Software License Agreement for SonicWALL Global Management System

To review the SonicWALL Global Management System Software License Agreement, see the SonicWALL Global Management System Introduction Guide.
Chapter 1 Introduction 1
  Installing and Upgrading 1

Chapter 2 Installing SonicWALL GMS 3
  Installation Overview 4
    Database and Driver Requirements 4
    SGMS Gateway Requirements 4
    Windows 2000/XP/2003 Requirements 5
    Solaris Requirements 5
  Pre-Installation 7
    Oracle Database 7
    SQL Server 2000 Database 7
    Java Database Connectivity (JDBC) Driver 8
    Creating the sgmsadm User 8
  Console or Stand-Alone Installation 9
  Agent Installation 15
  Upgrading from a Previous SonicWALL GMS Version 20
  Installing a Distributed Reporting Server 23
  GMS Support for Proxy Servers 23
  Completing the Registration Page 24

Chapter 3 Registering SonicWALL GMS 27
  Logging In 28

Appendix A Configuring an Oracle Database 31
  Solaris 31
    Installing the Oracle Server on Solaris 31
    Starting Oracle 33
    Making Sure Oracle is Running 33
    Installing the Oracle Client on Solaris 34
  Windows 2000/XP/2003 35
    Installing the Oracle Server on Windows 2000/XP/2003 35
    Installing the Oracle Client on Windows 2000/XP/2003 37

Appendix B Easy Provisioning 39
  Pre-Configuration 39
  On-Site Configuration 39

Appendix C Miscellaneous Procedures and Troubleshooting Tips 41
  Miscellaneous Procedures 41
    Backing up SonicWALL GMS Data 41
    Changing the SQL Server Authentication Mode 41
    Reinstalling SonicWALL GMS Using an Existing Database 41
    Uninstalling SonicWALL GMS and its Database 42
  Troubleshooting Tips 43
    Phase 2 Installation Hangs 43
    Registration Fails 43
    Installing the Console in Redundancy Mode 43
No Agent functionality on the Console 44
Securing Access to the GMS Web Server 44
Changing the GMS Web Server Port Number 45
Changing a SonicWALL GMS Agent IP Address 46
Changing the Default Syslog Server Port Number 46
Introduction

This guide is designed to help you install the SonicWALL Global Management System (SonicWALL GMS). If you have not used SonicWALL GMS before, you might want to familiarize yourself with SonicWALL GMS concepts and features. For more information, see the SonicWALL Global Management System Introduction Guide.

After installing SonicWALL GMS, it must be properly configured. For more information, see the SonicWALL Global Management System Configuration Guide.

When you are ready to install SonicWALL GMS, perform the following tasks:

- Install SonicWALL GMS. See Chapter 2, “Installing SonicWALL GMS.”
- Register SonicWALL GMS. See Chapter 3, “Registering SonicWALL GMS.”

Installing and Upgrading

You can either perform a fresh installation of GMS 2.9.4 using the installer or upgrade a previous installation of GMS 2.9, patched or unpatched. In a distributed environment, make sure you stop all GMS services on all GMS servers before proceding to perform an upgrade.

If the GMS Console (Web server) is set up for HTTP management, the upgrade to GMS 2.9.4 will preserve the HTTPS settings for the GMS Web server.

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

This chapter describes how to install or upgrade SonicWALL Global Management System (SonicWALL GMS) in a distributed environment, or as a stand-alone SonicWALL GMS.

Note: For more information on distributed environments, see the SonicWALL Global Management System Introduction Guide.

To install or upgrade SonicWALL GMS, complete the following procedures:

• Review the installation requirements. See “Installation Overview” on page 4.
• Perform any pre-installation tasks. See “Pre-Installation” on page 7.
• Do one of the following:
  • To install SonicWALL GMS as a Console SonicWALL GMS in a distributed environment or as a stand-alone SonicWALL GMS, see “Console or Stand-Alone Installation” on page 9.
  • To install SonicWALL GMS as an Agent SonicWALL GMS in a distributed environment, see “Agent Installation” on page 15.
  • To upgrade SonicWALL GMS from Version 2.4, see “Upgrading from a Previous SonicWALL GMS Version” on page 20.
Installation Overview

The SonicWALL GMS Installation program is an HTML-launched installer that automatically detects whether you are installing on a Windows 2000/XP Professional/Server 2003 or Solaris server. After the installation program detects the operating system, the installation procedure is identical.

Before installing SonicWALL GMS, review the following requirements.

- Database and driver requirements—see “Database and Driver Requirements,” below.
- GMS gateway requirements—see “GMS Gateway Requirements,” below.
- Operating system requirements:
  - Solaris Requirements—see “Solaris Requirements” on page 5.

Database and Driver Requirements

To use SonicWALL GMS, you must have an Oracle 9.2.0.1 (Standard or Enterprise Editions on Windows) or Microsoft SQL Server 2000 SP3 database.

SonicWALL GMS also requires a Java Database Connectivity (JDBC) driver to access the database. Oracle 9.2.0.1 includes a JDBC driver. For Microsoft SQL Server 2000 database, SonicWALL GMS 2.9 installs or upgrades the i-net SPRINTA(tm) JDBC driver. This driver is from i-net software GmbH.

SonicWALL GMS 2.9 services use JRE 1.4.2_05. However, GMS 2.9 automatically downloads the Java Plug-in 1.4.1_05 when accessing GMS. SonicWALL GMS 2.9 also uses Tomcat 4.1.29 and installs SPRINTA(tm) JDBC driver version 6.03.

Note: A copy of the i-net SPRINTA(tm) JDBC driver is included on the SonicWALL GMS CD-ROM.

System

The SonicWALL GMS database server must meet the following minimum requirements:

- 750 MHz processor
- 512 MB RAM
- 80 GB of free disk space

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

GMS Gateway Requirements

To use SonicWALL GMS, an GMS gateway must reside between each SonicWALL GMS agent server and the SonicWALL appliances that it manages. The GMS gateway allows each SonicWALL GMS agent server to securely communicate with its managed devices over VPN tunnels. SonicWALL GMS can use two types of VPN tunnels to communicate with the managed devices:

- Management VPN tunnel—the security association (SA) for this type of VPN tunnel must be configured in the managed SonicWALL appliance. For more information, see Chapter 4 of the SonicWALL Global Management Configuration Guide.

  The security association (SA) must also be created in the GMS gateway when adding a SonicWALL appliance to SonicWALL GMS. For more information, see Chapter 2 of the SonicWALL Global Management Configuration Guide.

  For this configuration, the GMS gateway must be a SonicWALL VPN-based appliance. The GMS gateway can be configured in NAT-Enabled or Standard mode.

- Site-to-site VPN tunnel—SonicWALL GMS can use VPN tunnels that already exist in the network to communicate with the managed devices. For more information, see Chapter 4 of the SonicWALL Global Management Configuration Guide.

