SonicWALL® Global Management System

POLICY AND MANAGEMENT

Centralized policy management, monitoring and reporting

- **Centralized security and network management**
- **Sophisticated VPN deployment and configuration**
- **Active device monitoring and alerting**
- **Centralized logging**
- **Software, hardware, virtual appliance options**
- **Intelligent reporting and activity visualization**
- **Offline management**
- **Streamlined license manager**
- **SNMP support**
- **Rich integration options**

The SonicWALL® Global Management System (GMS) provides organizations of any size, distributed enterprises and service providers with a flexible, powerful and intuitive solution to centrally manage and rapidly deploy SonicWALL appliances and security policy configurations. SonicWALL GMS™ also provides centralized real-time monitoring, and comprehensive policy and compliance reporting.

SonicWALL GMS' intuitive Web-based user interface easily allows for complete life cycle control of thousands of SonicWALL firewall, anti-spam, secure remote access, and backup and recovery appliances and services—from initial configuration to complex policy changes and remote updates. For enterprises, GMS simplifies the complexity of network management by offering a single management interface, thereby reducing administration time, complexity and the overall total cost of ownership (TCO). Service providers benefit from its multi-organizational management capabilities where it consolidates, groups and classifies thousands of individual customers' managed appliances and their respective security policies. Through an integrated reporting architecture, administrators can customize and schedule reports individually tailored to meet the needs of managed customers, executives and regulatory compliance audits for corporate departments. SonicWALL GMS can be flexibly deployed as a software application on a third party Windows® server, as a SonicWALL E-Class Universal Management Appliance, or as a SonicWALL GMS Virtual Appliance in a VMware® environment.

Features and Benefits

Centralized security and network management is achieved using a flexible, powerful and intuitive tool to deploy, manage and monitor a distributed network environment and set policies from a central location. Administrators can now define, distribute, enforce and deploy a full range of service and security policies for thousands of SonicWALL firewall, anti-spam, secure remote access, and backup and recover appliances.

Sophisticated VPN deployment and configuration enables distributed enterprise networks to reduce the administration time, costs and complexity associated with establishing and maintaining corporate security policies, VPN connectivity and network configurations. For Service Providers, it consolidates and unifies all security polices for thousands of customers allowing for greater efficiencies in meeting service level agreements (SLAs).

Active device monitoring and alerting supplies real-time alerts with integrated monitoring capabilities allowing administrators to take preventative action and deliver immediate remediation.

Centralized logging provides a central location for consolidating security events and logs for thousands of appliances, thereby allowing for a single point to conduct network forensics.

Flexible deployment options include **software** (leveraging existing infrastructure), **hardware** (leveraging a hardened high-performance appliance), or a **virtual appliance** (leveraging shared computing resources to optimize utilization, ease migration and reduce capital costs).

Intelligent reporting and activity visualization presents comprehensive management and graphical reports for security devices and user activity yielding greater insight into application usage trends and security events. It also enables the customization of these reports using corporate logos and colors, thereby delivering a cohesive branding message to users and customers.

Offline management enables scheduled configurations and/or firmware updates on managed appliances to occur offline to minimize service disruption to end users and customers.

Streamlined license manager displays a unified console for storing, applying, tracking and updating security license information for managed SonicWALL appliances, thereby simplifying the inventory for managing security and support license subscriptions.

SNMP support provides a powerful, real-time alerting mechanism for all TCP/IP and SNMP-enabled devices and applications, thus greatly enhancing the ability to pinpoint and respond to critical network events.

Rich integration options include a Web services application programming interface (API), CLI support for the majority of functions, and SNMP trap support. Both services providers and enterprises can use any of these options to integrate GMS with their professional services automation, management and monitoring, and other enterprise applications.

SONICWALL®

PROTECTION AT THE SPEED OF BUSINESS™

Specifications

SonicWALL GMS Standard Edition

SonicWALL GMS Software License
for 10 Nodes
01-SSC-3363

SonicWALL GMS Software License
for 25 Nodes
01-SSC-3311

SonicWALL GMS Software Upgrade
for 1 Node
01-SSC-7662

SonicWALL GMS Software Upgrade
for 5 Nodes
01-SSC-3350

SonicWALL GMS Software Upgrade
for 10 Nodes
01-SSC-7664

SonicWALL GMS Software Upgrade
for 25 Nodes
01-SSC-3301

SonicWALL GMS Software Upgrade
for 100 Nodes
01-SSC-3303

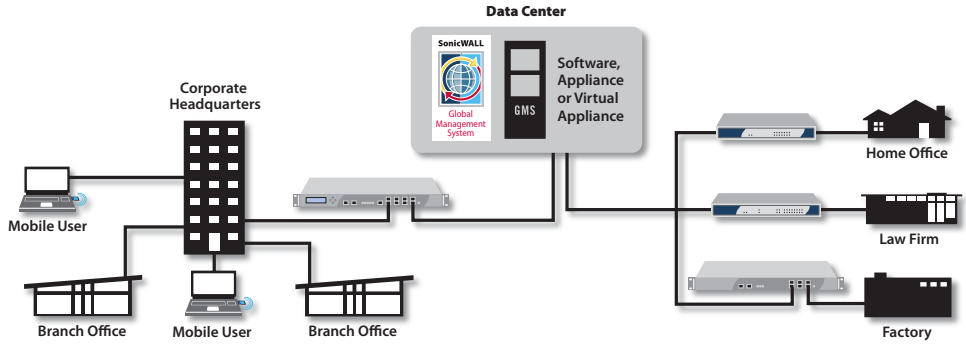
SonicWALL GMS Software Upgrade
for 250 Nodes
01-SSC-3304

