SonicWALL Global Management System Introduction Guide

Standard Edition

Version 2.9.4

Copyright Information

Software License Agreement for SonicWALL Global Management System

Software License Agreement

This Software License Agreement (SLA) 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 SLA. If you do not agree to the terms of this SLA, 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 SLA 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 SLA.

- The SOFTWARE PRODUCT is licensed as a single product.
- 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 SLA.
- 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 Internet Security Appliances. This number is specified and shipped with the SOFTWARE PRODUCT. Support for additional SonicWALL Internet Security Appliances is subject to a separate upgrade license.

OEM - If the SOFTWARE PRODUCT is modified and enhanced for a SonicWALL OEM partner, you must adhere to the software license agreement of the SonicWALL OEM partner.

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 SLA. 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.

Distribution Rights To i-net Sprinta^{TM} 2000 Driver

To i-net SPRINTA 2000 DRIVER - SonicWALL has been given a non-exclusive, worldwide license by i-net software GmbH to distribute directly and indirectly (through SonicWALL's distribution channels) the i-net SPRINTA 2000 driver to SonicWALL's end user customers to use the driver with SonicWALL ViewPoint. SonicWALL's end user customers may make a copy of the driver for backup or archival purposes only. SonicWALL's end user customers are not allowed to make other copies, transfer, re-distribute, use, translate, or reverse assemble/compile the driver with any other non-SonicWALL applications. i-net software GmbH holds copyright and title to the i-net SPRINTA 2000 Driver.

To Microsoft's SQL Server Developer's Edition (MSDE) - This software incorporates Microsoft's SQL Server Developer's Edition (MSDE) and your use is subject to the terms and conditions of Microsoft's MSDE End-User License Agreement (a copy of which is available on Microsoft's website: <http://www.microsoft.com/sql/howto-buy/deveula.asp>).

To Quest Software's (formerly Sitraka) JClass ServerChart - This software incorporates Quest Software's (formerly Sitraka) JClass ServerChart and your use is subject to the terms and conditions of Quest's Jclass License Agreement (a copy of which is available on Quest's website: <http://java.quest.com/jclass/licensing.shtml>).

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 SLA. 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 SLA 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 SLA.

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. 1160 Bordeaux Drive, Sunnyvale, California 94089.

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 SLA represents the entire agreement concerning the subject matter hereof between the parties and supersedes all prior agreements and representations between them. It may be amended only in writing executed by both parties. This SLA 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 SLA 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 SLA 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 SLA if you fail to comply with the terms and conditions of this SLA. In such event, 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 SLA 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 1143 Borregas Avenue, Sunnyvale, CA 94089, USA.

Introducing SonicWALL GMS

The SonicWALL Global Management System (SonicWALL GMS) is a browser-based application that can config-ure and manage thousands of SonicWALL Internet security appliances from a central location.

SonicWALL GMS is capable of managing large networks that use SonicWALL appliances. This dramatically low-ers the cost of managing a secure distributed network. SonicWALL GMS does this by enabling administrators to monitor the status of and apply configurations to all managed SonicWALL appliances, groups of SonicWALL appliances, or individual SonicWALL appliances.

You can also configure multiple site VPNs for SonicWALL appliances. From the SonicWALL GMS user interface (UI), you can add VPN licenses to SonicWALL appliances, configure VPN settings, and enable or disable remote-client access for each network.

SonicWALL GMS provides monitoring features that enable you to view the current status of SonicWALL appli-ances, pending tasks, and log messages. It also provides graphical reporting of firewall and network activities for the SonicWALL appliances. A wide range of informative real-time and historical reports can be generated to pro-vide insight into usage trends and security events.

SonicWALL GMS Applications

SonicWALL GMS is designed to be used within any organization that needs to centrally manage and configure multiple SonicWALL appliances. Some of the major uses for SonicWALL GMS include:

- Remote site management for distributed organizations—enables medium- to large-sized enterprises with multi-ple sites to centrally administer Internet security policies.
- Managed security services for system integrators—enables system integrators to offer turnkey managed secu-rity services to small- to medium-sized enterprises (SMEs).
- Managed security services for service providers—enables service providers to offer managed security services to SMEs.

New Features and Enhancements

SonicWALL GMS 2.8 offers the following new features:

Reporting

- Customized preferences for viewing Reports on a per user basis, instead of a global setting. This includes the number of top sites to view, chart types, and so on.
- Support for URL-based reporting for web usage and web filtering. This feature allows SonicWALL GMS users to view usage based on web sites, rather than user IDs or IP addresses.
- FTP Reports show more detail. For example, the Top Users report now shows the top sites the user accessed.
- Attack Reports show more detail. For example, each attack shows the IP addresses from which the attacks originated.
- IPS Reports show more detail. This includes each kind of intrusion, the source of intrusion, and more.
- Emailed reports can be filtered by IP addresses or users, enabling SonicWALL GMS to monitor the activity of a specific user or a system.
- In addition to weekly and monthly reports, Over Time reports can now report a specific number of days.
- Emailed Reports can now be sent as an attachment or inline text.
- Granular VPN usage reporting enables SonicWALL GMS users to view reports based on VPN SA Policies and service usage.
- New status reports show the percentage of time each firewall was up and functional.
- Improved report generation performance.
- CLI support for all new reports.
- Configurable maintenance window for Gen 2 summarizer to allow for database maintenance and other operations when GMS is not summarizing.
- Scheduled Reports can now be uniquely named to differentiate reports.

Monitoring and Management

- New Monitoring Tool monitors the state of firewalls, network appliances, servers, desktops and applications, using various probes such as ping, TCP, HTTP, HTTPS, etc. Enables custom control of alert notifications, probe frequencies, categories, priorities, and more
- Syslog Tail tool filters syslog packets received by GMS Agents, providing real time web-access to incoming syslog packets.
- Granular control of certain event notifications. Events notifications can include emails to GMS Administrators, email to firewall owners, SNMP traps, GMS Console Logging, or File Logging.
- New event notification when a unit fails over or recovers in a high availability pair.
- New event notification when an SP unit fails over to or from dial-up.

GMS Management

- Support for firmware upgrade of firewalls from firmware files.
- Support for management of GSC policies through SonicWALL GMS UI.
- Support for VPN Client License Sharing through SonicWALL GMS.
- License activation codes can be applied from the Policy Panel screens in addition to the license pool mechanism.
- Bold New Graphics (BNG) added to SonicWALL GMS user interface.
- Simplified installation—Phase 2 of the installation is automatically launched from Phase 1.
- SonicWALL GMS Table Audit Trailing support—SonicWALL GMS users can view when any row of GMS database tables are updated or inserted.
- New model code support—SonicWALL GMS periodically checks the mySonicWALL.com website for new SonicWALL appliance model codes without requiring patches.
- Ravlin device management no longer supported.
- Improved troubleshooting—firewall management IP is now exposed in the GMS UI.
- Improved granular control of debug log settings.
- GMS logs can be exported in HTML format.
- Support for firmware upgrade and registration of HA backup units through SonicWALL GMS.

Features

SonicWALL GMS offers the following features:

- Policy-Based Management

  SonicWALL GMS enables network administrators to globally define, distribute, enforce and deploy network security policies for managed SonicWALL appliances, creating a highly secure and controllable firewall configuration environment.

