



- **Gestion centralisée de la sécurité et du réseau**
- **Configuration aisée des règles**
- **Configuration et déploiement VPN efficaces**
- **Gestion hors ligne**
- **Gestion rationalisée des licences**
- **Tableau de bord universel**
- **Système de surveillance active et d'alerte**
- **Prise en charge SNMP**
- **Outils intelligents de reporting et de visualisation des activités**
- **Journalisation centralisée**
- **Reporting syslog de nouvelle génération en temps réel et historique**
- **Analyse du trafic applicatif**
- **Prise en charge multiplateforme étendue**
- **Flexibilité de déploiement**
- **Nombreuses options d'intégration**

Au fur et à mesure que les réseaux s'agrandissent et se dispersent, la gestion, la surveillance et la génération de rapports deviennent de plus en plus complexes et coûteuses. Parallèlement, les entreprises doivent assurer une disponibilité permanente du réseau et se conformer à des réglementations strictes, avec des budgets de plus en plus restreints. Les fournisseurs de services doivent pour leur part respecter les accords de niveau de service (SLA) sur un nombre accru de dispositifs clients et gérer des licences plus complexes, sans perdre de vue les objectifs de retour sur investissement. Seules des fonctionnalités d'analyse du trafic et de génération de rapports syslog de nouvelle génération permettent de visualiser la consommation de bande passante, le trafic applicatif et la productivité des employés. Les entreprises ont besoin d'outils de gestion simples et économiques, capables de prendre en charge des milliers d'appliances et de règles de sécurité.

SonicWALL® Global Management System (GMS®) fournit aux entreprises, environnements distribués et fournisseurs de services un outil puissant et intuitif permettant une gestion centralisée et un déploiement rapide des solutions de pare-feu, d'anti-spam, de sauvegarde et récupération et d'accès distant sécurisé SonicWALL. GMS assure également une surveillance centralisée en temps réel des réseaux et fournit des rapports exhaustifs sur les règles de sécurité et normes de conformité. Pour les entreprises, SonicWALL GMS optimise la gestion des règles de sécurité et le déploiement des appliances, réduisant par là-même la charge administrative. Pour les fournisseurs de services, GMS simplifie la gestion de la sécurité de nombreux clients et crée des sources de revenus supplémentaires. Les administrateurs peuvent réunir des solutions GMS en cluster pour augmenter la redondance et l'évolutivité. GMS offre diverses options de déploiement, sous forme de logiciel ainsi que d'appliance matérielle ou virtuelle.

### Fonctionnalités et avantages

La **gestion centralisée de la sécurité et du réseau** aide les administrateurs à déployer, gérer et surveiller un environnement réseau distribué.

GMS assure une **configuration aisée des règles** pour des milliers de dispositifs de pare-feu, d'anti-spam, de sauvegarde et récupération et d'accès distant sécurisé SonicWALL, d'un seul et même endroit.

Des fonctionnalités de **configuration et de déploiement VPN efficaces** simplifient la mise en service de la connectivité VPN et consolident des milliers de règles de sécurité.

La **gestion hors ligne** permet de planifier les configurations et/ou les mises à jour sur les appliances gérées afin de réduire à un minimum les interruptions de service.

La **gestion rationalisée des licences** associées aux appliances SonicWALL depuis une console unique simplifie la gestion des abonnements aux licences de sécurité et de support.

Le **tableau de bord universel** réunit des widgets personnalisables, des cartes géographiques et des options de reporting relatives aux utilisateurs.

Le **système de surveillance active et d'alerte** émet des alertes en temps réel et comprend des options de surveillance intégrées qui simplifient le dépannage en permettant aux administrateurs de prendre des mesures préventives et de remédier immédiatement aux problèmes.

La **prise en charge SNMP** fournit de puissants « traps » en temps réel pour l'ensemble des dispositifs et applications TCP/IP et SNMP, qui optimisent l'identification des événements réseau critiques et la capacité à y répondre.

Les **outils intelligents de reporting et de visualisation des activités** permettent d'établir des rapports graphiques et de gestion complets sur les dispositifs de

pare-feu, d'anti-spam, de sauvegarde et récupération et d'accès distant sécurisé SonicWALL, de manière à offrir un meilleur aperçu des habitudes d'utilisation et des événements de sécurité. Les fournisseurs de services bénéficient pour leur part d'une identité de marque cohérente.

La **journalisation centralisée** rassemble en un endroit les événements de sécurité et les journaux de milliers d'appliances, permettant de réaliser des analyses forensiques du réseau à partir d'un seul et même point.

