



- **Gestione centralizzata della sicurezza e della rete**
- **Semplice configurazione delle policy**
- **Sofisticate funzioni di configurazione e implementazione per reti VPN**
- **Gestione offline**
- **Gestione semplificata delle licenze**
- **Dashboard universale**
- **Monitoraggio attivo dei dispositivi con allarmi**
- **Supporto SNMP**
- **Reporting intelligente e visualizzazione delle attività**
- **Logging centralizzato**
- **Report in tempo reale o storici basati su syslog di nuova generazione**
- **Analisi del traffico delle applicazioni**
- **Ampio supporto multi-piattaforma**
- **Implementazione flessibile**
- **Numerose opzioni d'integrazione**

Le reti sempre più distribuite geograficamente comportano maggiori costi e complessità a livello di gestione, reporting e monitoraggio. Le aziende devono inoltre garantire la continuità delle connessioni e rispettare severe normative nonostante i budget limitati. I provider di servizi devono rispettare gli accordi sui livelli di servizio (SLA) per un numero maggiore di dispositivi dei clienti con sistemi di licenza più complessi, il tutto senza perdere di vista gli obiettivi di ritorno sull'investimento. Senza uno strumento di nuova generazione per l'analisi del traffico applicativo e la creazione di report basati su messaggi syslog, le aziende non hanno una chiara visione dell'utilizzo della banda, del volume di traffico generato dalle applicazioni o della produttività dei dipendenti. Le aziende necessitano di strumenti di gestione semplici, convenienti e scalabili in funzione di migliaia di appliance e policy di sicurezza.

SonicWALL® Global Management System (GMS®) è una soluzione potente e intuitiva che consente a organizzazioni, aziende distribuite e service provider di gestire con estrema rapidità soluzioni firewall, anti-spam e dispositivi di backup/ripristino e accesso remoto sicuro SonicWALL da un'unica postazione centrale. GMS offre funzioni di monitoraggio centralizzato in tempo reale e report dettagliati sulle policy e sulla conformità alle normative. Per le aziende, GMS semplifica la gestione delle policy di sicurezza e l'implementazione delle appliance, riducendo l'impegno degli amministratori. Per i service provider, GMS semplifica la gestione della sicurezza per svariati client, generando ulteriori opportunità di guadagno. Gli amministratori possono raggruppare diverse soluzioni GMS in cluster per ottenere una maggiore ridondanza e scalabilità. Grazie alle opzioni di implementazione flessibile, GMS può essere utilizzato in versione software, hardware o come appliance virtuale.

### Caratteristiche e vantaggi

La **gestione centralizzata della sicurezza e della rete** aiuta gli amministratori ad implementare, gestire e monitorare un ambiente di rete distribuito.

Il **semplice configurazione delle policy** per migliaia di firewall, strumenti anti-spam e dispositivi di backup/recovery e accesso remoto sicuro SonicWALL da una postazione centralizzata.

Le **sofisticate funzioni di configurazione e implementazione per reti VPN** semplificano la creazione di connessioni VPN e consolidano migliaia di policy di sicurezza.

La **gestione offline** consente di pianificare le configurazioni e/o gli aggiornamenti del firmware per le appliance gestite, riducendo al minimo i tempi di fermo.

La **gestione semplificata delle licenze** per le appliance SonicWALL da un'unica console semplifica la gestione della sicurezza e dei servizi in abbonamento.

Il **dashboard universale** offre widget personalizzabili, mappe geografiche e report basati sugli utenti.

Il **monitoraggio attivo dei dispositivi con allarmi** in tempo reale semplifica la risoluzione dei problemi e permette agli amministratori di adottare misure preventive e reagire immediatamente in caso di anomalie.

Il **supporto SNMP** fornisce potenti notifiche (trap) in tempo reale per tutti i dispositivi basati su TCP/IP e SNMP, migliorando la risoluzione dei problemi grazie alla rapida identificazione e reazione agli eventi critici della rete.

Il **reporting intelligente e la visualizzazione delle attività** forniscono una visione completa e report grafici su firewall, anti-spam e dispositivi di backup/ripristino e accesso remoto sicuro di SonicWALL, offrendo maggiore visibilità su trend di utilizzo ed eventi relativi alla

sicurezza e rafforzando l'immagine di brand per i provider di servizi.

Il **logging centralizzato** fornisce un unico strumento centralizzato in cui consolidare gli eventi di sicurezza e i log di migliaia di appliance o effettuare analisi dettagliate sull'uso della rete.