- Managed VPN Services

  SonicWALL GMS simplifies the task of globally defining, distributing, enforcing and deploying VPN policies for managed VPN gateways, making it easy to manage a global VPN network.

- Managed Remote VPN Client Connections

  SonicWALL GMS allows administrators to define user policies for remote Global VPN Client users. The user policies can either be emailed to remote users or directly downloaded from the SonicWALL VPN gateways.

- Comprehensive Security Service Management

  In addition to managing security and VPN policies, SonicWALL GMS enables network administrators to globally define, distribute, enforce and deploy all the firewall settings for managed SonicWALL appliances. It also enables network administrators to remotely upgrade SonicWALL appliances and add subscription services such as content filtering and virus scanning.

- License Management

  SonicWALL GMS provides centralized license management of SonicWALL upgrade and subscription services. This makes it easy to store, apply, track, and update upgrade and subscription license information for all managed SonicWALL appliances.

- Multi-Tier Policy Hierarchy Architecture

  SonicWALL GMS enables administrators to define and distribute one or more policies to an individual or a group of managed SonicWALL appliances. The policies can be executed immediately or can be scheduled to run at a later time. SonicWALL GMS supports up to seven levels of groups. Policies can be applied at any level.

- Scalable Architecture

  The SonicWALL GMS distributed architecture scales to support thousands of SonicWALL appliances, making large-scale deployments a reality. It allows network administrators to deploy a management architecture that scales to support a rapidly growing customer base while minimizing support staff and hardware.

- Load balancing and Redundancy for Security Management

  In a SonicWALL GMS multi-server configuration, each Agent is responsible for a set of SonicWALL appliances. If an Agent fails, peer SonicWALL GMS Agents will manage the SonicWALL appliances for the failed Agent. SonicWALL GMS also provides redundancy for the SonicWALL GMS Console.

- Role-Based Management

  SonicWALL GMS provides a multi-user architecture with customizable views. Multiple users with different management privileges can be defined to distribute management tasks across a group of administrators and operators.

- Centralized Reporting

  SonicWALL GMS provides graphical reporting of firewall and network activities for the SonicWALL appliances. A wide range of informative real-time and historical reports can be generated to provide insight into usage trends and security events.

  SonicWALL GMS provides aggregated reports for groups of SonicWALL appliances. It also enables the user, in addition to changing the date for a report, to set the number of users or sites as well as select a type of chart for the report.

- Centralized Monitoring

  SonicWALL GMS includes monitoring capabilities for fault and performance data analysis. Monitoring includes VPN and device up/down status, VPN statistics, uptime calculations, and security events for GMS management activities.

- Support for SNMP

  A powerful real-time alert mechanism greatly enhances the administrator's ability to pinpoint and respond to critical events. SonicWALL GMS can centrally receive firewall SNMP traps over the secure management tun-

nel and forward them to an SNMP management system, ensuring the security of firewall traps. The Son-icWALL GMS security events can also be forwarded to the SNMP management system as SNMP traps.

- Log Viewer

  SonicWALL GMS provides detailed daily firewall logs to analyze specific events.

- Command-Line Interface

  SonicWALL GMS features a command line interface that can add multiple SonicWALL appliances at once, configure security and VPN policies, change SonicWALL appliance settings, and display product-related sta-tus.

- Database Support

  SonicWALL GMS supports access to industry-leading relational databases for highly efficient and reliable data storage and retrieval.

- Audit Trailing

  All changes made in SonicWALL GMS are automatically logged, along with the identities of the individuals making the changes.

- GUI-Based Architecture

  The SonicWALL GMS user interface (UI) is easy to use and enables administrators to navigate through the managed SonicWALL appliances, view their settings, and make changes.

- Advanced Security Features
  - A random password is assigned to each SonicWALL appliance. All passwords are encrypted and stored in the database.
  - SonicWALL GMS communicates with managed SonicWALL appliances using Internet Protocol Security (IPSec) VPN tunnels.
  - SonicWALL GMS communicates with the SonicWALL registration database using HTTPS.
  - The SonicWALL GMS login password is encrypted.

- Enhanced Search Features

  SonicWALL GMS enables you to locate task or log entries by entering search criteria.

- Upgrade and Subscription Expiration Notices

  SonicWALL GMS sends an email notification to the SonicWALL GMS administrator when firewall upgrade and subscription services are about to expire for the managed SonicWALL appliances. By default, the emails are sent out 30 days and 7 days prior to the expiration dates. The SonicWALL GMS administrator can change the default values by specifying the period when to email the expiry notifications for the firewall upgrades and subscriptions.

Deployment Requirements

SonicWALL GMS requires a number of deployment components. Before installing SonicWALL GMS, review the following deployment requirements.

- Supported Platforms
    - Solaris 8
    - Windows 2000
    - Windows XP Professional
    - Windows Server 2003
- Supported Databases
    - Oracle version 9.2.0.1
    - Microsoft SQL Server 2000 SP3
- Supported Drivers

    SonicWALL GMS requires a Java database connectivity (JDBC) driver to communicate with the database. For Oracle, the JDBC driver is included with the Oracle database. For Microsoft SQL Server 2000, SonicWALL provides the Sprinta(tm) 2000 JDBC driver.

- Secure Communications Link

    SonicWALL GMS communicates with the managed SonicWALL appliances using IPSec VPN tunnels. These tunnels are created between the GMS gateway that resides between the SonicWALL GMS server(s) and the managed SonicWALL appliances. An GMS gateway can be any VPN-enabled SonicWALL appliance. A SonicWALL PRO 330 or GX is recommended.

    The GMS gateway can be configured either in the standard or NAT mode. For standard mode, the GMS Gateway must be running firmware version 6.3.1 or later.

- Supported Models:
    - SonicWALL TELE2/3
    - TELE3 TZ, TZX, and TELE3 SP
    - TZ170, TZ 170W, and TZ 170SP
    - SOHO2/3
    - XPRS and XPRS2
    - PRO Series
    - GX Series
- Supported Firmware

    The SonicWALL appliances and the GMS gateway must run firmware version 6.1.2.0 or later. No earlier versions of the firmware are supported.

- SonicWALL GMS Installation

    Installation is available on one server (single installation) or multiple servers (distributed installation).

    When SonicWALL GMS is installed on one system, firewall management redundancy and load balancing is not available for its SonicWALL appliances. Windows-based SonicWALL GMS services are the GMS Scheduler, GMS ViewPoint Scheduler, GMS ViewPoint Summarizer, GMS SNMP Manager, and GMS Web Server. Solaris-based SonicWALL GMS daemons are tomcat.sh, GMSsched.sh, sgmsvp1.sh, and sgmsvp2.sh.

    When installing SonicWALL GMS on multiple systems, management redundancy and load balancing is available for the managed SonicWALL appliances. Windows environments use the GMS Scheduler, GMS SNMP Manager, and GMS ViewPoint Summarizer services on the SonicWALL GMS Agents, GMS ViewPoint Scheduler, GMS ViewPoint Summarizer, GMS SNMP Manager, and GMS Web Server services on the SonicWALL GMS Console.

    Solaris environments use the sgmssched.sh, sgmsvp2.sh, and sgmsnmpmgr.sh daemons on the SonicWALL GMS Agents and the tomcat.sh, sgmsnmpmgr.sh, sgmsvp1.sh, and sgmsvp2.sh daemons on the SonicWALL GMS Console.

    Note: The SonicWALL GMS console and agent servers must use static IP addresses.

