SonicWall™ Global Management System (GMS) 8.4

Release Notes

September 2017

These release notes provide information about the SonicWall™ Global Management System (GMS) 8.4 release.

Topics:

About SonicWall GMS 8.4

SonicWall GMS 8.4 release provides new features and functionality, and fixes a number of known issues from previous releases. See New Features, Resolved Issues, and Known Issues sections.

SonicWall GMS can be used in a variety of roles in a wide range of networks. Network administrators can use SonicWall GMS in a Management Console role in an Enterprise network containing a single SonicWall NSA, TZ, or SuperMassive appliance and also in a Remote Management System role for managing multiple unit deployments for Enterprise and Service Provider networks consisting of hundreds and thousands of firewalls, Secure Mobile Access (SMA), and Email Security (ES) appliances.

New Features

This section describes the new features introduced in the GMS 8.4 release.

Topics:

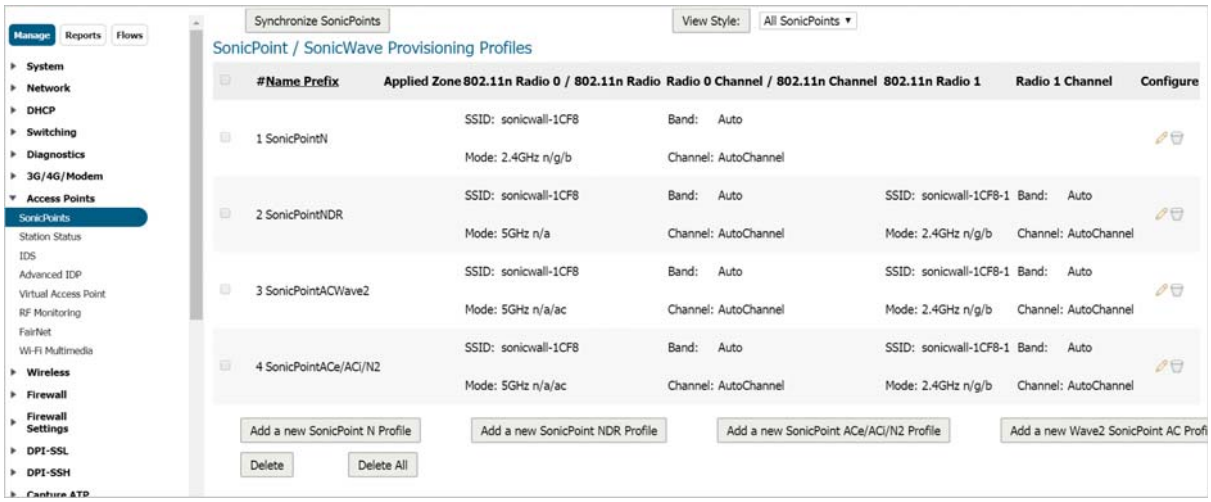
- Additional New Features
  - New E-CLI Commands Support
  - GRE Management Multicore Support
  - Restful API Support
  - Native Bridge Support
  - RADIUS Accounting Client Support
  - SSLVPN Concentrator and Authentication Cache
  - Bitmap Table Optimization
  - SWARM Service Enhancements
  - Advanced Flow Server
  - Granular ZebOS Debug Control in CLI
  - LiveDemo Support
  - OpenSSH 7.2 Support

SonicPoint Enhancements

These features provide the ability to show a series of SonicWave and SonicPoint devices in the tree control arena and provide more detailed reports and monitoring capabilities for each device type. Having SonicWave and SonicPoint device nodes represented in the tree control allows you to view anchor pages that provide information such as reporting data for the SonicWave and SonicPoint devices, location tracking (using a floor plan), as well as show you the network topology. These features provide you with a user-friendly interface where you can view details about your SonicWave and SonicPoint devices that were otherwise hidden inside SonicOS screens.

Access Points > SonicPoints

These features appear for units after SonicWave and SonicPoint devices have been connected to them.