  For this configuration, the GMS gateway can be a SonicWALL VPN-based appliance or another VPN device that is interoperable with SonicWALL VPN.
Installing SonicWALL GMS involves several steps. To successfully install SonicWALL GMS, do the following:

- Review the database requirements.
- Review the GMS gateway requirements.
- Review the system and network requirements.
- Install SonicWALL GMS. See “Console or Stand-Alone Installation” on page 9 or “Agent Installation” on page 15.

**System**

In order to install and run SonicWALL GMS, you must be logged in as the administrator and the SonicWALL GMS server must meet the following requirements:

- Local and remote browser access: Microsoft Internet Explorer 6.x and Netscape 4.7.
- If using Oracle 9.2.0.1 as the database, the Oracle Client must be installed on each Windows-based SonicWALL GMS server. This installs the JDBC driver on the SonicWALL GMS server.
- If using Microsoft SQL Server 2000 SP3 as the database, SonicWALL GMS installs the i-net SPRINTA(tm) JDBC driver on each Windows-based SonicWALL GMS server.
- 1.2GHz processor.
- 1GB RAM of memory.
- 85MB available disk space.

**Network**

In order to install and run SonicWALL GMS, the following network requirements must be met:

- The SonicWALL GMS server must have direct 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 1 KB/s for each device under management. For example, if SonicWALL GMS is monitoring 100 SonicWALL appliances, the connection must support up to 100 KB/s.

*Note: 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 may vary.*

**Solaris Requirements**

To successfully install SonicWALL GMS for Solaris, do the following:

- Review the database requirements.
- Review the GMS gateway requirements.
- Review the system and network requirements below.
- Run the SonicWALL GMS installation wizard. See “Console or Stand-Alone Installation” on page 9 or “Agent Installation” on page 15.

**System**

In order to install and run SonicWALL GMS, you must be logged in as the sgmsadm user. For information on creating the sgmsadm user, see “Pre-Installation” on page 7. Additionally, you must meet the minimum standard requirements.
The SonicWALL GMS server must meet the following MINIMUM requirements:

- Solaris 8 (English Operating System) running on a SPARC hardware platform.
- Local browser access: Netscape Navigator 4.7.
- Remote browser access: Microsoft Internet Explorer 6.x and Netscape 4.7.
- If using Oracle 9.2.0.1 as the database, the Oracle Client must be installed on each Solaris-based SonicWALL GMS server. This installs the JDBC driver on the SonicWALL GMS server.
- If using Microsoft SQL Server 2000 as the database, SonicWALL GMS installs the i-net SPRINTA(tm) JDBC driver.
- 650MHz UltraSPARC Ii processor
- 1GB memory
- Two 40GB IDE drives

**Network**

In order to install and run SonicWALL GMS, the following network requirements must be met:

- The SonicWALL GMS server must have direct 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 1 KB/s for each device under management. For example, if SonicWALL GMS is monitoring 100 SonicWALL appliances, the connection must support up to 100 KB/s.

*Note: 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.*
Pre-Installation

Select from the following:

• For Oracle installations, see “Oracle Database” on page 7.
• For SQL Server installations, see “SQL Server 2000 Database” on page 7.
• To create the sgmsadm user on Solaris, see “Creating the sgmsadm User” on page 8.

Oracle Database

Before installing SonicWALL GMS using Oracle, you must install the Oracle Server and Oracle Client. To install the Oracle Server, see “Installing the Oracle Server on Solaris” on page 31 or “Installing the Oracle Server on Windows 2000/XP/2003” on page 35. To install the Oracle Client, see “Installing the Oracle Client on Solaris” on page 34 or “Installing the Oracle Client on Windows 2000/XP/2003” on page 37.

SQL Server 2000 Database

Before installing SonicWALL GMS using Microsoft SQL Server 2000, complete the following procedure:

1. Install Microsoft SQL Server 2000 on a server.
2. When prompted, select the “Create a new instance of SQL Server, or install Client Tools” option.
3. When prompted, select the “Server and Client Tools” option.
4. When prompted, select the “Typical” setup type.
6. Once the database is installed, click Start, point to Programs, point to Microsoft SQL Server, and click Enterprise Manager.
8. Create a SonicWALL GMS database user (for example, GMSUser).
   For this database user, select the SQL Server Authentication mode option and enter a password. Make sure to assign this user the Database Creators server role.
9. Exit from the SQL Server Enterprise Manager.
10. If you plan to install the SonicWALL GMS Console on the same server as Microsoft SQL Server 2000, skip to “Java Database Connectivity (JDBC) Driver” on page 8.

SQL Server 2000 Client Tools

If you plan to install the SonicWALL GMS Console on a different server than the Microsoft SQL Server 2000 database server, you must install the Microsoft SQL Server 2000 Client Tools on the SonicWALL GMS Console server. To do this, run the Microsoft SQL Server 2000 database installation again and do the following:

1. When prompted, select the “Create a new instance of SQL Server, or install Client Tools” option.
2. When prompted, select the “Client Tools Only” option.
3. When prompted, select all components.

Note: It is not necessary to install the SQL Server 2000 Client Tools on each SonicWALL GMS agent server.
Java Database Connectivity (JDBC) Driver

To install the JDBC driver on a SonicWALL GMS server, follow these steps:

1. If using Oracle 9.2.0.1 as the database, install Oracle Client on each SonicWALL GMS server.
2. If using Microsoft SQL Server 2000 as the database, SonicWALL GMS installs the i-net SPRINTA(tm) 2000 JDBC driver on each SonicWALL GMS server. It copies the JDBC driver jar file (Sprinta2000.jar) to 
   <gms_directory>\etc directory and configures the CLASSPATH on your SonicWALL GMS system.

Creating the sgmsadm User

In the Solaris environment, the sgmsadm user must install SonicWALL GMS. To create the sgmsadm user, follow these steps:

1. Log into the Solaris server as root.
2. Enter the following command:
   # ./admintool
   The Admintool starts.
3. From the Users Menu, select Edit and click Add. The Add User dialog box appears.
4. Enter the following information:
   • Enter sgmsadm in the User Name field.
   • For the User ID, accept the default value.
   • Enter 10 in the Primary Group field.
   • Enter any comments about this account in the Comments field (i.e., GMS Install Account).
   • From the Login Shell pull-down menu, choose Bourne.
   • From the Password pull-down menu, choose Cleared until first login.
   • Enter a path for this account's home directory in the Path field (i.e., /export/home/sgmsadm).
5. Click Apply.
6. Click OK.
7. Exit from the Admintool: Users menu.

