two yellow boxes indicate that one or more appliances in the group have been added to SonicWALL GMS but not acquired.</td>
</tr>
<tr>
<td>![One yellow box with a lightning flash]</td>
<td>One yellow box with a lightning flash indicates that one or more tasks are pending on the provisioned appliance.</td>
</tr>
<tr>
<td>![Two yellow boxes with a lightning flash]</td>
<td>Two yellow boxes with a lightning flash indicate that tasks are pending on one or more provisioned appliances within the group.</td>
</tr>
<tr>
<td>![One red box]</td>
<td>One red box indicates that the appliance is not accessible from SonicWALL GMS.</td>
</tr>
<tr>
<td>![Two red boxes]</td>
<td>Two red boxes indicate that one or more appliance in the group is not accessible from SonicWALL GMS.</td>
</tr>
<tr>
<td>![Two red boxes with a lightning flash]</td>
<td>Two red boxes with a lightning flash indicate that one or more appliances in the group is not accessible from SonicWALL GMS and has one or more tasks pending.</td>
</tr>
<tr>
<td>![One red box with a yellow flash]</td>
<td>One red box with a yellow flash indicates that the appliance is not accessible from SonicWALL GMS and has one or more tasks pending.</td>
</tr>
</tbody>
</table>
Center Pane

The center pane displays for the four appliance tabs: **UTM**, **SSL-VPN**, **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 exists 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 **UTM** and **SSL-VPN**.

The current selection in the center pane is indicated by an arrow. For example, the figure to the left displays the current selection **System > Status**. The center pane options change based on the navigational tab and left pane selections, and selections in the center pane modify the configurations available in the right pane. For example, the figure below displays the tasks available for the **Policies** tab, with **View All** selected in the left pane. The right pane will display configuration options for the **System > Status** selection in this pane.

Right Pane

The right pane displays the available configuration tasks based on the current selection of navigational tab, left pane and center pane options. Configurations performed in the right pane modify global, group or appliance settings. For example, the figure on the left displays the status and tasks available for the **Policies** navigation tab, left pane selection **View All**, and center pane selection **System > Status**.
Next Steps

After installation, registration, and role configuration, the next steps in setting up your SonicWALL GMS deployment are performed in the SonicWALL GMS management interface. See the SonicWALL GMS 6.0 Administrator’s Guide for complete information about configuring SonicWALL GMS device management and reporting. This guide and other related documents are available on: http://www.sonicwall.com/us/Support.html

Suggested next steps include the following:

- **Provisioning units** – Log into each appliance that will be managed by SonicWALL GMS, and enable GMS Management.

- **Adding units** – In the SonicWALL GMS management interface, right-click in the left navigation pane and select *Add Unit* to add a SonicWALL appliance to GMS management.

- **Scheduling reports** – Use the Console panel of the SonicWALL GMS management interface to set up a reporting schedule for your managed appliances.
Copyright Notice

© 2009 SonicWALL, Inc.
All rights reserved.

Under the copyright laws, this manual or the software described within, cannot be copied, in whole or part, without the written consent of the manufacturer, except in the normal use of the software to make a backup copy. The same proprietary and copyright notices must be affixed to any permitted copies as were affixed to the original. This exception does not allow copies to be made for others, whether or not sold, but all of the material purchased (with all backup copies) can be sold, given, or loaned to another person. Under the law, copying includes translating into another language or format.

Specifications and descriptions subject to change without notice.

Trademarks

SonicWALL is a registered trademark of SonicWALL, Inc.


Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the U.S. and/or other countries.

Firefox is a trademark of the Mozilla Foundation.

Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies and are the sole property of their respective manufacturers.
This End User Licensing Agreement (EULA) is a legal agreement between you and SonicWALL, Inc. (SonicWALL) for the SonicWALL software product identified above, which includes computer software and any and all associated media, printed materials, and online or electronic documentation (SOFTWARE PRODUCT). By opening the sealed package(s), installing, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, do not open the sealed package(s), install or use the SOFTWARE PRODUCT. You may however return the unopened SOFTWARE PRODUCT to your place of purchase for a full refund.

The SOFTWARE PRODUCT is licensed, not sold.

You acknowledge and agree that all right, title, and interest in and to the SOFTWARE PRODUCT, including all associated intellectual property rights, are and shall remain with SonicWALL. This EULA does not convey to you an interest in or to the SOFTWARE PRODUCT, but only a limited right of use revocable in accordance with the terms of this EULA.