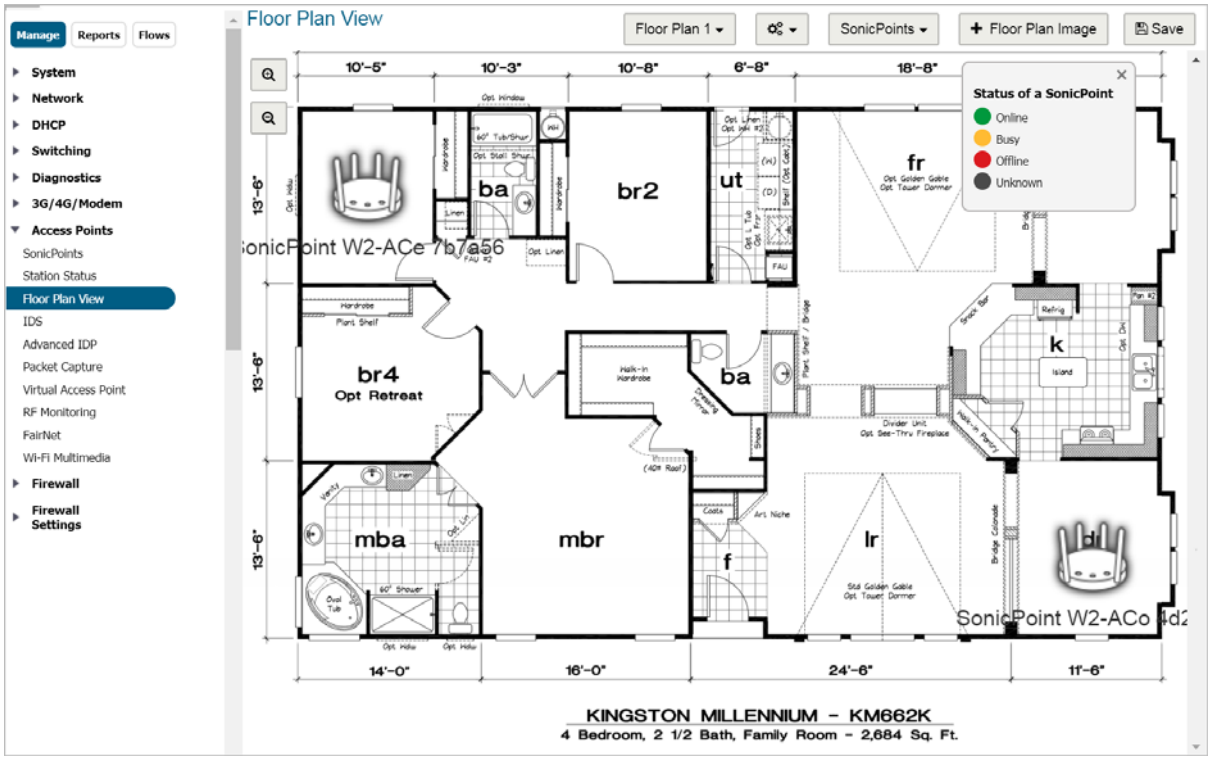


Access Points > Floor Plan View

Floor Plan View in the GMS user interface allows for a more visual approach to managing large numbers of SonicWave and SonicPoint devices. You can also track physical location and real-time status.

The Floor Plan View (FPV) is an add-on to the existing wireless access point management suite in GMS that provides a real-time picture of the actual wireless radio deployment environment of your wireless network and improves your ability to estimate the wireless coverage of new deployments. The FPV also provides the single-pane-of-glass console to be able to check access point statistics, monitor access point real-time status, configure access points, remove access points and even show the access point RF coverage from the consolidated the context menu.

The figure that follows shows a sample of a typical Floor Plan View.



In the FPV, the following colors indicate the status of an access point:

Color	Status	Definition
Green	Online	Access point is in an operational state.
Red	Offline	Access point is in initialization or non-responsive state.
Yellow	Busy	Firmware synchronization or configuration provisioning and scanning is in progress on the access point.

You can also save and export your Floor Plan View as a JPEG, PNG, or PDF. Click the **Settings** icon at the top right side of the window and click **Export as**... Select the file type you would like to use to export. The file downloads to your local drive.

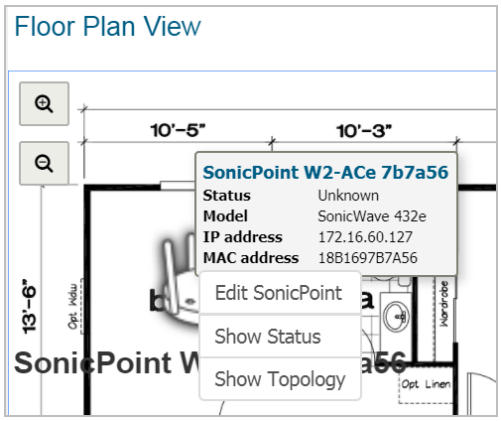
Network Topology

This feature allows you to visualize the network topology behind one or more firewalls managed within the GMS system. The system draws the topology by learning from the configuration on the firewall dynamically, and builds a network diagram which is easy for you to view and understand.