- Database Installation

    Installing the database on a separate system is highly recommended.

Scaling SonicWALL GMS

The SonicWALL Global Management System (SonicWALL GMS) is designed to be highly scalable to support service providers and enterprise customers with large numbers of SonicWALL appliances.

SonicWALL GMS offers a distributed management architecture, consisting of multiple servers: One console and several agents. Each agent server can manage a number of SonicWALL appliances. Additional capacity can be added to the management system by adding new agent servers. This distributed architecture also provides redundancy and load balancing, assuring reliable connections to the SonicWALL appliances under management (Figure 1).

Figure 1: SonicWALL GMS Two-Tier Distributed Configuration
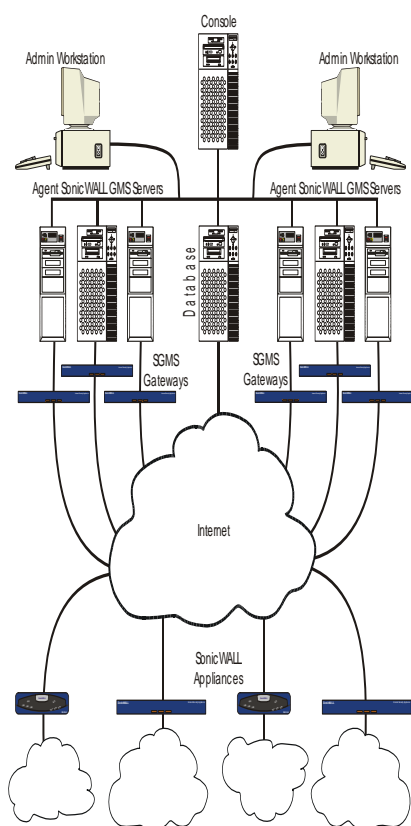
The distributed architecture uses multiple SonicWALL GMS servers. The console server provides the user a single interface to the management system. Each agent server can manage a number of SonicWALL appliances. This number depends on the GMS gateway that resides between the agent server and the SonicWALL appliances. For example, a PRO 330 agent server can manage up to 1,000 SonicWALL appliances.

- The GMS gateway that resides between a SonicWALL GMS agent server and the SonicWALL appliances provides the secure communications.
- Each SonicWALL appliance can have a primary agent server and a standby server. And each agent server can be a primary server for some SonicWALL appliances and a standby server for other SonicWALL appliances.
- Configuration of and changes to the SonicWALL GMS and the SonicWALL appliances are written into the database.
- The users at the Admin Workstations can access the SonicWALL GMS console through a Web browser (HTTP) from any location. The SonicWALL GMS can also e securely accessed using HTTPS. For configuration details, see Appendix A of the *SonicWALL Global Management System Configuration Guide*.
- The SonicWALL GMS console server can also be an agent server.

Using and Navigating SonicWALL GMS

The SonicWALL Global Management System (SonicWALL GMS) has an easy-to-use web browser-based user interface (UI) which is very similar to the standard SonicWALL firewall UI. However, the SonicWALL GMS UI is much more powerful. SonicWALL GMS can manage thousands of SonicWALL appliances. Through its interface, you can configure individual SonicWALL appliances, groups of SonicWALL appliances, or all SonicWALL appliances within the network.

This chapter describes the following:

- SonicWALL GMS registration process. See "Registering SonicWALL GMS" on page 8.
- SonicWALL GMS login process. See "Logging In" on page 9.
- SonicWALL GMS Policies, Reports, and Console panels. See "SonicWALL GMS Panels" on page 11.
- SonicWALL GMS global, group, and individual appliance views. See "Views" on page 14.
- SonicWALL GMS menus. See "SonicWALL GMS TreeControl Menu" on page 18.
- SonicWALL GMS icons. See "SonicWALL GMS Icons" on page 19.

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 2).

   Figure 2: Registration Page

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 9.

   Note: If registration fails see Appendix B of the SonicWALL Global Management System Installation Guide. 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://sgms_ipaddress` 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`.

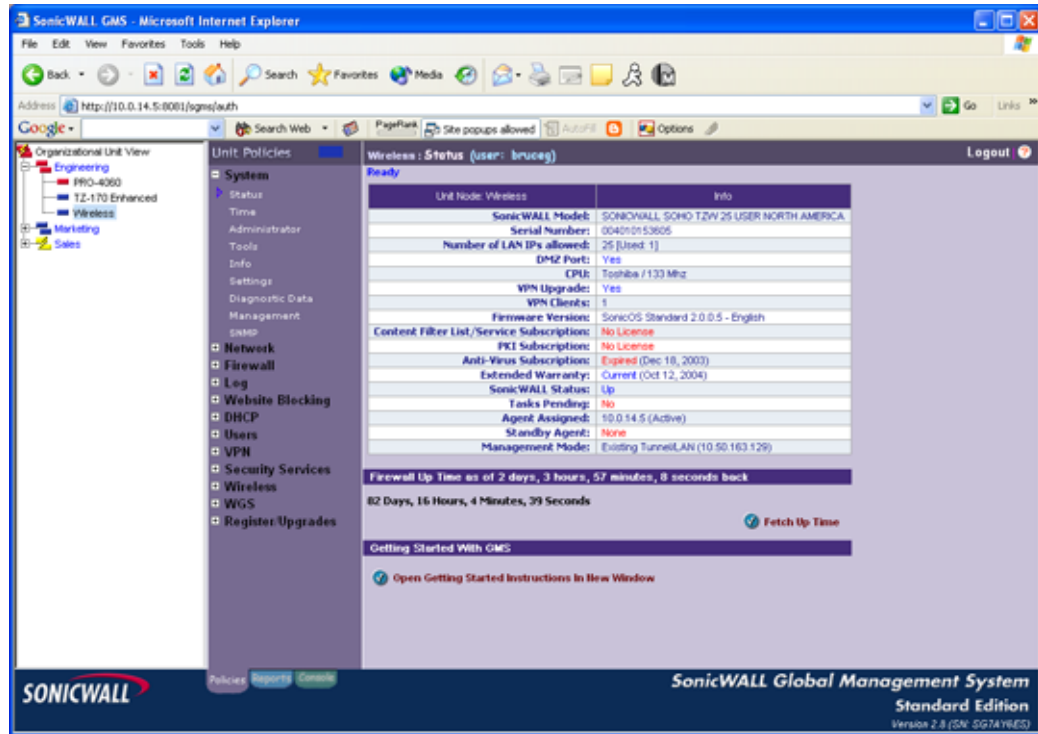   The SonicWALL GMS login page appears (Figure 3).