You also need to create the empty files sgmsConfig.xml and sgmsConfigBkp.xml. To do this, login as root and follow these steps:

1. Change to the root directory by entering:
   # cd /
2. Create the files by entering:
   # touch sgmsConfig.xml sgmsConfigBkp.xml
3. Change the permissions of the files by entering:
   # chmod 666 sgmsConfig.xml sgmsConfigBkp.xml
Console or Stand-Alone Installation

SonicWALL GMS Installation is a two-phase installation: Phase 1 installs SonicWALL GMS, and Phase 2 sets up the SonicWALL GMS database, installs the SonicWALL GMS services, and installs the Sprinta(tm) 2000 JDBC driver for using MS SQL Server 2000. Before installing SonicWALL GMS, review the system and network requirements for the Phase 1 installation, and perform any required pre-installation tasks. When you are ready to install SonicWALL GMS, follow these steps:

1. Log on to the computer as sgmsadm (Solaris system) or administrator (Windows system).
2. Insert the SonicWALL GMS CD-ROM or locate the SonicWALL GMS install file.
   - If you are installing GMS on a Microsoft Windows platform using the SonicWALL GMS CD-ROM, the Introduction screen is displayed. (Figure 1).
   - If you are installing GMS on a Microsoft Windows platform from the download file, run sgms.exe. The Introduction screen is displayed (Figure 1).
   - If you are installing GMS on a Solaris platform, run sgms.bin. The Introduction screen is displayed (Figure 1).

   Figure 1: Introduction Screen

3. Click Next. The License Agreement screen appears (Figure 2).

   Figure 2: License Agreement Screen

4. Accept the license agreement terms and click Next. The InstallShield Wizard will guide you through the installation process.
4. Select from the following:
   - To accept the terms of the license agreement, select **I accept the terms of the License Agreement** and click **Next**. If there is any important installation information, the Important Database Information screen appears (Figure 3).
   - To not accept the terms, select **I do NOT accept the terms of the License Agreement** and click **Next**. The SonicWALL GMS installation program closes and the product will not install.

   **Figure 3: Important Database Information Screen**

5. Read the Important Database Information screen and click **Next**.
   The Choose Install Folder screen appears (Figure 4).

   **Figure 4: Choose Install Folder Screen**

6. To accept the default location, click **Next**. To select a different location, click **Choose** and select a folder. The GMS Installation Options screen appears (Figure 5).
7. Select **Install GMS Console System** and click **Next**.

The SonicWALL GMS Installation Options screen appears (Figure 6).

**Figure 6: SonicWALL GMS Installation Options Screen**

8. If this server will be configured as a Console that manages Agents, select the **Disable Agent Installation** check box. If this is a stand-alone installation, **do not** select the **Disable Agent Installation** check box.

Click **Next**. The SonicWALL GMS Settings screen appears (Figure 7).
Do the following:

- Enter the IP address or host name of the Simple Mail Transfer Protocol (SMTP) server in the **SMTP Server Address** field.
- Enter the number of the web server port in the **Web Server Port** field (default: 80).
- Enter the e-mail addresses of GMS administrators who will receive e-mail notifications from SonicWALL GMS.
- Enter the IP address of the GMS gateway between the SonicWALL GMS and the network.
- Enter the password of the GMS gateway.
- To configure the installation program to verify the settings on this page before continuing, select the **Validate fields on this screen** check box.

Click **Install**. The installation program begins copying SonicWALL GMS files (Figure 8).

**Figure 8: Installation Status Screen**

Phase 2 of the installation begins.
9. Click Next.

The Database Settings dialog box appears (Figure 10).

Figure 10: Database Settings Dialog Box

10. Do the following:

- Select the type of database from the Database Vendor list box.
- Enter the IP address or name of the database host in the Database Host/IP field.
- Accept the default value for JDBC driver.
  
  *Note: If you are using the Oracle thin driver, append the IP address and port. For example:*
  
  jdbc:oracle:thin:@ip_address:port

- Accept the default value for JDBC URL.
- For Oracle Installations, enter the SID in the TNS Name field.
- Enter the database username in the Database User field.
- Enter the database user password in the Database Password field.

Click OK. The post-installation procedure is complete.

*Note: The installation program will create a minimal GMS database. Depending on the number of devices that will be managed, you may have to use database tools such as Microsoft SQL Server Enterprise Manager to change the database sizes.*

11. Restart the server.
12. If this is a Windows-based Console server, ensure that the following SonicWALL GMS services have started:
   - GMS Scheduler
   - GMS ViewPoint Scheduler
   - GMS ViewPoint Summarizer
   - GMS Web Server
   - GMS SNMP Manager

   If this is a Solaris-based Console, ensure the following SonicWALL GMS daemons have started:
   - sgmsvp1.sh
   - sgmsvp2.sh
   - sgmssched.sh
   - tomcat.sh
   - sgmsnmpmgr.sh

   **Note:** In addition to verifying these services, ensure that the sgmsConfig.xml file is in the C:\ or root directory. On Solaris systems, also ensure that the sgmsConfigBkp.xml file is in the root directory.

After installing SonicWALL GMS, you must register the product with the SonicWALL registration site, Mysonicwall.com. For more information, see Chapter 3, “Registering SonicWALL GMS.”
Agent Installation

SonicWALL GMS Installation is a two-phase installation: Phase 1 installs SonicWALL GMS, and Phase 2 installs the GMS Scheduler service and the SPRINTA(tm) 2000 JDBC driver for MS SQL Server 2000. Before installing SonicWALL GMS, review the system and network requirements and perform any required pre-installation tasks.

When you are ready to install SonicWALL GMS, follow these steps for the Phase 1 installation:

1. Log on to the computer as sgmsadm (Solaris system) or administrator (Windows system).
2. Insert the SonicWALL GMS CD-ROM or locate the SonicWALL GMS install file.
   - If you are installing GMS on a Microsoft Windows platform using the SonicWALL GMS CD-ROM, the Introduction screen is displayed.
   - If you are installing GMS on a Microsoft Windows platform from the download file, run sgms.exe. The Introduction screen is displayed.
   - If you are installing GMS on a Solaris platform, run sgms.bin. The Introduction screen displays.
3. Click Next. The License Agreement screen appears (Figure 11).

   **Figure 11: License Agreement Screen**

4. Select from the following:
   - To accept the terms of the license agreement, select I accept the terms of the License Agreement and click Next. The Important Database Information screen appears (Figure 12).
   - To not accept the terms, select I do NOT accept the terms of the License Agreement and click Next. The SonicWALL GMS installation program closes and the product will not install.
5. Read the Important Database Information screen and click Next.
   The Choose Install Folder screen appears (Figure 13).

   **Figure 13: Choose Install Folder Screen**

6. To accept the default location, click Next. To select a different location, click Choose and locate a folder. The GMS Installation Options screen appears (Figure 14).

   **Figure 14: GMS Installation Options Screen**
7. Select **Install GMS Agent System** and click **Next**. The SonicWALL GMS Settings screen appears (Figure 15).

**Figure 15: SonicWALL GMS Settings Screen**

Do the following:

- Enter the IP address of the GMS gateway between the SonicWALL GMS and the network.
- Enter the password of the GMS gateway.
- To configure the installation program to verify the settings on this page before continuing, select the **Validate fields on this screen** check box.

Click **Install**. The installation program begins copying SonicWALL GMS files (Figure 16).
After the files are copied, the second phase of the installation begins.

Figure 17: Phase 2 Installer Launch Screen

8. Click **Next**.

The Database Settings dialog box appears (Figure 18).