Grâce à des améliorations révolutionnaires au niveau de l'architecture, la fonctionnalité de **reporting syslog de nouvelle génération en temps réel et historique** simplifie le processus fastidieux de synthèse des données, permettant la génération en temps quasi réel de rapports sur les messages syslog entrants. Elle offre en outre la possibilité de zoomer sur les données ainsi que de nombreuses options de personnalisation des rapports.

L'**analyse du trafic applicatif** fournit des informations précieuses sur la consommation de bande passante, le trafic applicatif et les atteintes à la sécurité, tout en fournissant des services performants de dépannage et d'analyse forensique.

La **prise en charge multiplateforme étendue** des solutions de pare-feu, d'anti-spam, de sauvegarde et récupération et d'accès distant sécurisé SonicWALL permet de couvrir tous les produits SonicWALL installés sur un réseau.

Parmi les **nombreuses options d'intégration**, GMS comporte notamment une interface de programmation (API) de services Web, la prise en charge CLI pour la majorité des fonctions et la prise en charge de traps SNMP tant pour les fournisseurs de services que pour les entreprises.

## Spécifications



## SonicWALL Global Management System

GMS constitue une solution de gestion de la sécurité complète pour les entreprises et les fournisseurs de services.

## SonicWALL GMS Standard Edition

Licence logiciel SonicWALL GMS pour 5 nœuds  
01-SSC-7680

Licence logiciel SonicWALL GMS pour 10 nœuds  
01-SSC-3363

Licence logiciel SonicWALL GMS pour 25 nœuds  
01-SSC-3311

Mise à niveau logiciel SonicWALL GMS pour 1 nœud  
01-SSC-7662

Mise à niveau logiciel SonicWALL GMS pour 5 nœuds  
01-SSC-3350

Mise à niveau logiciel SonicWALL GMS pour 10 nœuds  
01-SSC-7664

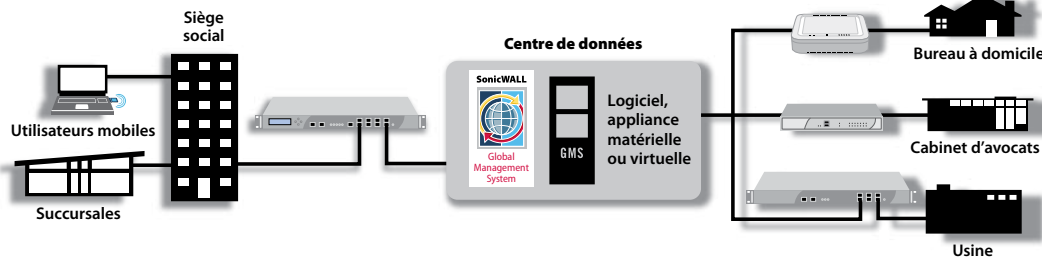
Mise à niveau logiciel SonicWALL GMS pour 25 nœuds  
01-SSC-3301

Mise à niveau logiciel SonicWALL GMS pour 100 nœuds  
01-SSC-3303

Mise à niveau logiciel SonicWALL GMS pour 250 nœuds  
01-SSC-3304

Mise à niveau logiciel SonicWALL GMS pour 1 000 nœuds  
01-SSC-3306

Vous trouvez un aperçu des références de support sur [www.sonicwall.com/us/products/6030.html](http://www.sonicwall.com/us/products/6030.html).



Les tableaux de bord contextuels affichent divers widgets informatifs : cartes géographiques, rapports syslog, synthèses de consommation de la bande passante, sites Internet les plus consultés ou données intéressantes concernant tels utilisateurs.



Surveillance aisée des appliances SonicWALL gérées grâce à des rapports graphiques intuitifs. Les anomalies de trafic sont facilement identifiées à partir des données d'utilisation selon un horaire particulier, l'auteur, le répondeur ou le service. Les rapports peuvent être exportés en fichier MS Excel ou PDF, ou être directement imprimés.

## Configuration minimum requise

Les configurations minimum requises pour SonicWALL GMS en ce qui concerne les systèmes d'exploitation, les bases de données, les pilotes, le matériel et les appliances SonicWALL prises en charge sont décrites ci-dessous :

## Système d'exploitation

Windows Server 2003 64 bits (SP2), Windows Server 64 bits (SP2), Windows Server 2008 SBS 64 bits (R2), Windows Server 2008 Standard 64 bits (R2).

Dans tous les cas, SonicWALL GMS fonctionne comme application 32 bits.

## Matériel pour un déploiement simple

Environnement x86 : serveur avec processeur Intel dual core 3 GHz minimum, 4 Go de mémoire vive et 300 Go d'espace disque.