Figure 3: SonicWALL GMS Login Page
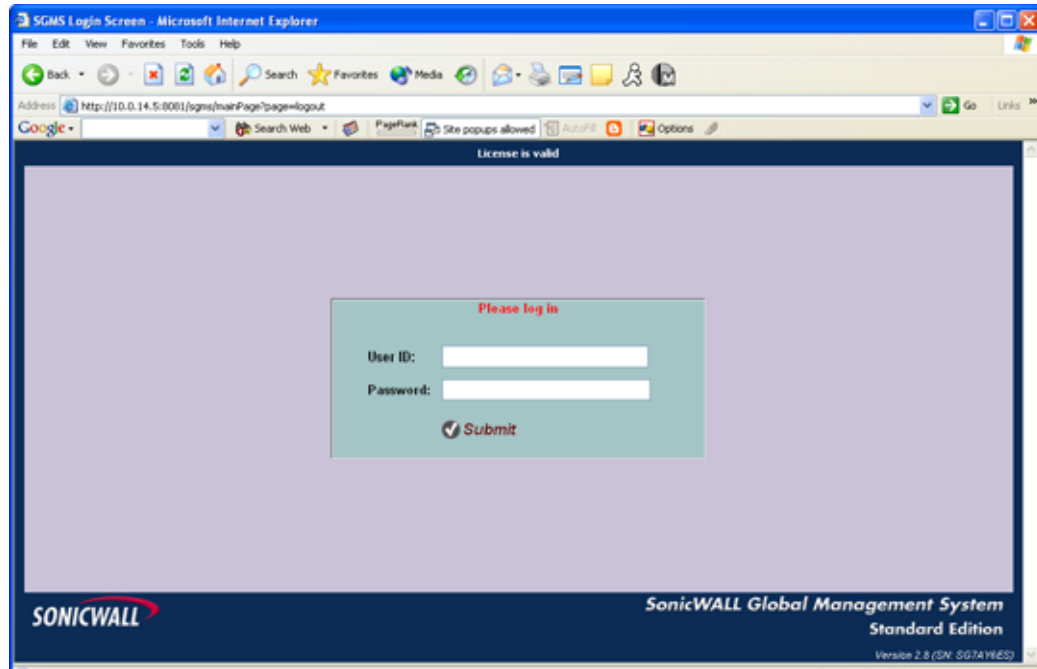
2. Enter the SonicWALL user ID (default: admin) and password (default: password).

3. Click **Submit**. The SonicWALL GMS UI opens (Figure 4).

Figure 4: SonicWALL GMS UI
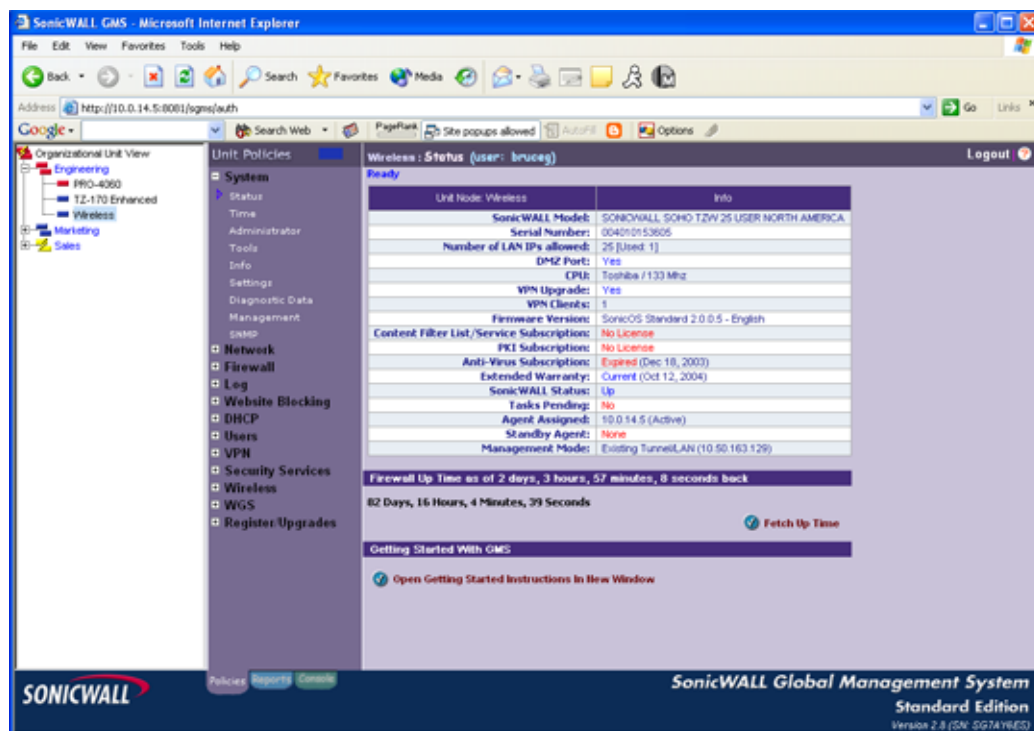
SonicWALL GMS Panels

SonicWALL GMS has three major configuration panels: the Policies Panel, the Reports Panel, and the Console Panel. The Policies Panel configures SonicWALL appliances. For information on the Policies Panel, see "Policies Panel," below. The Reports Panel reports on critical network events and activity, such as security threats, inappropriate Web use, and bandwidth levels. For information on the Reports Panel, see the "Reports Panel" on page 12. The Console Panel configures SonicWALL GMS settings. For information on the Console Panel, see "Console Panel" on page 12.

Policies Panel

The Policies Panel is used to configure SonicWALL appliances. From these pages, you can apply settings to all SonicWALL appliances being managed by SonicWALL GMS, all SonicWALL appliances within a group, or individual SonicWALL appliances.

To open the Policies Panel for SonicWALL appliances, click the **Policies Panel** tab at the bottom of the SonicWALL GMS UI. The SonicWALL appliance Policies Panel appears (Figure 5).

Figure 5: SonicWALL GMS UI: Policies Panel

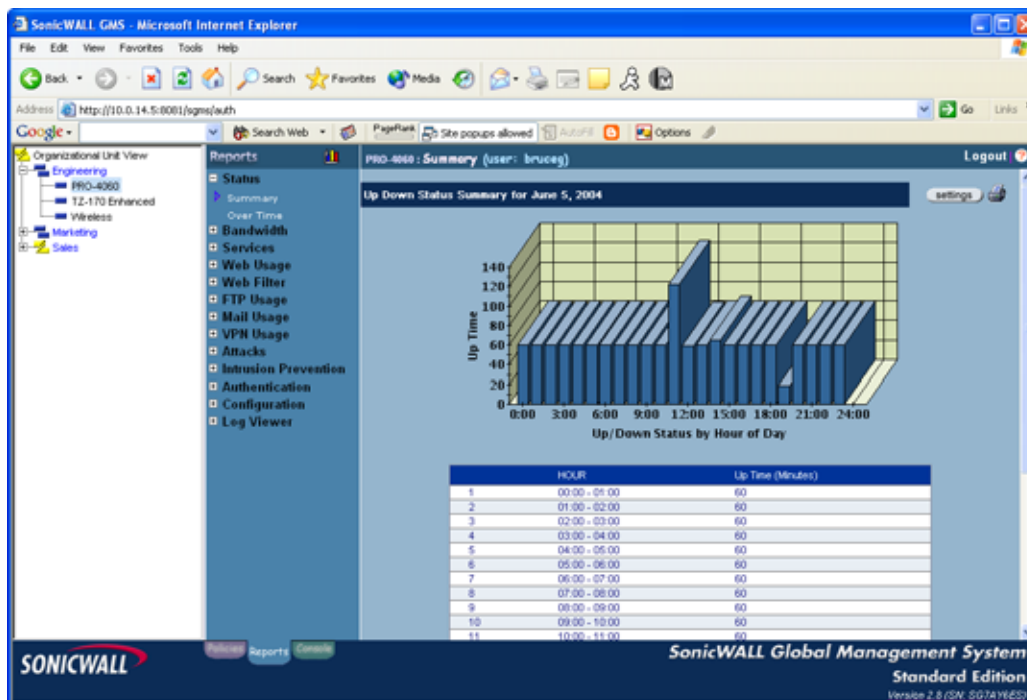From the Policies Panel, you can do the following:

- View the status of a SonicWALL appliance or group.
- Change general settings such as network settings, time, and SonicWALL passwords.
- Configure SonicWALL log settings.
- Configure website blocking options.
- Configure firewall options.
- Configure advanced settings, such as proxy settings, intranet settings, routes, DMZ addresses, one-to-one network address translation (NAT), and Ethernet settings.
- Configure Dynamic Host Configuration Protocol (DHCP) settings.
- Create Virtual Private Networking (VPN) Security Associations (SAs).
- Configure Remote Authentication Dial-In User Service (RADIUS), anti-virus, and high availability settings.
- Register SonicWALL appliances.
- Update SonicWALL firmware.
- Activate Public Key Infrastructure (PKI) certificates, other feature upgrades, and subscription services.