Il **report in tempo reale o storici basati su syslog di nuova generazione** semplificano il laborioso processo di riepilogo dei dati grazie a una rivoluzionaria architettura ottimizzata, fornendo report quasi in tempo reale sui messaggi syslog in arrivo, con la possibilità di eseguire analisi drill-down dei dati e personalizzare i report.

Il **analisi del traffico delle applicazioni** offre alle aziende una visione chiara e dettagliata su traffico delle applicazioni, uso della larghezza di banda e minacce alla sicurezza, integrata da potenti funzioni di risoluzione dei problemi e analisi forense.

Il **ampio supporto multi-piattaforma** per firewall, strumenti anti-spam e dispositivi di backup/recovery e accesso remoto sicuro di SonicWALL è disponibile per tutti i prodotti SonicWALL collegati in rete.

Le opzioni di **implementazione flessibile** - come software, dispositivo hardware ad alte prestazioni o appliance virtuale - consentono di ottimizzare l'utilizzo, semplificare la migrazione e ridurre i costi di capitale.

Le **numerose opzioni d'integrazione** includono un'interfaccia di programmazione delle applicazioni (API), il supporto CLI per la maggior parte delle funzioni e il supporto per trap SNMP sia per aziende che per provider di servizi.

## Specifiche tecniche



## SonicWALL Global Management System

GMS è una soluzione completa di gestione della sicurezza per imprese e service provider

## SonicWALL GMS edizione Standard

SonicWALL GMS, licenza software per 5 nodi  
01-SSC-7680

SonicWALL GMS, licenza software per 10 nodi  
for 10 Nodes  
01-SSC-3363

SonicWALL GMS, licenza software per 25 nodi  
for 25 Nodes  
01-SSC-3311

SonicWALL GMS, upgrade software per 1 nodo  
01-SSC-7662

SonicWALL GMS, upgrade software per 5 nodi  
01-SSC-3350

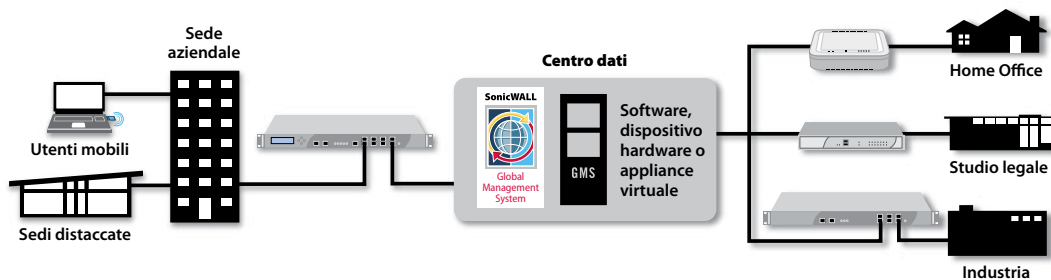
SonicWALL GMS, upgrade software per 10 nodi  
01-SSC-7664

SonicWALL GMS, upgrade software per 25 nodi  
01-SSC-3301

SonicWALL GMS, upgrade software per 100 nodi  
01-SSC-3303

SonicWALL GMS, upgrade software per 250 nodi  
01-SSC-3304

Per una panoramica dei prodotti supportati visitare il sito [www.sonicwall.com/us/products/6030.html](http://www.sonicwall.com/us/products/6030.html).



I dashboard sensibili al contesto visualizzano diversi widget informativi, come ad es. mappe geografiche, report basati su syslog, riepiloghi della larghezza di banda, siti Web più visitati oppure i dati più rilevanti per determinati utenti.



I report grafici intuitivi semplificano ulteriormente il monitoraggio delle appliance SonicWALL gestite. Eventuali anomalie del traffico sono facilmente rilevabili esaminando i dati di utilizzo in base a periodo di tempo, origine, destinazione o servizio. I report possono essere esportati in MS Excel o PDF o direttamente verso una stampante.

## Requisiti minimi di sistema

Di seguito sono riportati i requisiti minimi previsti per sistema operativo, database, driver e hardware, nonché le appliance SonicWALL supportate:

## Sistema operativo

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 tutti i casi descritti SonicWALL GMS funziona come applicazione a 32 bit.

## Hardware per impiego singolo

Ambiente x86: (minimo) processore server Intel con CPU dual-core da 3 GHz, 4 GB di RAM e 300 GB di spazio su disco.

## Hardware per impiego distribuito su server

Server GMS Ambiente x86: (minimo) processore server Intel con CPU dual-core da 3 GHz, 4 GB di RAM e 300 GB di spazio su disco.