Figure 18: Database Settings Dialog Box
9. Do the following:
   • Select the type of database from the Database Vendor list box.
   • Enter the IP address or name of the database host in the Database Host/IP field.
   • Accept the default value for JDBC driver.
     Note: If you are using the Oracle thin driver, append the IP address and port. For example: jdbc:oracle:thin:@ip_address:port
   • Accept the default value for JDBC URL.
   • For Oracle Installations, enter the SID in the TNS Name field.
   • Enter the database username in the Database User field.
   • Enter the database user password in the Database Password field.
   Click OK. The post-installation procedure is complete.

   Note: The installation program will create a minimal GMS database. Depending on the number of devices that will be managed, you may have to use database tools such as Microsoft SQL Server Enterprise Manager to change the database sizes.

10. Restart the server. Ensure that the GMS Scheduler, GMS SNMP Manager and GMS ViewPoint Summarizer services started on the Windows-based SonicWALL GMS Agent.
   The SonicWALL GMS daemons on a Solaris-based Agent are sgmsched.sh, sgmsvp2.sh, and sgmsnmpmgr.sh.
Upgrading from a Previous SonicWALL GMS Version

Upgrading SonicWALL GMS occurs in two phases. Phase 1 upgrades the SonicWALL GMS software and Phase 2 updates the SonicWALL GMS database.

**Note:** Refer to the release notes for the GMS version you are installing as an upgrade for specific installation notes or instructions.

**Warning:** Make sure to perform the upgrade procedure on the SonicWALL GMS Console and all Agent servers.

Before performing the SonicWALL GMS upgrade, be sure all the files in the SonicWALL GMS directory have read and write permissions.

To upgrade SonicWALL GMS, follow these steps:

1. Log on to the computer as sgmsadm (Solaris system) or administrator (Windows system).
2. Insert the SonicWALL GMS CD-ROM or locate the SonicWALL GMS install file.
   - If you are installing GMS on a Microsoft Windows platform using the SonicWALL GMS CD-ROM, the Introduction screen is displayed (Figure 19).
   - If you are installing GMS on a Microsoft Windows platform from the download file, run sgms.exe. The Introduction screen is displayed (Figure 19).
   - If you are installing GMS on a Solaris platform, run sgms.bin. The Introduction screen is displayed (Figure 19).

**Figure 19: Introduction Screen**

3. Click **Next**. The **License Agreement** screen appears (Figure 20).
4. Select from the following:
   • To accept the terms of the license agreement, select **I accept the terms of the License Agreement** and click **Next**. The SonicWALL GMS Upgrade screen appears (Figure 21).
   • If you do not accept the terms, select **I do NOT accept the terms of the License Agreement** and click **Next**. The SonicWALL GMS installation program closes and the product does not install.

   **Figure 21: SonicWALL GMS Upgrade Screen**

   Click **Install**. The installation program begins installing SonicWALL GMS (Figure 22).
Phase 2 of the installation begins.

Figure 22: Installation Status Screen

5. Click Next.
   The Database Settings dialog box appears (Figure 10).

Figure 23: Phase 2 Installer Launch Screen

Figure 24: Database Settings Dialog Box

6. Check the database settings and click OK. The post-installation procedure is complete.
7. Restart the server. Installation is complete.
8. Be sure that the following SonicWALL GMS services have started on the SonicWALL GMS Console (Windows system):

- GMS Scheduler
- GMS SNMP Manager
- GMS ViewPoint Scheduler
- GMS ViewPoint Summarizer
- GMS Web Server

The SonicWALL GMS daemons on a Solaris-based Console are sgmsched.sh, sgmsnmpmgr.sh, sgmsvp1.sh, sgmsvp2.sh, and tomcat.sh.

9. Be sure that the GMS Scheduler, GMS SNMP Manager, and GMS ViewPoint Summarizer services have started on the SonicWALL GMS Agent (Windows system).

The SonicWALL GMS daemons on a Solaris-based Agent are sgmsched.sh, sgmsnmpmgr.sh, and sgmsvp2.sh.

---

**Installing a Distributed Reporting Server**

When managing a large number of SonicWALL appliances, the reporting data that is sent from the SonicWALL appliances to SonicWALL GMS can become substantial. To reduce the load on SonicWALL GMS, you can install an extra server to handle the Reporting traffic.

*Note:* The Distributed Reporting feature only works for SonicWALL appliances that connect to SonicWALL GMS through HTTPS connections.

SonicWALL GMS supports two types of Distributed Reporting servers:

- Summarization only—the Agent servers collect syslog data and write them to a mapped drive located on the reporting server. This does not require any special configuration and works with all management modes (i.e., HTTPS, IPSec, existing tunnel).
- Summarization and Syslog Collection—the SonicWALL appliances are configured to send their syslog data directly to the Distributed Reporting server. This requires special configuration and only works with the HTTPS management mode.

To configure Summarization and Syslog Collection, follow these steps:

1. Obtain an appropriate server that meets the specifications in this installation guide.
2. Follow the steps in the *SonicWALL Global Management System Installation Guide* for a fully redundant agent installation.
3. SonicWALL GMS stores its configuration information in the sgmsConfig.xml file. Open the sgmsConfig.xml and adjust the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduler.terminate</td>
<td>true</td>
</tr>
<tr>
<td>snmpmgr.terminate</td>
<td>true</td>
</tr>
<tr>
<td>syslog.terminate</td>
<td>false</td>
</tr>
<tr>
<td>vpnscheduler.terminate</td>
<td>true</td>
</tr>
<tr>
<td>vpns summarizer.terminate</td>
<td>false</td>
</tr>
</tbody>
</table>

4. Save the file and exit.
5. Configure SonicWALL appliances to use HTTPS as the management method. For more information, refer to the *SonicWALL Global Management System Configuration Guide*.
6. To configure the SonicWALL GMS Agents to forward non-HTTPS reporting traffic to the Distributed Reporting server, Open the sgmsConfig.xml on each of the Agents and adjust the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>syslog.forwardToHost</td>
<td>IP address of Distributed Reporting server.</td>
</tr>
<tr>
<td>syslog.forwardToHostPort</td>
<td>Port for distributed reporting (default: 514).</td>
</tr>
</tbody>
</table>

7. Save the file and exit.

---

**GMS Support for Proxy Servers**

GMS is able to access the Internet using Proxy Servers for environments that do not have direct Internet access, and manage firewalls in the private Internet.
The following proxy tag entries are required:

```xml
<Parameter name="proxySet" value="1"/>
<Parameter name="proxyHost" value="10.0.30.62"/>
<Parameter name="proxyPort" value="3128"/>
<Parameter name="proxyUser" value="0A57CF01AB39ACF8863C8089321B9287"/>
<Parameter name="proxyPassword" value="EE80851182B4B962FC3E0EDF1F00275A"/>
```

*proxyUser* and *proxyPassword* are required only if the Proxy Server requires authentication, in which case these are TEAV encrypted as usual.

This supports both HTTP and HTTPS Proxy, as long as the settings are identical for both.

GMS provides a way to exempt certain Hosts in order to be connected directly instead of going through the Proxy Server.