Reports Panel

The Reports Panel is an essential component of network security that is used to report critical network events and activity, such as security threats, inappropriate Web use, and bandwidth levels.

To open the Reports Panel, click the **Reports Panel** tab at the bottom of the SonicWALL GMS UI (Figure 6).

Figure 6: SonicWALL GMS UI: Reports Panel

From the Reports Panel, you can do the following for SonicWALL appliances:

- View general bandwidth usage. These reports include a real-time report, a daily bandwidth summary report, a top users of bandwidth report, and a weekly summary report.
- View bandwidth usage, by service. These reports include a real-time report and a summary report.
- View web bandwidth usage. These reports include a daily bandwidth summary report, a top visited sites report, a top users of web bandwidth report, a report that contains the top sites of each user, and a weekly summary report.
- View the number of attempts that users made to access blocked websites. These reports include a daily summary report, a top blocked sites report, a top users report, a report that contains the top blocked sites of each user, and a weekly summary report.
- View file transfer protocol (FTP) bandwidth usage. These reports include a daily FTP bandwidth summary report, a top users of FTP bandwidth report, and a weekly summary report.
- View mail bandwidth usage. These reports include a daily mail summary report, a top users of mail report, and a weekly summary report.
- View VPN usage. These reports include a daily VPN summary report, a top users of VPN bandwidth report, and a weekly summary report.
- View reports on attempted attacks and errors. The attack reports include a daily attack summary report, an attack by category report, a top sources of attacks report, and a weekly attack summary report. The error reports include a daily error summary report and a weekly error summary report.
- View detailed logging information. The detailed logging information contains each transaction that occurred on the SonicWALL appliance.
- View successful and unsuccessful user and administrator authentication attempts. These reports include a user authentication report, an administrator authentication report, and a failed authentication report.

Console Panel

The Console Panel is used to configure SonicWALL GMS settings, view pending tasks, and manage licenses.

To open the Console Panel, click the **Console Panel** tab at the bottom of the SonicWALL GMS UI (Figure 7).

Figure 7: SonicWALL GMS UI: Console Panel
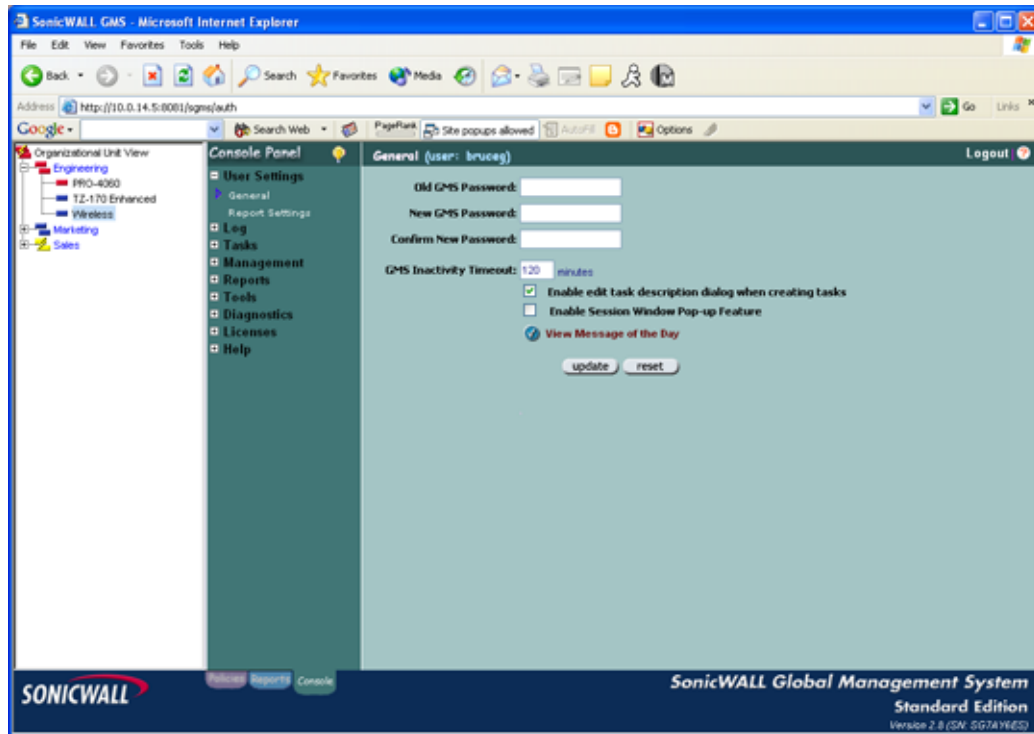
From the Console Panel, you can do the following:

- Change the SonicWALL GMS password.
- View the SonicWALL GMS log. The SonicWALL GMS log contains information on alert notifications, failed SonicWALL GMS login attempts, and other events that apply to SonicWALL GMS.
- Manage tasks. You can view the status of SonicWALL tasks and, if necessary, delete them.
- Manage upgrade and subscription licenses for SonicWALL appliances. After loading these licenses into the license pool, you can apply them to SonicWALL appliances from the Policies Panel.
- Manage SonicWALL GMS user logins and privileges, agents, and dynamic views.

Views

The SonicWALL GMS UI is a robust and powerful tool you can use to apply settings to all SonicWALL appliances being managed by SonicWALL GMS, all appliances or devices within a group, or individual appliances or devices simply by selecting the Global, Group, or Unit view within the SonicWALL GMS UI.

The SonicWALL GMS UI supports up to seven group levels of hierarchy.

Note: Views are only available in the Policies and Reports Panel. Changing views does not affect the Console Panel.