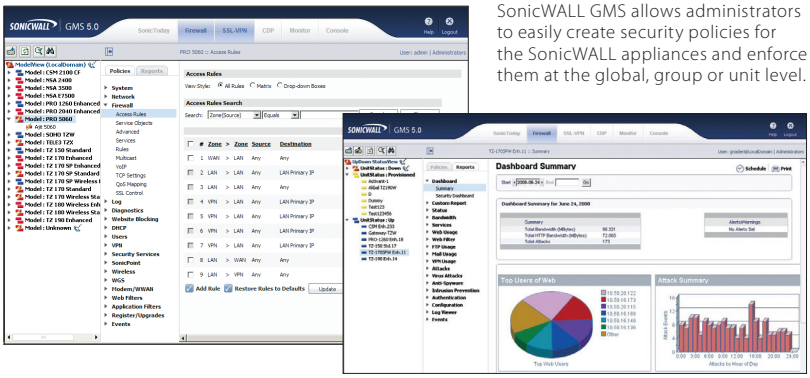
SonicWALL GMS Software Upgrade
for 1,000 Nodes
01-SSC-3306

Visit www.sonicwall.com/us/products/6030.html for an overview of support SKUs.

SonicWALL Global Management System

Providing a comprehensive security management solution for enterprises and service providers.





SonicWALL GMS allows administrators to easily create security policies for the SonicWALL appliances and enforce them at the global, group or unit level.

SonicWALL GMS allows administrators to generate a wide range of informative and historical reports to provide insight into usage trends, such as which Web sites have been accessed, by whom and security events of the managed SonicWALL appliances.

Minimum System Requirements

Below are the minimum requirements for SonicWALL GMS with respect to the operating systems, databases, drivers, hardware and SonicWALL supported appliances:

Operating System

Windows Server 2003 32 bit and 64 bit (SP2), Windows Server 2008 SBS 64 bit, Windows Server 2008 Standard 32 bit and 64 bit (SP1).

In all instances SonicWALL GMS is running as a 32 bit application.

Virtual Appliance

Hypervisor: VMware ESX and ESXi

Operation System Installed: Hardened SonicLinux

Appliance Size: 250 GB - 950 GB

Allocated Memory: 3 GB

VMware Hardware Compatibility Guide: http://www.vmware.com/resources/compatibility/search.php

Hardware for Single Deployment

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

Hardware for Distributed Server Deployment

GMS Server	x86 Environment: Minimum 3 GHz processor single-CPU Intel processor, 2 GB RAM and 300 GB disk space
Database Server	x86 Environment: Minimum 3 GHz processor dual-core CPU Intel processor, 2 GB RAM and 300 GB disk space

GMS Gateway

SonicWALL E-Class NSA, NSA or PRO Series Network Security Appliance with minimum firmware and SonicWALL VPN-based Network Security Appliances[1]

Supported Databases

External Databases: Microsoft SQL 2000 (SP4), Microsoft SQL 2005 32 bit and 64 bit (SP2), Microsoft SQL 2008 (SP1) 64 bit

Bundled with the GMS application: MySQL

Java

Java Plug-in version 1.5 or later

Supported SonicWALL Appliances Managed by GMS

SonicWALL Network Security appliances: E-Class NSA, NSA, PRO Series, TZ Series appliances

SonicWALL Continuous Data Protection (CDP) appliances, SonicWALL Content Security Manager (CSM) appliances, SonicWALL Secure Remote Access appliances: SRA for SMB and E-Class SRA, SonicWALL Email Security Appliances

All TCP/IP and SNMP-enabled devices and applications for active monitoring

Internet Browsers

Microsoft® Internet Explorer 6.0 or higher

Mozilla Firefox 2.0 or higher

Supported Firmware

SonicWALL Network Security appliances: E-Class NSA and NSA SonicOS Enhanced 5.0 or higher

SonicWALL PRO Series appliances: SonicOS Enhanced 3.2 or higher

SonicWALL TZ Series appliances: SonicOS Standard 3.1 or higher and SonicOS Enhanced 3.2 or higher

SonicWALL CDP appliances: SonicWALL CDP 2.3 or higher

SonicWALL CSM appliances: SonicWALL 2.0 or higher

SonicWALL SSL VPN appliances: SonicWALL SRA for SMB Firmware 2.0 or higher and SonicWALL Aventail E-Class SRA Firmware 9.0 or higher

SonicWALL Email Security Appliances: SonicWALL Email Security 7.0 firmware or higher

[1]When using the Management VPN Tunnel option for secure communication between the SonicWALL GMS server and managed appliances using VPN tunnels, a GMS Gateway is required. The GMS gateway should be at minimum a SonicWALL NSA with minimum firmware SonicOS Enhanced 5.0, or a SonicWALL PRO 2040 with minimum firmware SonicOS Enhanced 3.2. When using Existing VPN Tunnels or HTTPS as the management method, a GMS Gateway is not required.

SonicWALL's line-up of comprehensive protection

NETWORK SECURITY | SECURE REMOTE ACCESS | WEB AND E-MAIL SECURITY | BACKUP AND RECOVERY | POLICY AND MANAGEMENT

SonicWALL, Inc.
2001 Logic Drive, San Jose, CA 95124
T +1 408.745.9600 F +1 408.745.9300
www.sonicwall.com

SONICWALL®
PROTECTION AT THE SPEED OF BUSINESS™