



- **Centralized security and network management**
- **Easily set policies**
- **Sophisticated VPN deployment and configuration**
- **Offline management**
- **Streamlined license management**
- **Universal dashboard**
- **Active-device monitoring and alerting**
- **SNMP support**
- **Intelligent reporting and activity visualization**
- **Centralized logging**
- **Real-time and historic next-generation syslog reporting**
- **Application traffic analytics**
- **Extensive cross-platform support**
- **Flexible deployment options**
- **Rich integration options**

Managing, monitoring and reporting on growing distributed networks is increasingly complex and costly. Meanwhile, businesses must ensure uptime and meet strict regulations, within constrained budgets. Service providers must maintain service level agreements (SLAs) on more customer devices with more complex licensing, while meeting return on investment (ROI) targets. Without next-generation application traffic analytics and syslog reporting, organizations have no insight into bandwidth utilization, application traffic or employee productivity. Organizations need easy, affordable management tools that scale across thousands of appliances and security policies.

The SonicWALL® Global Management System (GMS®) provides organizations, distributed enterprises and service providers with a powerful and intuitive solution to centrally manage and rapidly deploy SonicWALL firewall, anti-spam, backup and recovery, and secure remote access solutions. GMS provides centralized real-time monitoring, and comprehensive policy and compliance reporting. For enterprise customers, GMS streamlines security policy management and appliance deployment, minimizing administration overhead. For Service Providers, GMS simplifies the security management of multiple clients and creates additional revenue opportunities. Administrators can cluster GMS solutions for added redundancy and scalability. Flexible deployment options include software, hardware and a virtual appliance.

Features and Benefits

Centralized security and network management helps administrators deploy, manage and monitor a distributed network environment.

Easily set policies for thousands of SonicWALL firewall, anti-spam, backup and recovery, and secure remote access devices from a central location.

Sophisticated VPN deployment and configuration simplify the enablement of VPN connectivity and consolidate thousands of security policies.

Offline management enables scheduling of configurations and/or firmware updates on managed appliances to minimize service disruptions.

Streamlined license management for SonicWALL appliances via a single unified console, simplifies the management of security and support license subscriptions.

Universal dashboard features customizable widgets, geographic maps and user-centric reporting.

Active-device monitoring and alerting provide real-time alerts with integrated monitoring capabilities, greatly enhancing troubleshooting efforts allowing administrators to take preventative action and deliver immediate remediation.

SNMP support provides powerful, real-time traps for all TCP/IP and SNMP-enabled devices and applications, greatly enhancing troubleshooting efforts to pinpoint and respond to critical network events.

Intelligent reporting and activity visualization presents comprehensive management and graphical reports for SonicWALL firewall, anti-spam, backup and recovery, and secure remote access devices yielding greater insight into usage trends and security events, while delivering a cohesive branding for service providers.

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

Real-time and historic next-generation syslog reporting, through a revolutionary enhancement in architecture, streamlines the time-consuming summarization process, allowing for near real-time reporting on incoming syslog messages, and provides the ability to drill down into data and customize reports extensively.

Application traffic analytics provides organizations with powerful insight into application traffic, bandwidth utilization and security threats while providing powerful troubleshooting and forensics capabilities.

Extensive cross-platform support for SonicWALL firewall, anti-spam, backup and recovery, and secure remote access platforms, provides coverage for all SonicWALL products on the network.

Flexible deployment options include software, a hardened high-performance appliance, or a virtual appliance to optimize utilization, ease migration and reduce capital costs.

Rich integration options include an application programming interface (API) for web services, CLI support for the majority of functions, and SNMP trap support for both services providers and enterprises.

Specifications

SonicWALL Global Management System

GMS provides a comprehensive security management solution for enterprises and service providers.

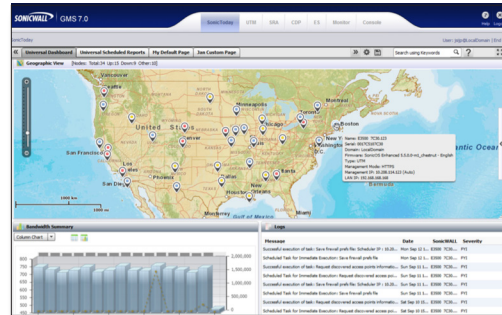
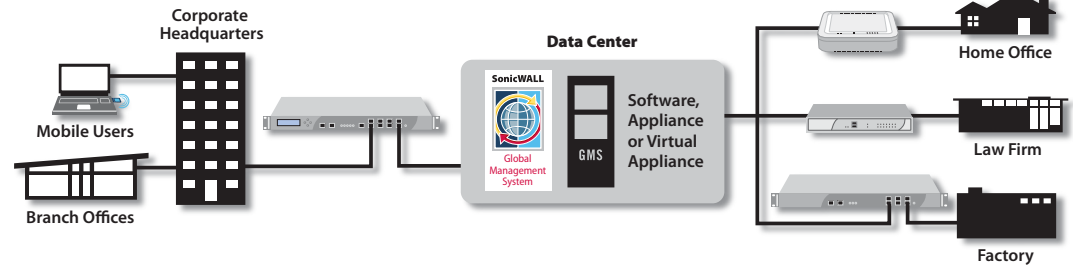