## Appliance virtuale

Hypervisor: VMware ESX e ESXi

Sistema operativo installato: SonicLinux hardened

Dimensioni appliance: 250 GB, 950 GB

Memoria allocata: 4 GB

Guida alla compatibilità hardware per VMware: <http://www.vmware.com/resources/compatibility/search.php>

## Database supportati

Database esterni: Microsoft SQL 2005 64 bit (SP2), Microsoft SQL 2008 64 bit (R2)

In bundle con l'applicazione GMS: MySQL

## Browser

Microsoft® Internet Explorer 8.0 o successivo

Mozilla Firefox 6.0 o successivo

Google Chrome 13.0 e successivi

Supportato solo su piattaforme Microsoft Windows

## Java

Java SE Runtime Environment 1.6 o successivo

## Gateway GMS

Firewall delle serie SonicWALL SuperMassive™ E10000, E-Class NSA (Network Security Appliance), NSA o PRO con versione firmware minima e firewall SonicWALL basati su VPN<sup>1</sup>

## Appliance SonicWALL supportate e gestibili da GMS

Appliance di sicurezza di rete SonicWALL: appliance delle serie SuperMassive E10000, E-Class NSA, NSA, PRO, TZ<sup>2</sup>

Appliance SonicWALL Continuous Data Protection (CDP)

Appliance SonicWALL Content Security Manager (CSM)

Appliance SonicWALL Secure Remote Access (SRA): E-Class SRA e SRA per le PMI

Appliance SonicWALL Email Security

Tutti i dispositivi basati su TCP/IP e SNMP e applicazioni per il monitoraggio attivo

## Firmware supportato

Serie SonicWALL SuperMassive E10000: SonicOS Enhanced 5.0 o superiore

SonicWALL E-Class NSA e NSA: SonicOS Enhanced 5.0 o superiore

Serie SonicWALL PRO: SonicOS Enhanced 3.2 o superiore

Serie SonicWALL TZ: SonicOS Standard 3.1 o superiore e Enhanced 3.2 o superiore

SonicWALL CDP: SonicWALL CDP 2.3 o superiore

SonicWALL CSM: SonicWALL 2.0 o superiore

SonicWALL SRA per le PMI: firmware 2.0 o superiore

SonicWALL Aventail E-Class SRA: firmware 9.0 o superiore<sup>4</sup>

SonicWALL Email Security: firmware SonicWALL Email Security 7.0

<sup>1</sup> In tutti i casi descritti SonicWALL GMS funziona come applicazione a 32 bit. I database in bundle funzioneranno in modalità a 64 bit sui sistemi operativi Windows a 64 bit.

<sup>2</sup> Quando si utilizza l'opzione Management VPN Tunnel per la comunicazione sicura tra il server SonicWALL GMS e le appliance gestite tramite tunnel VPN, è necessario un gateway GMS. Il gateway GMS deve essere almeno un'appliance SonicWALL NSA (Network Security Appliance) con versione firmware min. SonicOS Enhanced 5.0 oppure un SonicWALL PRO 2040 con versione firmware min. SonicOS Enhanced 3.2. Il gateway GMS non è necessario se come metodo di gestione si utilizzano tunnel VPN esistenti o HTTPS. <sup>3</sup> I vecchi modelli SonicWALL XPRS/XPRES2, SonicWALL SOHO2, SonicWALL Tele2 e SonicWALL Pro/Pro-VX non sono supportati. <sup>4</sup> Solo nuove appliance Aventail E-Class SSL-VPN con numeri di serie a 12 cifre esadecimali.



UMA EM5000 GMS Mobile è un'applicazione gratuita per Apple® iPhone® (attualmente disponibile in versione beta), utilizzabile dagli amministratori per connettersi in mobilità al proprio sistema GMS e ottenere una panoramica di tutti i dispositivi gestiti, controllare lo stato dei dispositivi e analizzare gli allarmi GMS in tempo reale.



## Linea di soluzioni di sicurezza dinamica SonicWALL



SICUREZZA DI RETE



ACCESSO REMOTO SICURO



SICUREZZA WEB / E-MAIL



BACKUP E RECOVERY



GESTIONE BASATA SU POLICY

SonicWALL Italy  
T + 39.010.7407851  
Italy@sonicwall.com

Contatti Supporto SonicWALL  
[www.sonicwall.com/emea/4724.html](http://www.sonicwall.com/emea/4724.html)



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™