## Matériel pour un déploiement de serveurs distribués

Serveur GMS Environnement x86 : serveur avec processeur Intel dual core 3 GHz minimum, 4 Go de mémoire vive et 300 Go d'espace disque.

## Appliance virtuelle

Hyperviseur : VMware ESX et ESXi

Système d'exploitation installé : SonicLinux renforcé

Taille de l'appliance : 250 Go, 950 Go

Mémoire allouée : 4 Go

Guide de compatibilité matérielle VMware : <http://www.vmware.com/resources/compatibility/search.php>

## Bases de données prises en charge

Bases de données externes : Microsoft SQL 2005 64 bits (SP2), Microsoft SQL 2008 64 bits (R2)

Inclus dans l'application GMS : MySQL

## Navigateurs Internet

Microsoft® Internet Explorer 8.0 ou version supérieure

Mozilla Firefox 6.0 ou version supérieure

Google Chrome 13.0 et plus

pris en charge uniquement sur les plates-formes Microsoft Windows

## Java

Java SE Runtime Environment 1.6 ou version ultérieure

## Passerelle GMS

Pare-feu série SonicWALL SuperMassive™ E10000, NSA E-Class, NSA ou PRO avec firmware minimum et pare-feu VPN SonicWALL<sup>1</sup>

## Appliances SonicWALL prises en charge pour la gestion avec GMS

Appliances de sécurité réseau SonicWALL : séries SuperMassive E10000, NSA E-Class, NSA, PRO et TZ<sup>2</sup>

Appliances de protection continue des données SonicWALL CDP

Appliances SonicWALL CSM (Content Security Manager)

Appliances SonicWALL SRA (Secure Remote Access) : SRA E-Class et SRA pour PME

Appliances SonicWALL Email Security

Tous les appareils et applications compatibles TCP/IP et SNMP pour la surveillance active

## Firmware pris en charge

Série SonicWALL SuperMassive E10000 : SonicOS Enhanced 5.0 ou version supérieure

NSA et NSA E-Class SonicWALL : SonicOS Enhanced 5.0 ou version supérieure

Série PRO SonicWALL : SonicOS Enhanced 3.2 ou version supérieure

Série TZ SonicWALL : SonicOS Standard 3.1 ou version supérieure et SonicOS Enhanced 3.2 ou version supérieure

CDP SonicWALL : SonicWALL CDP 2.3 ou version supérieure

CSM SonicWALL : SonicWALL 2.0 ou version supérieure

SRA SonicWALL pour PME : firmware 2.0 ou version supérieure

SRA E-Class SonicWALL Aventail : firmware 9.0 ou version supérieure<sup>4</sup>

SonicWALL Email Security : firmware SonicWALL Email Security 7.0

<sup>1</sup> Dans tous les cas, SonicWALL GMS fonctionne comme application 32 bits. Les bases de données incluses fonctionnent en mode 64 bits sur le système d'exploitation Windows 64 bits. <sup>2</sup> Une passerelle GMS est nécessaire en cas d'utilisation de l'option « Management VPN Tunnel » pour la sécurisation des communications entre le serveur SonicWALL GMS et les appliances gérées via des tunnels VPN. La passerelle GMS doit être au moins une NSA SonicWALL exécutant au minimum SonicOS Enhanced 5.0, ou une PRO 2040 SonicWALL exécutant au minimum SonicOS Enhanced 3.2. En cas d'utilisation de tunnels VPN existants ou de HTTPS comme méthode de gestion, le recours à une passerelle GMS n'est pas nécessaire. <sup>3</sup> Les anciens modèles SonicWALL XPRS/XPRS2, SonicWALL SOHO2, SonicWALL Tele2 et SonicWALL Pro/Pro-VX ne sont pas pris en charge. <sup>4</sup> Uniquement les appliances VPN SSL E-Class Aventail récentes utilisant des numéros de série de 12 caractères hexadécimaux.



UMA EM5000 GMS Mobile est une application Apple® iPhone® gratuite (actuellement disponible en logiciel bêta) utilisée par les administrateurs en déplacement pour se connecter à distance à leur système GMS et visualiser tous les dispositifs gérés, contrôler leur état et consulter les alertes GMS à leur réception.



## La gamme complète de solutions de sécurité dynamique SonicWALL



SÉCURITÉ RÉSEAU



ACCÈS DISTANT SÉCURISÉ



SÉCURISATION WEB ET DE MESSAGERIE



SAUVEGARDE ET RÉCUPÉRATION



GESTION ET RÈGLES

## SonicWALL France

T +33 1 49 33 73 19 France@sonicwall.com

## SonicWALL BeNeLux

T +32 (0) 15 280 985 Benelux@sonicwall.com

## Contacts du support SonicWALL

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



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™