- The SOFTWARE PRODUCT is licensed as a single product and can only be used as such.
- You may also store or install a copy of the SOFTWARE PRODUCT on a storage device, such as a network server, used only to install or run the SOFTWARE PRODUCT on your other computers over an internal network.
- You may not resell, or otherwise transfer for value, rent, lease, or lend the SOFTWARE PRODUCT.
- The SOFTWARE PRODUCT is trade secret or confidential information of SonicWALL or its licensors. You shall take appropriate action to protect the confidentiality of the SOFTWARE PRODUCT. You shall not reverse-engineer, de-compile, or disassemble the SOFTWARE PRODUCT, in whole or in part. The provisions of this section will survive the termination of this EULA.
- You agree and certify that neither the SOFTWARE PRODUCT nor any other technical data received from SonicWALL, nor the direct product thereof, will be exported outside the United States except as permitted by the laws and regulations of the United States, which may require U.S. Government export approval/licensing. Failure to strictly comply with this provision shall automatically invalidate this License.

License

SonicWALL grants you a non-exclusive license to use the SOFTWARE PRODUCT for a number of SonicWALL eligible products. This number is specified and shipped with the SOFTWARE PRODUCT. Support for additional SonicWALL eligible products is subject to a separate upgrade license.
Upgrades

If the SOFTWARE PRODUCT is labeled as an upgrade, you must be properly licensed to use a product identified by SonicWALL as being eligible for the upgrade in order to use the SOFTWARE PRODUCT. A SOFTWARE PRODUCT labeled as an upgrade replaces and/or supplements the product that formed the basis for your eligibility for the upgrade. You may use the resulting upgraded product only in accordance with the terms of this EULA. If the SOFTWARE PRODUCT is an upgrade of a component of a package of software programs that you licensed as a single product, the SOFTWARE PRODUCT may be used and transferred only as part of that single product package and may not be separated for use on more than one computer.

Support Services

SonicWALL may provide you with support services related to the SOFTWARE PRODUCT ("Support Services"). Use of Support Services is governed by the SonicWALL policies and programs described in the user manual, in “online” documentation, and/or in other SonicWALL-provided materials. Any supplemental software code provided to you as part of the Support Services shall be considered part of the SOFTWARE PRODUCT and subject to terms and conditions of this EULA. With respect to technical information you provide to SonicWALL as part of the Support Services, SonicWALL may use such information for its business purposes, including for product support and development. SonicWALL shall not utilize such technical information in a form that identifies its source.

Ownership

As between the parties, SonicWALL retains all title to, ownership of, and all proprietary rights with respect to the SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text, and ‘applets” incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT. The SOFTWARE PRODUCT is protected by copyrights laws and international treaty provisions. The SOFTWARE PRODUCT is licensed, not sold. This EULA does not convey to you an interest in or to the SOFTWARE PRODUCT, but only a limited right of use revocable in accordance with the terms of this EULA.

U.S. Government Restricted Rights

If you are acquiring the Software including accompanying documentation on behalf of the U.S. Government, the following provisions apply. If the Software is supplied to the Department of Defense (“DoD”), the Software is subject to “Restricted Rights”, as that term is defined in the DOD Supplement to the Federal Acquisition Regulations (“DFAR”) in paragraph 252.227 7013(c) (1). If the Software is supplied to any unit or agency of the United States Government other than DOD, the Government’s rights in the Software will be as defined in paragraph 52.227 19(c) (2) of the Federal Acquisition Regulations (“FAR”). Use, duplication, reproduction or disclosure by the Government is subject to such restrictions or successor provisions. Contractor/Manufacturer is: SonicWALL, Inc. 2001 Logic Drive, San Jose, CA 95124-3452, USA.
Exports License

Licensee will comply with, and will, at SonicWALL’s request, demonstrate such compliance with all applicable export laws, restrictions, and regulations of the U.S. Department of Commerce, the U.S. Department of Treasury and any other any U.S. or foreign agency or authority. Licensee will not export or re-export, or allow the export or re-export of any product, technology or information it obtains or learns pursuant to this Agreement (or any direct product thereof) in violation of any such law, restriction or regulation, including, without limitation, export or re-export to Cuba, Iran, Iraq, Libya, North Korea, Sudan, Syria or any other country subject to applicable U.S. trade embargoes or restrictions, or to any party on the U.S. Export Administration Table of Denial Orders or the U.S. Department of Treasury List of Specially Designated Nationals, or to any other prohibited destination or person pursuant to U.S. law, regulations or other provisions.

