

SonicWall Global Management System

Centralized policy management, monitoring and reporting

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

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

Simple policy configuration — 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 firmware updates on managed appliances to minimize service disruptions.

Streamlined license management — Simplifies appliance management via a unified console, and the management of security and support license subscriptions.

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

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

Benefits:

- Centralized security and network management
- Simplified policy configuration
- Sophisticated VPN deployment and configuration for simplifying connectivity and consolidating security policies
- Offline management
- Streamlined license management
- Universal dashboard for customizable, user-centric reporting
- Active-device monitoring and alerting for fast problem remediation
- SNMP support
- Intelligent reporting and activity visualization
- Centralized logging
- Real-time and historic next-generation syslog reporting
- Application traffic analytics for better insight into network activity and threats
- Real-time and historic data flow reporting
- Extensive cross-platform support
- Flexible deployment options
- Rich integration options

SNMP support — Provides powerful, real-time traps for all Transmission Control Protocol/Internet Protocol (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 — Provides comprehensive management and graphical reports for SonicWall firewall, anti-spam, backup and recovery and secure remote access devices. Enables 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. Also provides the ability to drill down into data and customize reports extensively.

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

Real-time and historic data flow reporting — Offers administrators an effective and efficient interface to visually monitor their network in real-time, providing the ability to identify applications and websites with high bandwidth demands, view application usage per user and anticipate attacks and threats encountered by the network.

Extensive cross-platform support — Provides coverage for all SonicWall products on the network.

Flexible deployment options — Optimize utilization, ease migration and reduce capital costs.

Rich integration options — Provide application programming interface (API) for web services, command line interface (CLI) support for the majority of functions and SNMP trap support for both service providers and enterprises.

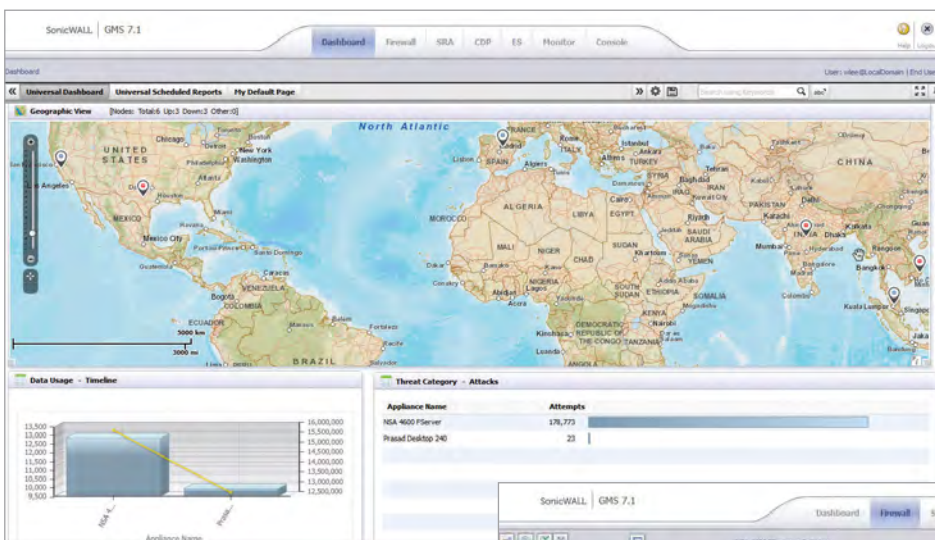
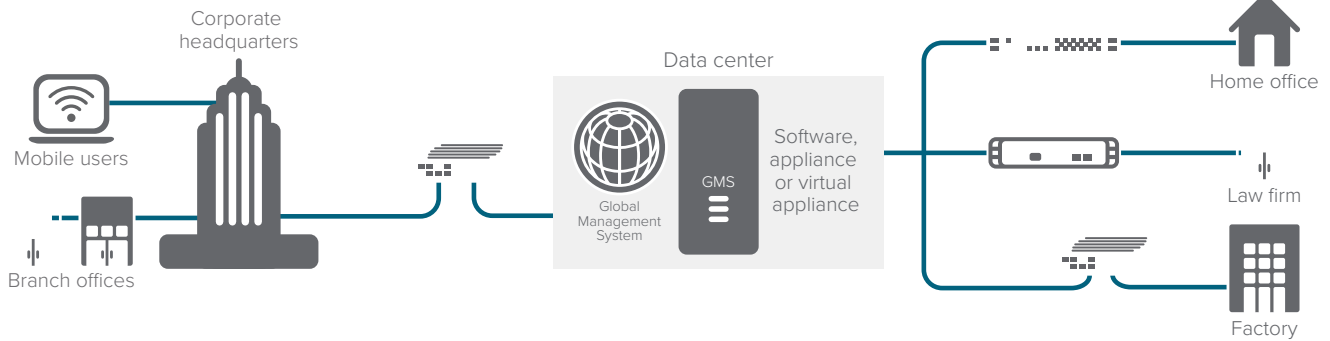
About Us

