



- **Zentrales Sicherheits- und Netzwerkmanagement**
- **Einfache Regeldefinition**
- **Effiziente VPN-Implementierung und -Konfiguration**
- **Offline-Verwaltung**
- **Effiziente Lizenzverwaltung**
- **Umfassendes Dashboard**
- **Aktive Überwachung von Geräten und Alarmierung**
- **SNMP-Unterstützung**
- **Intelligentes Reporting und Visualisierung der Benutzer-Aktivitäten**
- **Zentrales Logging**
- **Echtzeit- und historisches Next-Generation-Syslog-Reporting**
- **Analyse des Anwendungsverkehrs**
- **Umfassende plattformübergreifende Unterstützung**
- **Flexible Implementierung**
- **Vielfältige Integrationsmöglichkeiten**

In wachsenden, verteilten Netzwerken wird nicht nur die Verwaltung und Überwachung, sondern auch das Reporting immer komplexer und kostspieliger. Unternehmen müssen trotz beschränkter Budgets eine kontinuierliche Netzverfügbarkeit gewährleisten und strengen Auflagen nachkommen. Auch Service Provider stehen vor vielerlei Herausforderungen: Sie sind verpflichtet, Service Level Agreements (SLAs) für eine wachsende Zahl von Kundengeräten mit zunehmend komplexer Lizenzierung einzuhalten und müssen gleichzeitig ihre ROI (Return on Investment)-Zielvorgaben erfüllen. Ohne eine moderne Lösung zur Analyse des Anwendungsverkehrs und zur Erstellung von Syslog-Berichten haben Unternehmen keinen Einblick in wichtige Kennzahlen zur Bandbreitennutzung, Mitarbeiterproduktivität und zum Anwendungsverkehr. Für die effiziente Verwaltung Tausender von Anwendungen und Sicherheitsregeln benötigen Organisationen einfache und erschwingliche Verwaltungstools.

SonicWALL® Global Management System (GMS®) bietet Organisationen, Service-Anbietern und Unternehmen mit verteilten Netzwerken eine leistungsstarke und intuitive Lösung, mit der sich SonicWALL Firewall-, Anti-Spam-, Backup und Recovery-, Secure Remote Access Appliances zentral verwalten und schnell implementieren lassen. Darüber hinaus ermöglicht GMS eine zentralisierte Echtzeit-Überwachung sowie ein umfassendes Reporting zu Sicherheitsregeln und Compliance-Vorgaben. Enterprise-Kunden profitieren mit GMS von einer strafferen Verwaltung der Sicherheitsregeln, einer effizienteren Implementierung von Appliances und einem reduzierten Verwaltungsaufwand. Service Providern bietet GMS ein vereinfachtes Sicherheitsmanagement für mehrere Clients und zusätzliche Umsatzchancen. Durch die Bündelung von GMS-Lösungen profitieren Administratoren von mehr Redundanz und Skalierbarkeit. GMS lässt sich dabei flexibel als Software-, Hardware- oder Virtual Appliance-Lösung implementieren.

## Funktionen und Vorteile

### Zentrales Sicherheits- und Netzwerkmanagement.

Unterstützt Administratoren bei der Implementierung, Verwaltung und Überwachung einer verteilten Netzwerkkumgebung.

**Einfache Regeldefinition** für Tausende von SonicWALL Firewall-, Anti-Spam-, Backup und Recovery- sowie Secure Remote Access-Geräte von einer zentralen Stelle aus.

**Effiziente VPN-Implementierung und -Konfiguration.** Vereinfacht die Bereitstellung von VPN-Konnektivität und konsolidiert Tausende von Sicherheitsregeln.

**Offline-Verwaltung.** Ermöglicht zeitgesteuerte Konfigurationsarbeiten und/oder Firmware-Updates bei verwalteten Appliances, um Ausfallzeiten zu reduzieren.

Eine **effiziente Lizenzverwaltung** für SonicWALL Appliances über eine zentrale, einheitliche Konsole vereinfacht die Verwaltung von Security- und Support-Lizenz-Subskriptionen.

**Umfassendes Dashboard** mit personalisierbaren Widgets, geografischen Karten und benutzerorientierten Reporting-Funktionen.

**Aktive Überwachung von Geräten und Alarmierung.** Echtzeit-Alarme mit integrierten Überwachungsfunktionen ermöglichen es Administratoren, Präventivmaßnahmen zu ergreifen und eine umgehende Problembehebung zu veranlassen.

**SNMP-Unterstützung.** Bietet leistungsstarke Echtzeit-Traps für alle TCP/IP- und SNMP-Geräte und -Anwendungen. Damit lassen sich Fehler bei kritischen Ereignissen im Netzwerk schnell lokalisieren und beheben.

**Intelligentes Reporting und Visualisierung der Benutzer-Aktivitäten.** Bietet umfassende grafische Reports für SonicWALL Firewall-, Anti-Spam-, Backup und Recovery- sowie Secure Remote Access-Geräte. Administratoren erhalten so einen detaillierten Einblick in

die Nutzungstrends und Security-Events. Service Provider profitieren von einem einheitlichen Corporate Branding.