This section describes each view and what to consider when making changes. Select from the following:
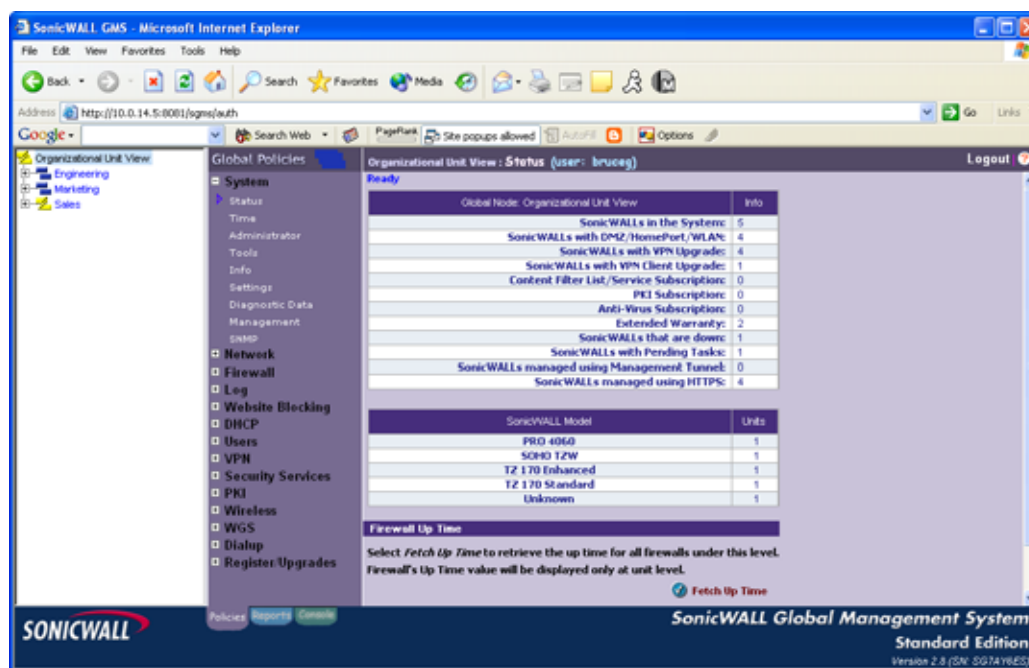
- Global View—see "Global View," below.
- Group View—see "Group View" on page 15.
- Unit View—see "Unit View" on page 16.

Global View

From the Global view of the Policies Panel, changes are applied to all SonicWALL appliances that are being managed by SonicWALL GMS.

To open the Global view, click the Global View icon in the upper-left hand corner of the left pane. The Global Status page appears (Figure 8).

Figure 8: Global Status Page

As you navigate the SonicWALL GMS Policies Panel screens with the Global view selected and make changes, those changes are broken down into configuration tasks and applied to each SonicWALL appliance being managed by SonicWALL GMS.

As SonicWALL GMS processes the tasks, some devices may be down or offline. When this occurs, SonicWALL GMS spools the task and reattempts the update later.

Note: Depending on the page that you are configuring, the SonicWALL appliance(s) may automatically restart. We recommend scheduling the tasks to run when network activity is low. For information on which changes require restarting, refer to their configuration instructions.

Making global changes through the SonicWALL GMS UI enables you to save time by instituting changes that affect all SonicWALL appliances within the network through a single operation. Although this is very convenient, making changes to all the devices can have unintended consequences. Be careful when making global changes.

Global View Status Page

The Global View Status page contains a list of statistics for all SonicWALL appliances within the network. These include the following:

- SonicWALLs in the System—specifies the number of SonicWALL appliances managed by the SonicWALL GMS.
- SonicWALLs with DMZ/HomePort/WLAN—specifies the number of SonicWALL appliances that have a DMZ port.
- SonicWALLs with VPN Upgrade—specifies the number of SonicWALL appliances that are licensed for a VPN upgrade.
- SonicWALLs with VPN Client Upgrade—specifies the number of SonicWALL appliances that are licensed for VPN Clients.
- Content Filter Subscription List/Service—specifies the number of SonicWALL appliances that are licensed for Content Filter Subscriptions.
- PKI Subscription—specifies the number of SonicWALL appliances that have PKI subscriptions.
- Anti-Virus Subscription—specifies the number of SonicWALL appliances that have anti-virus subscriptions.
- Extended Warranty—specifies the number of SonicWALL appliances that have an extended warranty.
- SonicWALLs that are down—specifies the number of SonicWALL appliances that are down.
- SonicWALLs with Pending Tasks—specifies the number of SonicWALL appliances that have pending tasks.
- SonicWALL managed using Management Tunnel—specifies the number of SonicWALL appliances that are being managed by SonicWALL GMS using the management VPN tunnel.
- SonicWALL Models—specifies the number and types of SonicWALL appliances that are being managed by SonicWALL GMS.
- Fetch Uptime—the Uptime parameter indicates how long the SonicWALL has been running since the last time it was powered up or restarted. To display the current uptime setting at the unit level for each SonicWALL appliance in the network, click **Fetch Uptime**.

Group View

From the Group view of the Policies panel, changes you make are applied to all SonicWALL appliances within the group.

To open the Group view, click a group icon in the left pane of the SonicWALL GMS UI. The Group Status page appears (Figure 9).

Figure 9: Group Status Page
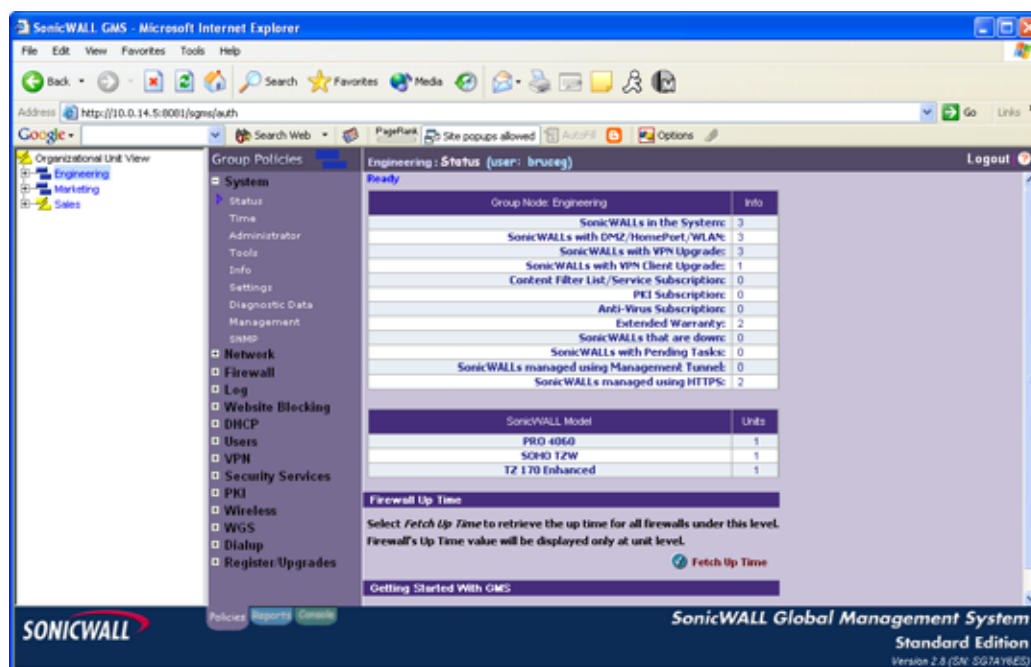
As you move through the SonicWALL GMS UI with the Group view selected and make changes, those changes are broken down into configuration tasks and applied to each subgroup and each SonicWALL appliance within the group.

As SonicWALL GMS processes the tasks, some SonicWALL appliances may be down or offline. When this occurs, SonicWALL GMS spools the task and reattempts the update later.

Note: Depending on the page that you are configuring, the SonicWALL appliance(s) may automatically restart. We recommend scheduling the tasks to run when network activity is low. For information on which changes require restarting, refer to their configuration instructions.