The following tag needs to be added to sgmsConfig.xml. The value can be changed for your specific setup.

```xml
<Parameter name="nonProxyHosts" value="something.com|www.foo*|192.168.0.*"/>
```

* = Wildcard (any string)
| = Delimiter for the hosts in the list.

## Completing the Registration Page

After you complete one of the three update processes, the registration page will display. A sample registration page appears in the following figure.

**Figure 25: Registration Page**

An example of a filled-out registration page appears in the following figure.
Figure 26: Sample Filled-Out Registration Page
Registering SonicWALL GMS

The first time you start SonicWALL GMS, the Registration page will appear. To register SonicWALL GMS, follow these steps:

**Note:** SonicWALL GMS must be registered before you can use it. To complete registration, SonicWALL GMS must have direct access to the Internet.

1. Select from the following:
   - For Windows, double-click the GMS icon on your desktop.
   - For Solaris, open a browser and enter `http://localhost/sgms/login` or `http://localhost`.

   The SonicWALL GMS registration screen appears (Figure 27).

2. Enter your contact information in the appropriate fields.

3. Enter the SonicWALL GMS serial number in the **GMS Serial Number** field.

4. When you are finished, click **Update**.

   SonicWALL GMS will contact the SonicWALL registration site, Mysonicwall.com. After SonicWALL GMS is successfully registered, the Login page appears. For more information, see “Logging In” on page 28.

   **Note:** If registration fails, see Appendix C, “Miscellaneous Procedures and Troubleshooting Tips.” If the problem is not documented, contact SonicWALL technical support.
Logging In

To start SonicWALL GMS and log in, follow these steps:

1. Select from the following:
   - For Windows, double-click the GMS icon on your desktop. If you are logging in from a remote location, open a web browser and enter http://sgms_ipaddress/sgms/login or http://localhost.
   - For Solaris, open a browser and enter http://localhost/sgms/login. If you are logging in from a remote location, open a web browser and enter http://sgms_ipaddress/sgms/login or http://sgms_ipaddress.

The SonicWALL GMS login page appears (Figure 28).

Figure 28: SonicWALL GMS Login Page

2. Enter the SonicWALL user ID (default: admin) and password (default: password).

   Note: After the password is entered, an authenticated management session is established that times out after 5 minutes of inactivity. The default time-out can be changed from the General/User Settings page on the Console Panel.

   For the security purposes, it is highly recommended to change the default password for the user admin. The maximum size of the SonicWALL GMS User ID is 24 alphanumeric characters. If the password is more than 32 characters long, it will automatically be truncated.
3. Click **Submit**. The SonicWALL GMS UI opens (Figure 29).

**Figure 29: SonicWALL GMS UI**

For information on using the SonicWALL GMS UI, see the *SonicWALL Global Management System Configuration Guide*. 
Configuring an Oracle Database

This appendix describes how to install the Oracle 9.2.0.1 Server and the Oracle Client on a Solaris workstation or a Windows 2000/XP/2003 system.

For more information, see the Oracle website at http://docs.oracle.com/database_mp_9i.html.

Solaris

This section describes how to install the Oracle Server and the Oracle Client on a Solaris workstation. Select from the following:

- To install Oracle Server, see “Installing the Oracle Server on Solaris,” below.
- To install the Oracle Client, see “Installing the Oracle Client on Solaris” on page 34.

Installing the Oracle Server on Solaris

This section describes how to install the Oracle 9.2.0.1 Server on a Solaris workstation.

Pre-Installation

Before installing the Oracle 9.2.0.1 Server on a Solaris workstation, follow these steps:

1. Log in as root.
2. Open the /etc/system file with a text editor.
3. Change the SHMMAX kernel parameter to at least 4294967295:
   ```bash
   set shmsys:shminfo_shmmax=4294967295
   ```
4. Save and close the file.
5. Reboot the system.
7. Create the /space/u01 and /space/u02 directories by entering:
   ```bash
   # mkdir /space/u01
   # mkdir /space/u02
   ```
8. Ensure that the /space/u01 directory has approximately 820 MB.
9. Ensure that the /space/u01 directory has at least 410 MB and space to grow as the database size increases.
10. Create UNIX groups and users and the Oracle configuration directory with the following commands:
   ```bash
   groupadd dba
groupadd oinstall
   useradd -g oinstall -G dba -d /space/u01 -s /bin/sh oracle
   passwd oracle (set default password - e.g. oracle)
   mkdir /var/opt/oracle
   chown oracle /space/u01 /space/u02
   chgrp oinstall /space/u01 /space/u02
   ```
11. Log in as the Oracle user.
12. Edit or create the $HOME/.profile and add the following lines:

```
#!/bin/sh
ORA_HOME=/space/u01/app/oracle/product/9.0.1.1
ORA_OWNER=oracle
```

Note: Make sure ORACLE_BASE points to the Oracle home directory and ORACLE_HOME reflects the Oracle version that is installed.

13. Save and close the file.

14. Execute the new .profile.

```
. ~/.profile
```

### Installation

To install the Oracle 9.2.0.1 Server on a Solaris workstation, follow these steps:

1. Insert the Oracle Installation CD.
2. Log in as root.
3. Open a terminal window and enter the following command:

```
xhost +
```
4. Open another terminal window, switch to the Oracle user, and start the installation:

```
su - oracle
cd /cdrom/oracle9i
./runInstaller
```

The installation program starts.

5. Select the default choices, except for the following:
   - When prompted for the UNIX Group Name, enter oinstall.
   - When prompted for which product to install, select **Oracle9i Enterprise Edition**.
   - When prompted for an installation type, select the “typical” installation.
   - When prompted for the Global Database Name and SID, use your fully qualified machine name (e.g., solaris1.sonicwall.com). The SID will automatically default to your hostname (e.g., solaris1).
   - When prompted for the Directory for Database Files, enter the mount point that you created (e.g., /space/u02).

6. During installation, the installation program will prompt you to run a generated script as root. When this occurs, simply follow the on-screen instructions.

### Post-Installation

After installing the Oracle 9.2.0.1 Server, configure the Oracle server to automatically start during system boot:

1. Login as root.
2. Open the /var/opt/oracle/oratab file with a text editor.
3. Change the ending 'N' to 'Y' so the dbstart script will restart it.
4. Save and close the file.
5. Create the /etc/init.d/dbora file:

```
touch /etc/init.d/dbora
```
6. Open the /etc/init.d/dbora with a text editor and add the following:

```
#!/bin/sh
ORA_HOME=/space/u01/app/oracle/product/9.0.1.1
ORA_OWNER=oracle
if [ ! -f $ORA_HOME/bin/dbstart ]; then
  echo "Oracle startup: cannot find start script"
```
exit
fi

case "$1" in
'start')
su - $ORA_OWNER -c $ORA_HOME/bin/dbstart &
su - $ORA_OWNER -c "lsnrctl start"
&
';
'stop')
su - $ORA_OWNER -c $ORA_HOME/bin/dbshut &
&
esac

Note: Make sure ORA_HOME points to the Oracle home directory and reflects the Oracle version that is installed.