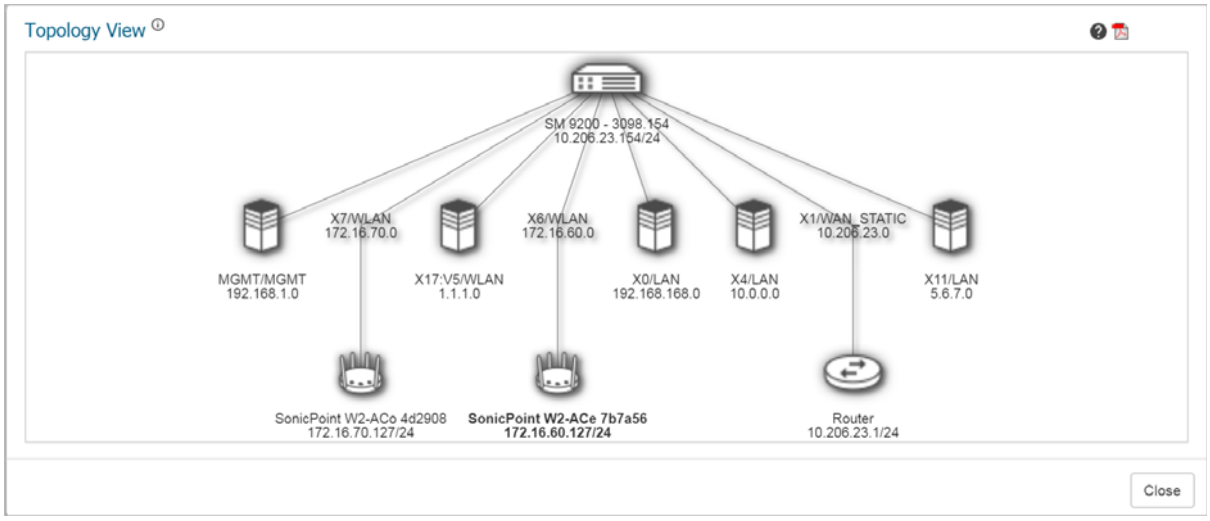
SonicWave and SonicPoint devices can be managed by in topology view, which can present the network topology from GMS to the SonicWave and SonicPoint device endpoints. The SonicWave and SonicPoint device real-time status can be monitored, and the context-menu can provide SonicWave and SonicPoint device configuration options as well.

This feature shows the logical relationship between devices among all WLAN-related devices, and allows managing the devices directly in the Topology View. To see the Topology view, under **Access Points > Floor Plan**

View. The Context Menu is accessible by right-clicking on the SonicWave or SonicPoint device (top ellipse) icons as shown below:



Select **Show Topology**. When the page opens, a tree-like diagram is shown by connecting devices known to GMS and shows their relationship similar to the following figure:



Topology View provides a graphic presentation of the WLAN network for administrators with the most often used information and status. The devices are drawn as nodes on a tree and the tree is zoomable with the mouse and mouse wheel. Information shown in the tree includes the device type, IP address, interface connected to, name, number of clients, and a simulated LED light on certain device that shows the working status. A Tooltip bubble shows detailed information on each device.

Network Topology Attributes

Attributes include:

- **Route Objects**: Source and destination networks, gateways, and interfaces used.
- **Interfaces**: Allows you to know your device's networks. This interface provides information like how many SonicWave and SonicPoint devices are connected to the device.
- **ARP entries**: For Ethernet addresses or MAC addresses from an IPv4 address.
- **SonicPoints**: SonicWave and SonicPoint devices in the network that can be identified.
- **VAP**: Indicates configurations that use virtual interfaces that in turn use some zones.
- **VPN**: SAs and others.

Support for SonicOS 6.2.7.7 and SuperMassive 9800

Review the SonicOS 6.2.7.7 Release Notes for complete information on the additional SuperMassive 9800 feature support.

Support for SonicOS 6.2.9

Review the SonicOS 6.2.9 Release Notes for complete information on the additional feature support.

Support for Windows Server 2016

Support for Microsoft Windows Server 2016 has been added including the Japanese language variant. Windows Server 2012 is also still supported.

Support for VMware ESXi 6.5

Support for VMware ESXi 6.5 has been added. ESXi 6.0 and 5.5 are also still supported.

Support for SonicOS 6.5

Review the SonicOS 6.5 Release Notes for complete information on the additional feature support.

Resolved Issues

The following is a list of issues addressed in this release.

Appliance

Resolved Issue	Issue ID
Enabling the complete backup schedule (such as by day) cannot be updated or customized. Occurs when the day is set back to Sunday, irrespective of any other changes to the day.	189443
Scheduled GMS backup does not function correctly. Occurs when attempting to schedule a backup using the GMS backup tool.	187264

CLI

Resolved Issue	Issue ID
Incorrect values are applied when modifying MAC address objects using the GMS CLI. Occurs when customers attempt to update the MAC address object values for a Group of firewalls using the GMS CLI.	190595
Creating FQDN Address objects fail using the GMS CLI. Occurs when attempting to create or update FQDN Address objects on a group of firewalls using the GMS CLI.	190593

Console Panel

Resolved Issue	Issue ID
Updates fail and invalid input messages appear. Occurs while testing Active Directory users within a domain.	189614