**Zentrales Logging.** Erlaubt eine zentrale Konsolidierung von Security-Events und -Protokollen für Tausende von Appliances. So können von einem zentralen Punkt aus forensische Netzwerkanalysen durchgeführt werden.

**Echtzeit- und historisches Next-Generation-Syslog-Reporting.** Bahnbrechende Verbesserungen der Architektur verkürzen den zeitaufwendigen Zusammenfassungsprozess, so dass Berichte über eingehende Syslog-Nachrichten nahezu in Echtzeit erstellt werden können. Außerdem lassen sich Daten per Drill-Down abrufen und Berichte umfassend personalisieren.

**Analyse des Anwendungsverkehrs.** Bietet Organisationen aussagekräftige Daten zum Anwendungsverkehr, zur Bandbreitennutzung und zu Sicherheitsbedrohungen. Gleichzeitig stehen leistungsstarke Troubleshooting- und Forensik-Funktionen zur Verfügung.

**Umfassende plattformübergreifende Unterstützung** für SonicWALL Firewall-, Anti-Spam-, Backup und Recovery- sowie Secure Remote Access-Plattformen gewährleistet die Abdeckung aller SonicWALL-Produkte im Netzwerk.

**Flexible Implementierung** in Form von Software, einer gehärteten High-Performance-Appliance oder als Virtual Appliance, um die Auslastung zu optimieren, Migrationen zu vereinfachen und Investitionskosten zu senken.

**Vielfältige Integrationsmöglichkeiten** wie z. B. eine API (Application Programming Interface)-Schnittstelle für Web Services, CLI-Unterstützung für die meisten Funktionen und SNMP Trap-Unterstützung für Service Provider und Unternehmen.

Technische Daten



SonicWALL Global Management System

GMS bietet Unternehmen und Service Providern eine umfassende Security-Management-Lösung.

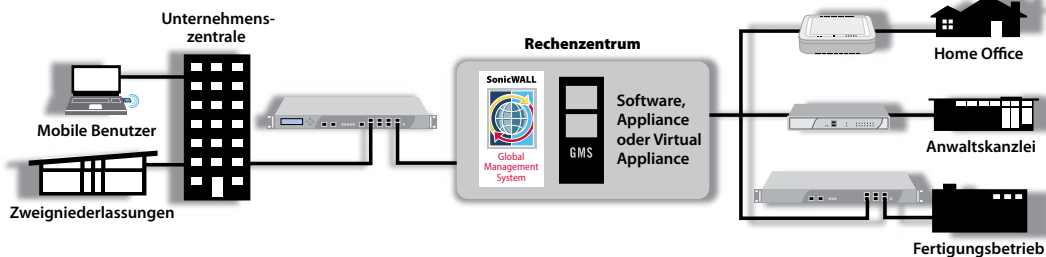
SonicWALL GMS Standard Edition

- SonicWALL GMS Software-Lizenz für 5 Nodes 01-SSC-7680
- SonicWALL GMS Software-Lizenz für 10 Nodes 01-SSC-3363
- SonicWALL GMS Software-Lizenz für 25 Nodes 01-SSC-3311
- SonicWALL GMS Software-Upgrade für 1 Node 01-SSC-7662
- SonicWALL GMS Software-Upgrade für 5 Nodes 01-SSC-3350
- SonicWALL GMS Software-Upgrade für 10 Nodes 01-SSC-7664
- SonicWALL GMS Software-Upgrade für 25 Nodes 01-SSC-3301
- SonicWALL GMS Software-Upgrade für 100 Nodes 01-SSC-3303
- SonicWALL GMS Software-Upgrade für 250 Nodes 01-SSC-3304
- SonicWALL GMS Software-Upgrade für 1.000 Nodes 01-SSC-3306

Unter [www.sonicwall.com/us/products/6030.html](http://www.sonicwall.com/us/products/6030.html) erhalten Sie einen Überblick über die Support-Artikelnummern.



Mit der kostenlosen Apple® iPhone®-Anwendung UMA EM5000 GMS Mobile (momentan als Beta-Software erhältlich) können sich Administratoren remote in das GMS-System einloggen und sich alle verwalteten Geräte anzeigen lassen, den Status von Geräten abfragen und zeitnah auf Warmmeldungen von GMS reagieren.



Kontextsensitive Dashboards bieten vielfältige informative Widgets, wie geografische Karten, Syslog-Berichte, Bandbreitenübersichten, Auflistungen der am häufigsten besuchten Websites oder der für bestimmte Benutzer relevantesten Daten.



Die Überwachung verwalteter SonicWALL Appliances wird dank der intuitiven grafischen Berichte zum Kinderspiel. Auffälligkeiten im Netzwerkverkehr lassen sich anhand der Nutzungsdaten für bestimmte Zeiträume, Aufrufer, Antwortstellen oder Services identifizieren. Die Berichte können anschließend in MS Excel oder PDF exportiert bzw. direkt am Drucker ausgegeben werden.