7. Link the newly created script into startup sequence using the following commands:

```bash
ln -s /etc/init.d/dbora /etc/rc0.d/K10dbora
ln -s /etc/init.d/dbora /etc/rc2.d/S99dbora
```

8. The dbstart script has some awk code that does not identify the Oracle version correctly. Change to the directory where dbstart is located:

```bash
cd /ORACLE_HOME/app/oracle/product/9.0.1.1/bin/
```

9. Enter the following command:

```bash
$ diff -c dbstart.save dbstart
```

10. Open the dbstart file with a text editor and add the two lines as shown in the following “diff -c” report:

```bash
$ diff -c dbstart.save dbstart
```

```bash
*** dbstart.save Tue Jan 30 17:32:26 2001
--- dbstart Tue Jan 30 17:40:30 2001
***************
*** 69,73 ****
--- 69,75 ----
fi
STATUS=1
+ # awk script above is not working right, so hard-coding VERSION
+ VERSION=9.1
  if [ "$VERSION" = "9.1" ]
  then
```

11. Save and close the file.

12. Make sure you are logged in as root and open /etc/services file with a text editor.

13. Add the Oracle Server listener to the file by adding the following:

```bash
listener 1521/tcp # Net8 listener
```

14. Save and close the file.

Starting Oracle

After you have completed all installation steps, do the following:

- Start Oracle by entering the following command:

  ```bash
dbstart
  ```

- Start the TNS listener by entering the following command:

  ```bash
  lsnrctl start
  ```

Making Sure Oracle is Running

After you have started Oracle, make sure it is running by doing the following:

- Test Oracle by entering the following command:

  ```bash
  ps -ef | grep ora_
  ```

- Test the TNS listener by entering the following command:

  ```bash
  ps -ef | tns
  ```
Installing the Oracle Client on Solaris

To install the Oracle Client, simply load the CD-ROM and follow the on-screen instructions. However, make sure to select the following:

- Make sure to select the **Administration** option. This will allow you to add tables and perform other tasks without having to go to the Oracle Server.
- Make sure to use the default port (1521).

After installing the Oracle Client, follow these steps:

1. Log in as the Oracle user.
2. Modify the $ORACLE_HOME/dbs/<instancename>.ora file to increase the levels to a MEDIUM size database. Use init.ora as an example that also contains all information about each variable.
3. Configure the following in the .profile for the user who will install SonicWALL GMS:
   ```
   ORACLE_HOME
   ORACLE_SID
   LD_LIBRARY_PATH=$ORACLE_HOME/lib:
   CLASSPATH=$ORACLE_HOME/jdbc/lib/classes12.zip: $ORACLE_HOME/jdbc/lib/nls_charset12.zip:
   ```
4. Set the number of open cursors to at least 200.
Windows 2000/XP/2003

This section describes how to install the Oracle Server and the Oracle Client on a Windows XP/2000/2003 system. Select from the following:

- To install the Oracle Client, see “Installing the Oracle Client on Windows 2000/XP/2003” on page 37.

Installing the Oracle Server on Windows 2000/XP/2003

To install Oracle Server, follow these steps:

1. Load the CD-ROM and follow the on-screen instructions for a Typical Installation.
2. When prompted, it is recommended to select c:\Oracle\Ora91 as the installation directory.
3. When prompted, do the following:
   - Global Database Name—enter `sgmsdb.company.com` where `company` is the name of your organization.
   - SID—ensure that `sgmsdb` is entered in the SID field.
4. When you are finished, click **Install**.

Oracle 8.1 begins installing. At the end of the installation, a dialog box appears that contains information about the installation (Figure 30). This information includes database settings, user account names, and passwords.

**Figure 30: Oracle Database Configuration Assistant Alert Dialog Box**

5. Write down the information. When you are finished, click **OK**.
6. Click **Start**, point to **Programs**, point to **Oracle**, point to **Application Development**, and click **SQL Plus**. The Log On dialog box appears (Figure 31).

**Figure 31: Logon Dialog Box**

7. Enter “SYSTEM” in the **User Name** field, “manager” in the **Password** field, and “sgmsdb” in the **Host String** field. SQL Plus opens (Figure 32).
8. Create a SonicWALL GMS user by entering the following command:

   create user username identified by password;
   commit;

   For example, to create the user “sgms” with the password “sgms,” enter the following:

   create user sgms identified by sgms;
   commit;

9. Give the SonicWALL GMS user connect, resource, and database administrator (DBA) access by entering the following:

   grant CONNECT, RESOURCE, DBA to username;
   commit;

   For example, to grant access to the user “sgms”, enter the following:

   grant CONNECT, RESOURCE, DBA to sgms;
   commit;

10. Exit SQL Plus.

11. Open the init.ora file with a text editor. If you selected the recommended installation directory, the file will be located in the \C:\Oracle\ADMIN\sgmsdb\pfidle directory.

12. Locate the db_files parameter and change its value to 1500. For example:

   db_files=1500

13. Locate the db_file_multiblock_read_count parameter and change its value to 32. For example:

   db_file_multiblock_read_count=32

14. Save the changes and close the file.

15. Click Start, point to Settings, point to Control Panel, and click System. The System Properties page appears (Figure 33).
16. Click the **Advanced** tab. The Advanced page appears.
17. Click **Environmental Variables**. The Environmental Variables page appears.
18. Double-click the CLASSPATH variable. If the variable does not exist, click **New**. The Edit System Variable or the New System Variable dialog box appears (Figure 34).

**Figure 34: Edit System Variable Dialog Box**

19. Append the following to the Variable Value:
   
   C:\Oracle\Ora81\jdbc\lib\classes12.zip; C:\Oracle\Ora81\jdbc\lib\nls_charset12.zip;

   *Note: Do not delete any other entries in the Variable Value field.*

20. Click **OK**.
21. Reboot the system. Oracle is installed and configured.

### Installing the Oracle Client on Windows 2000/XP/2003

To install the Oracle Client, simply load the CD-ROM and follow the on-screen instructions. However, make sure to select the following:

- To add tables and perform other tasks without having to go to the Oracle Server, make sure to select the **Administration** option.
- Make sure to use the default port (1521).

To use the administration tool, click **Start**, point to **Programs**, point to **Oracle for Windows NT**, point to **Database Administration**, and select **DBA Studio**. The username is **SYSTEM** and the password is **manager**.

To test queries on your databases, click **Start**, point to **Programs**, point to **Oracle for Windows NT**, point to **Application Development**, and click **SQL Plus**. You can use **scott** as the username and **tiger** as the password (defaults shipped with system samples) and the hostname where the Oracle Server is located as the Hostname. To see if everything is working properly, select * from depts as the sample query.

*Note: After installing Oracle Client or other tools that include their own JRE, the registry is sometimes updated with that JRE information. Subsequent attempts to use javac, start TomCat, or other applications or utilities might...*
result in error messages about version number mismatches in the registry. Reinstalling the JRE 1.3 should fix these problems.