Over a 25 year history, SonicWall has been the industry's trusted security partner. From network security to access security to email security, SonicWall has continuously evolved its product portfolio, enabling organizations to innovate, accelerate and grow. With over a million security devices in almost 200 countries and territories worldwide, SonicWall enables its customers to confidently say yes to the future.



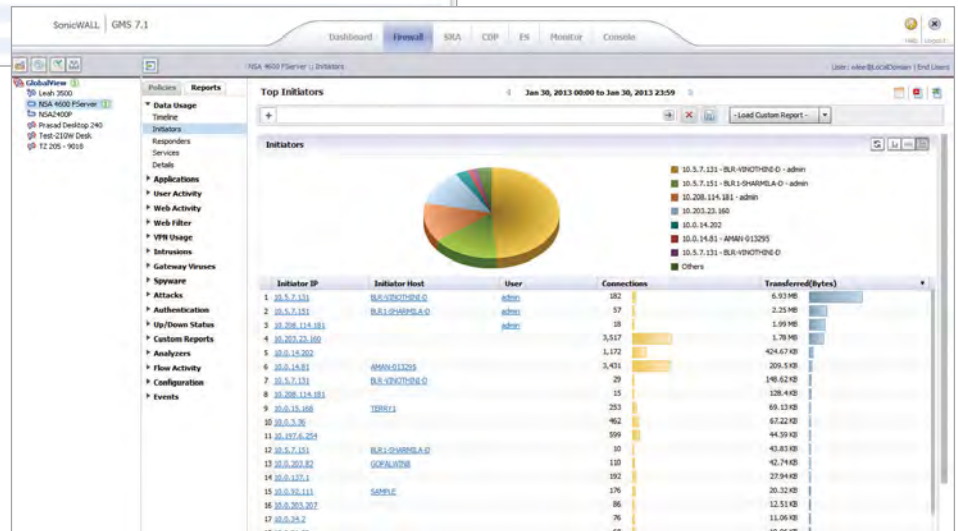
SonicWall Global Management System

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



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.

Intuitive graphical reports simplify managed appliance monitoring. Easily identify traffic anomalies based on usage data for a specific timeline, initiator, responder or service. Export reports to a Microsoft® Excel® spreadsheet, portable document format (PDF) file 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 system¹

Windows Server 2003 64 bit (SP2)
Windows Server 2008 SBS 64 bit (SP2)
Windows Server 2008 R2 Standard 64 bit (SP1)
Windows Server 2008 Standard 64 bit (SP2)

Hardware for single deployment

x86 Environment: Minimum 3 GHz processor server dual-core CPU Intel processor, 8 GB RAM (4 GB minimum) and 300 GB disk space.

Hardware for distributed server deployment

GMS server: x86 Environment: Minimum 3 GHz processor Server dual-core CPU Intel processor, 8 GB RAM (4 GB minimum) 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: 8 GB (4 GB minimum)

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 firewalls

Supported SonicWall appliances managed by GMS

SonicWall Network Security Appliances: SuperMassive E10000 Series, E-Class NSA, NSA, PRO, TZ Series appliances®

SonicWall Continuous Data Protection (CDP) appliances

SonicWall Content Security Manager (CSM) appliances

SonicWall Secure Remote Access (SRA) 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 higher³

SonicWall Email Security: SonicWall Email Security 7.0 firmware

IPv6 support

GMS 7.2 supports IPv6 management and configuration of firewalls, Domain Name System (DNS) and Neighbor Discovery Protocol (NDP).

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. In Virtual Appliance, GMS is running in 64-bit mode.

2 Legacy SonicWall XPRS/XPRS2, SonicWall SOHO2, SonicWall Tele2 and SonicWall Pro/Pro-VX models are not supported.

3 Only newer Aventail E-Class SSL VPN appliances using 12 character hexadecimal serial numbers.

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/en/products/GMS_Software.html#tab=purchase for an overview of support SKUs.

GMS Mobile is a free beta Apple® iPhone® application that administrators can use to remotely log in to their GMS system to check device status and review alerts as they come in.