Making group changes through the SonicWALL GMS UI enables you to save time by instituting changes that affect all SonicWALL appliances within the group through a single operation. Although this is very convenient, some changes can have unintended consequences. Be careful when making these changes.

Group View Status Page

The Group View Status page contains a list of statistics for all SonicWALL appliances within the group. These include the following:

- SonicWALLs in the System—specifies the number of SonicWALL appliances managed by SonicWALL GMS.
- SonicWALLs with DMZ/HomePort/WLAN—specifies the number of SonicWALL appliances that have a DMZ port.
- SonicWALLs with VPN Upgrade—specifies the number of SonicWALL appliances that are licensed for a VPN upgrade.
- SonicWALLs with VPN Client Upgrade—specifies the number of SonicWALL appliances that are licensed for VPN Clients.
- Content Filter Subscription List/Service—specifies the number of SonicWALL appliances that are licensed for Content Filter List subscriptions.
- PKI Subscription—specifies the number of SonicWALL appliances that have PKI subscriptions.
- Anti-Virus Subscription—specifies the number of SonicWALL appliances that have anti-virus subscriptions.
- Extended Warranty—specifies the number of SonicWALL appliances that have an extended warranty.
- SonicWALLs that are down—specifies the number of SonicWALL appliances that are down.
- SonicWALL managed using Management Tunnel—specifies the number of SonicWALL appliances that are being managed by SonicWALL GMS using the management VPN tunnel.
- SonicWALLs with Pending Tasks—specifies the number of SonicWALL appliances that have pending tasks.
- SonicWALL Models—specifies the number and types of SonicWALL appliances that are being managed by SonicWALL GMS.
- Fetch Uptime—the Uptime parameter indicates how long the SonicWALL has been running since the last time it was powered up or restarted. To display the current uptime setting at the unit level for each SonicWALL appliance in the group, click **Fetch Uptime**.

Unit View

From the Unit view of the Policies panel, changes you make are only applied to the selected SonicWALL appliance. To open the Unit view, click a SonicWALL appliance in the left pane of the SonicWALL GMS UI. The Status page for the SonicWALL appliance appears (Figure 10).

Figure 10: Unit Status Page
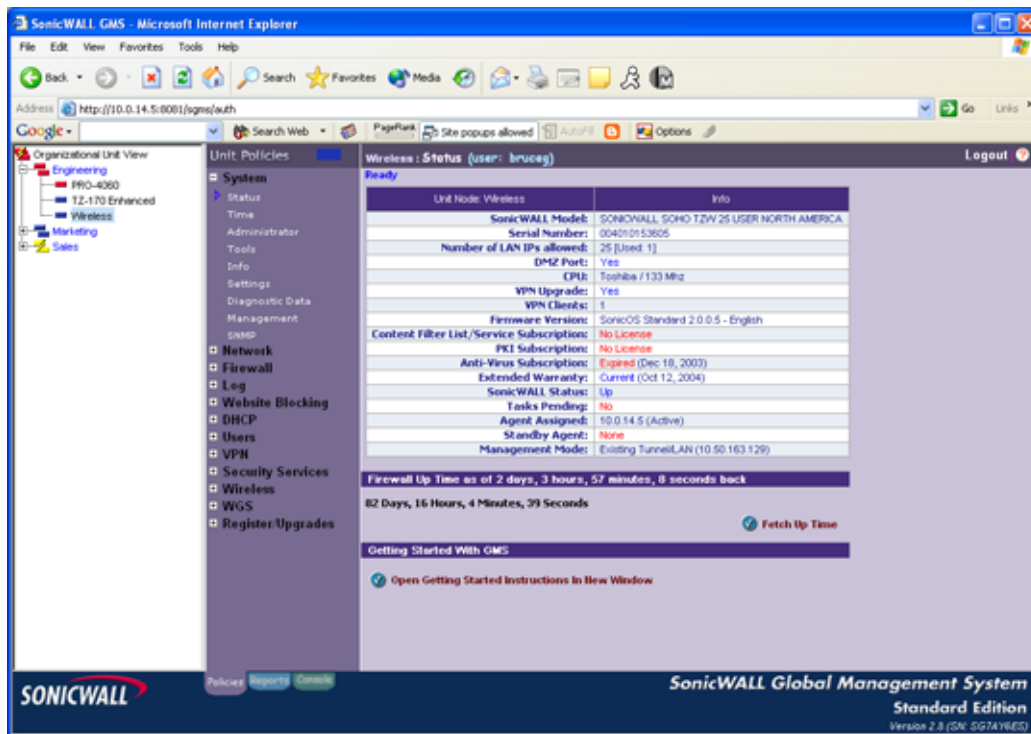
As you navigate the SonicWALL GMS UI with a single SonicWALL appliance selected and make changes, those changes are broken down into configuration tasks and sent to the selected SonicWALL appliance.

As SonicWALL GMS processes the tasks, the SonicWALL appliance may be down or offline. When this occurs, SonicWALL GMS spools the task and reattempts the update later.

Note: Depending on the page that you are configuring, the SonicWALL appliance may automatically restart. We recommend scheduling the tasks to run when network activity is low. For information on which changes require restarting, refer to their configuration instructions.

Unit View Status Page

The Unit View Status page contains a list of statistics for the selected SonicWALL appliance. These include the following:

- SonicWALL Model—specifies the model of the SonicWALL appliance. If the unit is not registered, "Not Registered" appears instead of a model number.
- Serial Number—specifies the serial number of the SonicWALL appliance.
- Number of LAN IPs allowed—specifies the number of IP addresses that are allowed on the LAN.
- DMZ Port—specifies whether the SonicWALL appliance has a DMZ port.
- CPU—specifies the CPU used on the SonicWALL appliance.
- VPN Upgrade—specifies whether the SonicWALL is licensed for a VPN upgrade.
- VPN Clients—specifies whether the SonicWALL is licensed for VPN Clients.
- Firmware Version—specifies the version of the firmware installed on the SonicWALL appliance.
- Content Filter Subscription List/Service—specifies whether the SonicWALL appliance is licensed for a Content Filter List subscription.
- PKI Subscription—specifies whether the SonicWALL appliance has a PKI subscription.
- Anti-Virus Subscription—specifies whether the SonicWALL appliance has an anti-virus subscription.
- Extended Warranty—specifies whether the SonicWALL appliance has an extended warranty.
- SonicWALL Status—specifies the operational status of the SonicWALL appliance.
- Tasks Pending—specifies whether the SonicWALL appliance has any pending tasks.
- Agent Assigned—specifies the IP address of the SonicWALL GMS agent server that is the primary agent managing the SonicWALL appliance.
- Standby Agent—specifies the IP address of the peer SonicWALL GMS that acts as the backup agent for this SonicWALL appliance. If the primary agent fails, this SonicWALL GMS server will manage the appliance.
- Managed using Management Tunnel—specifies if the SonicWALL appliance is being managed by SonicWALL GMS using the management VPN tunnel.
- Fetch Uptime—the Uptime parameter indicates how long the SonicWALL has been running since the last time it was powered up or restarted. To display the current uptime setting at the unit level for the selected SonicWALL, click **Fetch Uptime**.

From the Unit view on the Reports Panel, you can generate real-time and historical reports for the selected SonicWALL appliance.

As you navigate the SonicWALL GMS UI, you can generate graphical reports and view detailed log data for the selected SonicWALL appliance. For more information, see "Reports Panel" on page 12 or the *SonicWALL Global Management System ViewPoint Guide*.