Miscellaneous

This EULA represents the entire agreement concerning the subject matter hereof between the parties and supercedes all prior agreements and representations between them. It may be amended only in writing executed by both parties. This EULA shall be governed by and construed under the laws of the State of California as if entirely performed within the State and without regard for conflicts of laws. Should any term of this EULA be declared void or unenforceable by any court of competent jurisdiction, such declaration shall have no effect on the remaining terms hereof. The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.

Termination

This EULA is effective upon your opening of the sealed package(s), installing or otherwise using the SOFTWARE PRODUCT, and shall continue until terminated. Without prejudice to any other rights, SonicWALL may terminate this EULA if you fail to comply with the terms and conditions of this EULA. SonicWALL reserves the right to terminate this EULA five (5) years after the SOFTWARE PRODUCT is issued to Licensee. In event of termination, you agree to return or destroy the SOFTWARE PRODUCT (including all related documents and components items as defined above) and any and all copies of same.

Limited Warranty

SonicWALL warrants that a) the software product will perform substantially in accordance with the accompanying written materials for a period of ninety (90) days from the date of purchase, and b) any support services provided by SonicWALL shall be substantially as described in applicable written materials provided to you by SonicWALL. Any implied warranties on the software product are limited to ninety (90) days. Some states and jurisdictions do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you.
Customer Remedies

SonicWALL's and its suppliers’ entire liability and your exclusive remedy shall be, at SonicWALL's option, either a) return of the price paid, or b) repair or replacement of the SOFTWARE PRODUCT that does not meet SonicWALL's Limited Warranty and which is returned to SonicWALL with a copy of your receipt. This Limited Warranty is void if failure of the SOFTWARE PRODUCT has resulted from accident, abuse, or misapplication. Any replacement SOFTWARE PRODUCT shall be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer. Outside of the United States, neither these remedies nor any product Support Services offered by SonicWALL are available without proof of purchase from an authorized SonicWALL international reseller or distributor.

No Other Warranties

To the maximum extent permitted by applicable law, SonicWALL and its suppliers/licensors disclaim all other warranties and conditions, either express or implied, including, but not limited to, implied warranties of merchantability, fitness for a particular purpose, title, and non-infringement, with regard to the SOFTWARE PRODUCT, and the provision of or failure to provide support services. This limited warranty gives you specific legal rights. You may have others, which vary from state/jurisdiction to state/jurisdiction.

Limitation of Liability

Except for the warranties provided hereunder, to the maximum extent permitted by applicable law, in no event shall SonicWALL or its suppliers/licensors be liable for any special, incidental, indirect, or consequential damages for lost business profits, business interruption, loss of business information,) arising out of the use of or inability to use the SOFTWARE PRODUCT or the provision of or failure to provide support services, even if SonicWALL has been advised of the possibility of such damages. In any case, SonicWALL's entire liability under any provision of this EULA shall be limited to the amount actually paid by you for the SOFTWARE PRODUCT; provided, however, if you have entered into a SonicWALL support services agreement, SonicWALL's entire liability regarding support services shall be governed by the terms of that agreement. Because some states and jurisdiction do not allow the exclusion or limitation of liability, the above limitation may not apply to you.

Manufacturer is SonicWALL, Inc. with headquarters located at 2001 Logic Drive, San Jose, CA 95124-3452, USA.

The SonicWALL GMS 6.0 documentation set includes the following user guides:

- SonicWALL GMS 6.0 Release Notes
- SonicWALL GMS 6.0 Getting Started Guide
- SonicWALL UMA EM5000 Getting Started Guide
- SonicWALL GMS 6.0 Administrator’s Guide

For basic and advanced deployment examples, refer to SonicWALL GMS user guides and deployment technotes.
SonicWALL Live Product Demos

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

- Unified Threat Management Platform
- Secure Cellular Wireless
- Continuous Data Protection
- SSL VPN Secure Remote Access
- Content Filtering
- Secure Wireless Solutions
- Email Security
- GMS and ViewPoint

For further information, visit: <http://livedemo.sonicwall.com/>