After installing the Oracle Client, follow these steps:

1. Log in as the Oracle user.

2. Modify the `$ORACLE_HOME/dbs/<instancename>.ora` file to increase the levels to a MEDIUM size database. Use `init.ora` as an example that also contains all information about each variable.

3. Configure the following for the user that will install SonicWALL GMS:
   
   ```
   ORACLE_HOME
   ORACLE_SID
   LD_LIBRARY_PATH=$ORACLE_HOME/lib:
   CLASSPATH=$ORACLE_HOME/jdbc/lib/classes12.zip: $ORACLE_HOME/jdbc/lib/nls_charset12.zip:
   ```

4. Set the number of open cursors to at least 200.
Easy Provisioning

To simplify deployment of SonicWALL appliances for ISPs and other service providers, SonicWALL recommends two Easy Provisioning methods. These include:

- Pre-Configuration
- On-Site Configuration

Pre-Configuration

In this configuration, the SonicWALL appliance is configured by the ISP before shipment to the customer. The customer simply unpacks and connects the firewall.

Figure 35: Pre-Configuration

On-Site Configuration

In this configuration, the parameters for the SonicWALL appliance are configured using the SonicWALL Provisioning Tool. The firewall is shipped to the customer and the configuration file is applied by the customer or a field service technician.
This configuration method only requires the SonicWALL appliance to be unpacked once.
Miscellaneous Procedures and Troubleshooting Tips

This chapter contains miscellaneous SonicWALL Global Management System (SonicWALL GMS) procedures and troubleshooting tips.

Miscellaneous Procedures

This section contains information on procedures that you may need to perform. Select from the following:

- It is highly recommended that you regularly back up the SonicWALL GMS data. For more information, see “Backing up SonicWALL GMS Data” on page 41.
- SonicWALL GMS requires Mixed Mode authentication when using SQL Server 2000. To change the authentication mode, see “Changing the SQL Server Authentication Mode” on page 41.
- If you are reinstalling SonicWALL GMS, preserving the previous configuration settings can save a lot of time. To reinstall SonicWALL GMS using an existing SonicWALL GMS database, see “Reinstalling SonicWALL GMS Using an Existing Database” on page 41.
- If you need to uninstall SonicWALL GMS from a server, it is important to do it correctly. To uninstall SonicWALL GMS, see “Uninstalling SonicWALL GMS and its Database” on page 42.

Backing up SonicWALL GMS Data

SonicWALL GMS stores its configuration data in the GMS database, SGMSDB. It is important to back up this database and the individual ViewPoint databases (sgmsvp_yyyy_mm_dd) on a regular basis.

This can be accomplished by backing up the entire Oracle or MS SQL Server 2000 using the database backup tool. When using this tool, there is no need to stop the SonicWALL GMS services for database backup. However, make sure that the backup occurs when SonicWALL GMS activity is the lowest and that the backup operation schedule does not clash with the SonicWALL GMS scheduler.

Note: It is also recommended to regularly back up the entire contents of the SonicWALL GMS directory, the sgmsConfig.xml file, and the sgmsConfigBkp.xml file (Solaris only).

Changing the SQL Server Authentication Mode

SonicWALL GMS requires the Mixed Mode authentication mode. To change the authentication mode from Windows Mode to Mixed Mode, follow these steps:

1. Start the Microsoft SQL Server Enterprise Manager.
2. Right-click the appropriate SQL Server Group and select Properties from the pop-up menu.
3. Click the Security tab.
4. Change the Authentication mode from Windows only to SQL Server and Windows.
5. Click OK.

Reinstalling SonicWALL GMS Using an Existing Database

If you need to reinstall SonicWALL GMS, but want to preserve the settings in an existing SonicWALL GMS database, follow these steps:
1. Install a new database, using the same username and password that you used for the existing SonicWALL GMS database.
2. Install SonicWALL GMS using this new database. For more information, see Chapter 2, “Installing SonicWALL GMS.”
3. Stop all SonicWALL GMS services.
4. Open the sgmsConfig.xml and web.xml files with a text editor. Change the values for the dbhost and dburl parameters to match the existing SonicWALL GMS database.
5. Restart the SonicWALL GMS services.
6. Uninstall the new database.

Uninstalling SonicWALL GMS and its Database

This section describes how to uninstall SonicWALL GMS and its components. Select from the following:
- To uninstall SonicWALL GMS on the Windows platform, see “Windows” on page 42.
- To uninstall SonicWALL GMS on the Solaris platform, see “Solaris” on page 42.
- To uninstall SonicWALL GMS databases from Microsoft SQL Server 2000, see “MS SQL Server 2000” on page 43.
- To uninstall SonicWALL GMS databases from Oracle, see “Oracle” on page 43.

Windows

To uninstall SonicWALL GMS from a Windows system, follow these steps:
1. Click Start, point to Settings, and click Control Panel.
2. Double-click Add/Remove Programs. The Add/Remove Programs Properties window appears (Figure 37).

   ![Figure 37: Add/Remove Programs Properties](image)

4. Follow the on-screen prompts.
5. Restart the system. SonicWALL GMS is uninstalled.

Solaris

To uninstall SonicWALL GMS from a Solaris system, follow these steps:
1. Change to the `<gms_directory>/UninstallerData` directory.
2. Enter the following command:
   Uninstaller_SGMS
3. Follow the on-screen prompts to remove SonicWALL GMS.
4. Restart the system. SonicWALL GMS is uninstalled.

**MS SQL Server 2000**

To uninstall or remove the SonicWALL GMS databases in the MS SQL Server 2000, you can execute the following DOS command from any SonicWALL GMS server:

```
osql -U username -P password -S dbHost_IP -q "drop database SGMSDB"
osql -U username -P password -S dbHost_IP -q "drop database sgmsvp_yyyy_mm_dd"
```

Or you can use the MS SQL Server's Enterprise Manager and delete the SGMSDB and sgmsvp_ databases.

**Oracle**

To uninstall or remove the SonicWALL GMS databases in the Oracle, use the Oracle Database Configuration Assistant. Once the databases are removed, the associated services will also be removed. You can also do the following:

1. Log into sqlplus as SYSTEM/_MANAGER (password ‘manager’ is the default provided at the time of server install).
2. Execute the following commands:
   ```
drop user sgms cascade; /* Deletes the user sgms */
cREATE USER sgms IDENTIFIED BY sgms; /* Creates a user sgms with password sgms */
grant CONNECT, RESOURCE, DBA to sgms; /* Grants rights to the user sgms */
SELECT username FROM all_users WHERE username LIKE 'SGMSVP_%'; /* Retrieves a list of VP databases */
drop user SGMSVP_2001_11_15; /* Repeat this for the usernames that the step iv displays */
exit;
```

**Troubleshooting Tips**

This section contains SonicWALL GMS troubleshooting tips.

**Phase 2 Installation Hangs**

**Problem:** Phase 2 installation hangs on the SonicWALL GMS Console. During the Phase 2 installation, SonicWALL GMS connects to the SQL 2000 database server and creates the SGMSDB, but then hangs on sgms_sessions.sql.