SonicWALL GMS TreeControl Menu

This section describes the content of the TreeControl menu within the SonicWALL GMS UI. To open a TreeControl menu, right-click the Global icon, a Group icon, or a Unit icon and select from the following:

- Find—opens a Find dialog box where you can search for groups or units.
- Add Unit—adds a new SonicWALL appliance.
- Delete—deletes the selected group or SonicWALL appliance.
- Rename Unit—renames the selected SonicWALL appliance.
- Properties—displays the properties for the selected SonicWALL appliance.
- Add/Delete/Modify View—opens a dialog box where you can create, delete, or modify a view.
- Change View—changes to another view.
- Expand Node—expands the navigational tree to display all groups and SonicWALL appliances managed by SonicWALL GMS.
- Collapse Node—collapses all groups and SonicWALL appliances managed by SonicWALL GMS.
- Reassign Agents—opens a dialog box where you can change the IP address of the primary and standby schedulers and the type of VPN tunnel (management vs. site-to-site) used between SonicWALL GMS and the managed SonicWALL appliances.

SonicWALL GMS Icons

This section describes the meaning of icons that appear in the left pane of the SonicWALL GMS window.

Group is in the normal operational state. All units within the group are accessible from the SonicWALL GMS and no tasks are pending or scheduled (blue icons).

Unit is in the normal operational state. The unit is accessible from the SonicWALL GMS and no tasks are pending or scheduled (blue icon).

One or more units within the group has failed or is not accessible from SonicWALL GMS (red icons).

The unit has failed or is not accessible from SonicWALL GMS (red icon).

Tasks are currently pending or running on one or more units within the group (blue icons with lightening bolt).

One or more tasks is currently pending or running on the unit (blue icon with lightening bolt).

One or more units within the group has failed or is not accessible from SonicWALL GMS and has one or more tasks pending (red icons with lightening bolt).

The unit has failed or is not accessible from SonicWALL GMS and has one or more tasks pending (red icon with lightening bolt).

Tasks are currently scheduled on one or more units within the group (blue icons with calendar).

One or more tasks are currently scheduled on the unit (blue icon with calendar).

One or more units with the group has been added to SonicWALL GMS (provisioned) but not yet acquired (yellow icons).

The unit has been added to SonicWALL GMS (provisioned) but not yet acquired (yellow icon).

Tasks are currently pending on one or more provisioned units within the group (yellow icons with lightening bolt).

One or more tasks are currently pending on the provisioned unit (yellow icon with lightening bolt).

Getting Help

In addition to this manual, SonicWALL GMS provides on-line help resources. To get help, follow these steps:

1. Start and log into SonicWALL GMS.
2. Navigate to the page where you need help.
3. Click the Question Mark (?) in the upper right-hand corner of the window.
4. Help for the selected page appears.

Planning

The SonicWALL Global Management System (SonicWALL GMS) uses a very innovative method for organizing SonicWALL appliances.

SonicWALL appliances are not forced into specific, limited, rigid hierarchies. Simply create a set of fields that define criteria that separate SonicWALL appliances (e.g., country, city, state). Then, create and use views to display and sort appliances on the fly.

To organize SonicWALL appliances, follow these steps:

- Create custom fields that will be useful to your organization. See "Creating Views with Custom Fields" on page 22.
- Review the standard SonicWALL fields. See "Creating Views with Pre-Defined Fields" on page 22.
- Create views that will make your job easier. See "Sample Views" on page 23.

Creating Views with Custom Fields

When you first configure SonicWALL GMS, you should create custom fields that will be entered for each Son-icWALL appliance.

SonicWALL GMS supports up to ten custom fields. The following are examples of custom fields that you might want to use:

- Geographic—useful for organizing SonicWALL appliances geographically. Especially useful when used in combination with other grouping methods. Geographic fields may include the following:
  - Country
  - Time Zone
  - Region
  - State
  - City
- Customer-based—useful for organizations that are providing managed security services for multiple customers. Customer-based fields may include:
  - Company
  - Division
  - Department
- Configuration-based—useful when SonicWALL appliances will have very different configurations. (e.g., Filtering, No Filtering, Pornography Filtering, Violence Filtering, VPN).
- User-type—useful for making different service offerings available to different user types. For example, engineering, sales, and customer service users might have very different configuration requirements. Or, if this is offered as a service to end users, you might allow or disallow network address translation (NAT) depending on the number of IP addresses that you want to make available.

Note: For information on creating custom views, refer to the SonicWALL Global Management System Configuration Guide.

Creating Views with Pre-Defined Fields

SonicWALL GMS includes standard fields that can be used to sort SonicWALL appliances based on their model, their firmware version, and other criteria. SonicWALL GMS fields currently include the following:

- AV Status—places the SonicWALL appliances into two groups: appliances that have anti-virus subscriptions and appliances that do not.
- AV Enabled—places the SonicWALL appliances into two groups: appliances that have the anti-virus feature enabled and appliances that do not.
- CFL Status—places the SonicWALL appliances into two groups: appliances that have content filter list subscriptions and appliances that do not.
- Firmware—creates a group for each Firmware version and places each SonicWALL appliance into its corresponding group.
- Model—creates a group for each SonicWALL model and places each SonicWALL appliance into its corresponding group.
- Nodes—creates a group for each node range and places each SonicWALL appliance into its corresponding group.
- PKI Status—places the SonicWALL appliances into two groups: appliances that have PKI and appliances that do not.
- Registered—places the SonicWALL appliances into two groups: appliances that are registered and appliances that are not.
- VPN Present—places the SonicWALL appliances into two groups: appliances that have VPN and appliances that do not.
- Unit Status—places the SonicWALL appliances in 3 groups: appliances that are up, down, or provisioned.

Sample Views

After creating custom criteria, GMS administrators can set up views to perform different functions.

Note: Each view can show a maximum of seven fields. Multiple views can be created.

Standard Geographic Views

When the number of SonicWALL appliances managed by SonicWALL GMS becomes large, you can divide the appliances geographically among SonicWALL administrators.

For example, if one administrator is responsible for each time zone in the United States, you can choose the following grouping methods:

- Administrator 1: Country: USA, Time Zone: Pacific, State, City.
- Administrator 2: Country: USA, Time Zone: Mountain, State, City.
- Administrator 3: Country: USA, Time Zone: Central, State, City.
- Administrator 4: Country: USA, Time Zone: Eastern, State, City.

Firmware Views

To ensure that all SonicWALL appliances are using the current firmware, you can create a view to check and update firmware versions and batch process firmware upgrades when network activity is low.

For example, if you want to update all SonicWALL appliances to the latest firmware at 2:00 A.M., you can use the following grouping method:

- Firmware Version, Time Zone

If you want to update SonicWALL appliances for companies that have agreed to the upgrade and you want the upgrades to take place at 2:00 A.M., you can use the following grouping method:

- Company, Firmware Version, Time Zone

Registration Views

To ensure that all SonicWALL appliances are registered, you can create a registration view and check it periodically. To create a registration view, you can use the following grouping method:

- Registration Status, any other grouping fields

Upgrade Views

You can create views that contain information on which upgrades customers do not have and forward this information to the Sales Department.

For example, you can choose the following grouping methods:

- Content Filter List, Company, Division, Department
- Anti-Virus, Company, Division, Department
- Warranty Status, Company, Division, Department