Mindestanforderungen an das System

Im nachfolgenden Abschnitt werden die Mindestanforderungen für SonicWALL GMS hinsichtlich Betriebssystem, Datenbanken, Treibern, Hardware sowie der von SonicWALL unterstützten Appliances aufgelistet:

Betriebssystem

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).

SonicWALL GMS wird dabei jeweils als 32-Bit-Anwendung ausgeführt.

Hardware für Einzelinstallationen

x86-Umgebung: Server mit mindestens 3-GHz-Dualcore-Intel Prozessor, 4 GB RAM und 300 GB Festplattenspeicher

Hardware für Installationen mit verteilten Servern

GMS-Server x86-Umgebung: Server mit mindestens 3-GHz-Dualcore-Intel Prozessor, 4 GB RAM und 300 GB Festplattenspeicher

Virtual Appliance

Hypervisor: VMware ESX und ESXi  
 Installiertes Betriebssystem Gehärtetes SonicLinux  
 Appliance-Kapazität: 250 GB, 950 GB  
 Zugewiesener Speicher: 4 GB  
 VMware-Kompatibilitätsrichtlinien für Hardware: <http://www.vmware.com/resources/compatibility/search.php>

Unterstützte Datenbanken

Externe Datenbanken: Microsoft SQL 2005 64 Bit (SP2), Microsoft SQL 2008 64 Bit (R2)

In GMS-Anwendung integriert: MySQL

Internet-Browser

Microsoft® Internet Explorer 8.0 oder höher  
 Mozilla Firefox 6.0 oder höher  
 Google Chrome 13.0 und höher  
 Nur auf Microsoft Windows-Plattformen unterstützt

Java

Java SE Runtime Environment 1.6 oder höher

GMS-Gateway

Firewalls der SonicWALL SuperMassive™ E10000-Serie, E-Class Network Security Appliance (NSA)-, NSA- oder PRO-Serie mit erforderlicher Firmware und SonicWALL VPN-basierten Firewalls<sup>1</sup>

Für die Verwaltung mit GMS unterstützte SonicWALL Appliances

SonicWALL Network Security Appliances: Appliances der SuperMassive E10000-Serie, E-Class NSA-, NSA-, PRO- und TZ-Serie<sup>3</sup>  
 SonicWALL Continuous Data Protection Appliances  
 SonicWALL Content Security Manager (CSM) Appliances  
 SonicWALL Secure Remote Access Appliances: E-Class SRA und SRA für KMUs  
 SonicWALL Email Security Appliances  
 Alle TCP/IP- und SNMP-Geräte und -Anwendungen für aktive Überwachung

Unterstützte Firmware

SonicWALL SuperMassive E10000-Serie: SonicOS Enhanced 5.0 oder höher  
 SonicWALL E-Class NSA und NSA: SonicOS Enhanced 5.0 oder höher  
 SonicWALL PRO-Serie: SonicOS Enhanced 3.2 oder höher  
 SonicWALL TZ-Serie: SonicOS Standard 3.1 oder höher und Enhanced 3.2 oder höher  
 SonicWALL CDP: SonicWALL CDP 2.3 oder höher  
 SonicWALL CSM: SonicWALL 2.0 oder höher  
 SonicWALL SRA für KMUs: Firmware 2.0 oder höher  
 SonicWALL Aventail E-Class SRA: Firmware 9.0 oder höher<sup>4</sup>  
 SonicWALL Email Security: SonicWALL Email Security 7.0-Firmware

<sup>1</sup> SonicWALL GMS wird dabei jeweils als 32-Bit-Anwendung ausgeführt. Integrierte Datenbanken laufen im 64-Bit-Modus auf 64-Bit-Windows-Betriebssystemen. <sup>2</sup> Bei der Option mit einem Management VPN Tunnel für die sichere Datenübertragung zwischen dem SonicWALL GMS-Server und den verwalteten Appliances (mithilfe von VPN-Tunneln) ist ein GMS-Gateway erforderlich. Als GMS-Gateway sollte mindestens eine SonicWALL NSA mit SonicOS Enhanced 5.0 oder höher bzw. eine SonicWALL PRO 2040 mit SonicOS Enhanced 3.2 oder höher eingesetzt werden. Wenn zur Verwaltung bestehende VPN-Tunnels oder HTTPS eingesetzt werden, ist kein GMS-Gateway erforderlich. <sup>3</sup> Bestehende SonicWALL XPRS/XPRS2-, SonicWALL SOHO2-, SonicWALL Tele2- und SonicWALL Pro/Pro-VX-Modelle werden nicht unterstützt. <sup>4</sup> Nur neuere Aventail E-Class SSL VPN Appliances mit 12-stelligen Seriennummern im Hexadezimalformat

SonicWALL-Lösungen für dynamische Sicherheit



**SonicWALL Deutschland**  
 Tel: +49 89 4545 946 [www.sonicwall.de](http://www.sonicwall.de)  
**SonicWALL Schweiz**  
 Tel: +41 44 810 31 35 [www.sonicwall.ch](http://www.sonicwall.ch)  
**SonicWALL Österreich**  
 Tel: +41 44 810 31 35 [www.sonicwall.at](http://www.sonicwall.at)



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™