**Solution:** Install Microsoft SQL Server 2000 Client Tools on the SonicWALL GMS Console system.

**Registration Fails**

**Problem:** Registration of SonicWALL GMS, activation of SonicWALL GMS node license upgrades, or activation of SonicWALL GMS service contact fails with the following error message:

“Upgrade failed: Error During Impersonation of user”.

**Cause:** The password for the SonicWALL GMS account on mysonicwall.com (as mysonicwall thinks it is) does not match the password in the SGMSDB database.

**Solution:** Edit the SonicWALL GMS account on mysonicwall.com to use the password from SGMSDB database.

**Installing the Console in Redundancy Mode**

To configure the SonicWALL GMS Console in redundancy mode, follow these steps:

1. Complete Phase 1 & Phase 2 installations on the first SonicWALL GMS Console.
2. Complete Phase 1 & Phase 2 installations on the second SonicWALL GMS Console.
3. Register SonicWALL GMS from the first SonicWALL GMS Console.
4. Copy the sgms.o file to the second SonicWALL GMS Console.
No Agent functionality on the Console

If during the installation, you have selected not to install the Agent functionality on the GMS Console, you can do the following to retrieve the Agent functionality after installation:

1. Go to the `<gms_directory>\Temp` folder.
2. Open the file `shedInstall.bat` with a text editor.
3. Remove “REM” from the file.
4. Save the file and exit.
5. Execute the batch file.
   
   The GMS Scheduler service starts installing.
6. Start the GMS Scheduler service.

Securing Access to the GMS Web Server

This section describes how to configure SonicWALL GMS to run using HTTPS.

Creating a Keystore with a Valid Test Certificate

To configure SonicWALL GMS to use HTTPS, you must create a keystore with a valid test certificate. To do this, follow these steps:

1. From the command-line on the SonicWALL GMS Console, change to the following directory:
   
   `gms_directory\jre\bin`

   where `gms_directory` is the directory where SonicWALL GMS was installed.

2. Enter the following command:
   
   `.\keytool -genkey -alias spcert -keyalg RSA -keystore gms_directory\etc\keystore`

3. You are prompted to enter the keystore password and other information.

4. When prompted to confirm the information, type `yes` and press Enter.

5. Enter key password for `<spcert>`. If the password is the same as the keystore password, hit Enter.
   
   The certificate is issued for evaluation and testing purposes. To create a secure website using this certificate, see “Creating a Secure Website” on page 44. To use HTTPS with a valid certificate, you will need to obtain a certificate through a valid certificate authority (e.g., Verisign and Thawte) and store the certificate in the keystore that you just created.

   Note: For information on getting a certificate from Thawte, visit http://www.orionserver.com/docs/ssl-howto.html.

Creating a Secure Website

This section describes how to create a secure website with server side authentication. To do this, follow these steps:

1. Open the `<gms_directory>\jre\lib\security\java.security` file with a text editor.

2. Locate the following entry:

   `provider.2`

3. Replace it with the following:

   `provider.3`

4. Insert the following line above the line that you just edited:

   `security.provider.2=com.sun.net.ssl.internal.ssl.Provider`

5. Save the file and exit.

6. Open the `<gms_directory>\Tomcat\conf\server.xml` file with a text editor.

7. Locate the following entry:

   `</Connector>`

   `<Connector className="org.apache.tomcat.service.PoolTcpConnector">
   <Parameter name="handler" value="org.apache.tomcat.service.http.HttpConnectionHandler"/>
   <Parameter name="port"
8. Remove the comment characters (<!--, -->).

9. Change the port value from 8443 to 443.

10. Enter the following lines below the port entry:

   ```
   <Parameter name="keypass" value="keystore_password"/>
   <Parameter name="keystore" value="gms_directory\etc\keystore"/>
   </Connector>
   ```

   where keystore_password is the keystore password that you entered when creating the certificate and gms_directory is the directory where SonicWALL GMS was installed.

   The following is an example of a modified server.xml entry:

   ```
   <Connector className="org.apache.tomcat.service.PoolTcpConnector">
     <Parameter name="handler" value="org.apache.tomcat.service.http.HttpConnectionHandler"/>
     <Parameter name="port" value="443"/>
     <Parameter name="keypass" value="sgms11"/>
     <Parameter name="keystore" value="D:\SGMS2\etc\keystore"/>
     <Parameter name="clientAuth" value="false"/>
     </Connector>
   ```

11. To disallow normal HTTP traffic, locate and comment out the following section:

   ```
   <!-- Normal HTTP -->
   </Connector>
   ```

   When you are finished, it should look like the following:

   ```
   <!-- Normal HTTP -->
   <!--
   <Connector className="org.apache.tomcat.service.PoolTcpConnector">
     <Parameter name="handler" value="org.apache.tomcat.service.http.HttpConnectionHandler"/>
     <Parameter name="port" value="80"/>
   </Connector>
   -->
   ```

12. Save the file and exit.

13. Restart the GMS Web Server service.

Securely Accessing SonicWALL GMS

To securely access SonicWALL GMS, open a web browser and enter **https://sgms_address** where sgms_address is the address of the SonicWALL GMS server.

If you are using a Windows server, modify the desktop shortcut. Make sure it points to **https://localhost**.

Changing the GMS Web Server Port Number

During installation, you can specify a different port number for the GMS Web Server. After installation, follow these steps:

1. Open the following file:
2. Locate the following line:
   Parameter name="port" value="80"
3. Change the default value of 80 to another port number:
4. Save the file and exit.

Changing a SonicWALL GMS Agent IP Address

If you have changed the IP address of the SonicWALL GMS Agent, follow these steps:
1. Stop all SonicWALL GMS services.
2. Change the “GMS Scheduler” service status to manual mode (Windows only).
3. If you are using MS SQL Server, execute the following SQL commands from a DOS window:
   osql -U <userid> -P <password> -Q "update sgmsdb.dbo.schedulers set ipAddress = 'new ip' where ipAddress = 'old ip'"
4. If you are using Oracle, execute the following SQL commands as root:
   sqlplus <userid>/<password>@<sid>
   update schedulers set ipAddress = 'new ip' where ipAddress = 'old ip';
   commit;
5. Change the “GMS Scheduler” service status to Automatic mode (Windows only).
6. Restart all SonicWALL GMS services.

Changing the Default Syslog Server Port Number

By default, the SonicWALL GMS syslog server default port number is 514 on Windows systems. To change the port number, follow these steps:
1. Open the sgmsConfig.xml file with a text editor.
2. Add the following line to the end of the file before the </Configuration> section:
   Parameter name="syslog.syslogServerPort" value="port_number"
   where port_number is the new port number.
3. Save the file and exit.

By default, the SonicWALL GMS' syslog server default port number is 3003 on Solaris systems. To change the port number, follow these steps:
1. Open the sgmsConfig.xml file with a text editor.
2. Locate the following parameter:
   syslog.syslogServerPort" value="3003"
3. Change the syslog server port value to another number.
4. Save the file and exit.