SonicWALL GMS Standard Edition

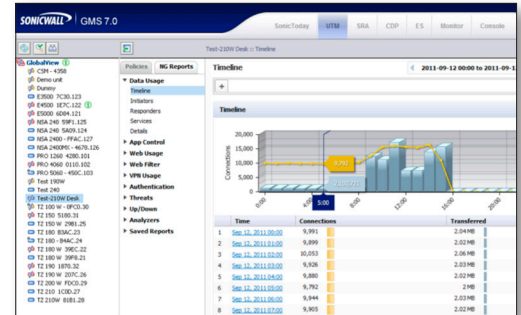
- SonicWALL GMS Software License for 5 Nodes 01-SSC-7680
- SonicWALL GMS Software License for 10 Nodes 01-SSC-3363
- SonicWALL GMS Software License for 25 Nodes 01-SSC-3311
- SonicWALL GMS Software Upgrade for 1 Node 01-SSC-7662
- SonicWALL GMS Software Upgrade for 5 Nodes 01-SSC-3350
- SonicWALL GMS 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.

GMS Mobile is a free Apple® iPhone® application (currently available as beta software) used by GMS admins on the go to remotely log into their GMS system to see an overview of all the devices under management, check device status, and review GMS alerts as they come in.



Context-sensitive dashboards display a variety of informational widgets, such as geographical maps, syslog reports, bandwidth summaries, top websites accessed, or the data that is most relevant to specific users



Monitoring managed SonicWALL appliances is a breeze with intuitive graphical reports. Easily identify traffic anomalies based on usage data for a specific timeline, initiator, responder or service. Export reports to MS Excel, PDF or directly to a printer.

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 64 bit (SP2), Windows Server 64 bit (SP2), Windows Server 2008 SBS 64 bit (R2), Windows Server 2008 Standard 64 bit (R2).

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

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 Server dual-core CPU Intel processor, 4 GB RAM and 300 GB disk space.

Virtual Appliance

- Hypervisor: VMware ESX and ESXi
- Operation System Installed: Hardened SonicLinux
- Appliance Size: 250 GB, 950 GB
- Allocated Memory: 4 GB
- VMware Hardware Compatibility Guide: <http://www.vmware.com/resources/compatibility/search.php>

Supported Databases

External Databases: Microsoft SQL 2005 64 bit (SP2), Microsoft SQL 2008 64 bit (R2)
Bundled with the GMS application: MySQL

Internet Browsers

- Microsoft® Internet Explorer 8.0 or higher
- Mozilla Firefox 6.0 or higher
- Google Chrome 13.0 and above
- Supported only on Microsoft Windows platforms

Java

Java SE Runtime Environment 1.6 or later

GMS Gateway

SonicWALL SuperMassive™ E10000 Series, E-Class Network Security Appliance (NSA), NSA or PRO Series firewall with minimum firmware and SonicWALL VPN-based firewalls¹

Supported SonicWALL Appliances Managed by GMS

- SonicWALL Network Security appliances: SuperMassive E10000 Series, E-Class NSA, NSA, PRO, TZ Series appliances³
- SonicWALL Continuous Data Protection appliances
- SonicWALL Content Security Manager (CSM) appliances
- SonicWALL Secure Remote Access appliances: E-Class SRA and SRA for SMB
- SonicWALL Email Security appliances
- All TCP/IP and SNMP-enabled devices and applications for active monitoring

Supported Firmware

- SonicWALL SuperMassive E10000 Series: SonicOS Enhanced 5.0 or higher
- SonicWALL E-Class NSA and NSA: SonicOS Enhanced 5.0 or higher
- SonicWALL PRO Series: SonicOS Enhanced 3.2 or higher
- SonicWALL TZ Series: SonicOS Standard 3.1 or higher and Enhanced 3.2 or higher
- SonicWALL CDP: SonicWALL CDP 2.3 or higher
- SonicWALL CSM: SonicWALL 2.0 or higher
- SonicWALL SRA for SMB: Firmware 2.0 or higher
- SonicWALL Aventail E-Class SRA: Firmware 9.0 or higher⁴
- SonicWALL Email Security: SonicWALL Email Security 7.0 firmware

¹ In all instances SonicWALL GMS is running as a 32 bit application. Bundled databases will run in 64-bit mode on 64-bit Windows OS. ² 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. ³ Legacy SonicWALL XPRS/XPRS2, SonicWALL SOHO2, SonicWALL Tele2, and SonicWALL Pro/Pro-VX models are not supported. ⁴ Only newer Aventail E-Class SSL VPN appliances using 12 character hexadecimal serial numbers.



SonicWALL's line-up of dynamic security solutions

- 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



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™