Firewall Configuration

Resolved Issue	Issue ID
Modifying Address Objects at the Group level does not function correctly. Occurs when modifying the Address Object name at the Group level and getting an 'Internal server policy' error because of a `NullPointer` exception.	192985
Certain interfaces do not appear in GMS when using the SonicOS 6.2.5.1-25n firmware. Occurs because of a corrupt password using the `iface_l2tp_shared_secret` command.	184969

Firmware Upgrade

Resolved Issue	Issue ID
The upgrade firewall firmware fails when using 'Local file.' Occurs when attempting to upgrade the firewall firmware from GMS using the file from a local computer.	185410

Net Monitor

Resolved Issue	Issue ID
The UI does not load correctly with two possible reasons: the certificate has expired (happened after Sep 2, 2017) or because of a class file not found error (`ClassNotFoundError`). Click **Details** on the error screen to examine the reason (or both). Occurs because of a corruption in the class file of the monitor jar.	192136
The Net Monitor screen fails to load properly and returns a Java exception. Occurs when using Internet Explorer.	189551

Policies Panel

Resolved Issue	Issue ID
Fail to create or update CFS objects using GMS. Occurs when attempting to create or modify CFS Objects or Profiles using GMS.	190591
Modification of a NAT64 policy creates duplicate NAT policies. Occurs when the inbound interface is changed from Any to X0.	189319
Reverse inheritance from an appliance with a NAT64 policy does not inherit the Pref64 address objects at the group level.	188917
GMS shows redundant drop-down list entries. Occurs when using Inbound and outbound interfaces.	188882
Comment modification causes failures in GMS but is successful in the appliance. Occurs when modifying comments in a NAT64 policy.	188881
Tasks fail to enable/disable access rules on the firewall when using GMS. Occurs when attempting to update the firewall access rule settings using GMS.	188310

Policies Panel (Continued)

Resolved Issue	Issue ID
The inheritance preview screen is blank. Occurs when attempting to inherit settings that contain special characters for the Geo-IP screen.	187878
No option to create a prefs backup for TZ units when using GMS. Occurs when attempting to do a backup of the TZ unit using GMS under **Firewall > Policies > Register/Upgrades**.	187595
Changes are not being properly submitted for AccessRule changes. Occurs when attempting to update the firewall Access Rules using GMS.	187223
The Group tab and VPN Access configurations are not being properly applied to inherited users. Occurs when attempting to inherit firewall local user settings using GMS.	185227
New local users are being added with Expired Account Lifetimes to the firewall. Occurs when attempting to modify the firewall's local user settings with GMS at the Group level.	185225
In the group level, the maximum URL cache can be set at 7680. But while doing Fwd inheritance to unit with a NSA3600, the task creation itself fails because the NSA3600 expects a cache in the range of 25600-51200.	185084
Incorrect data in the User Name/User Password fields return an 'Update Failed: invalid input' error message. Occurs when using special characters as part of the name or password.	185030
Adding SonicWall Auto Provisioning Server/Client using certificates returns an incorrect error message requiring the user to enter a Shared Secret. Occurs when selecting the Certificate option on the General tab of **Policies > VPN > Configure**.	185028
ACL Enforcement settings of VAP are not visible in the GUI. Occurs when the ACL enforcement settings of the firewall VAP of are not in sync with GMS.	184910
An error message displays in **View > Logs**. Occurs when the deletion of Dynamic Ranges fails.	184791
The addition of an IPv6 dynamic range causes a failure in **Policies > DHCP**. Occurs when working within the firewall.	184788
The VLANs tab of **Policies > Network > Portshield Groups**, still shows the VLAN Trunk as Disabled in the GMS UI. Occurs after enabling the VLAN Trunk option from the drop-down menu.	184652
Under **Polices > Log > Categories**, the "Report Events via Syslog" option cannot be disabled. Occurs when an event profile contains multiple values.	184087
Policies > Firewall Settings > Advanced > Jumbo Frame support is not available in GMS 8.3. Occurs when comparing the features of GMS with the firewall user interface.	183672
Forward inheritance for External switch configuration functions correctly, but the Console log message indicates the task has failed. Occurs when the group level support for switch configuration is removed.	183530
The Update button does not function correctly in the Edit window of the **Policies > Logs > Categories** screen. Occurs when editing the main Log Categories.	183429
Incorrect settings are applied to DPI-SSL Content Filter Category Inclusions/Exclusions in GMS. Occurs when applying configuration settings at the group level.	182907

Reporting

Resolved Issue	Issue ID
Group level reports do not show correct data. Occurs at the Group level that only show data for one Group and should not show any group level Analyzer data.	192674
The group level intrusion reports are not correct. Occurs when comparing group level intrusion summary reports for two groups.	190319
Scheduled reports are returned blank for firewall service subscriptions. Occurs when attempting to generate a Scheduled report from GMS using the firewall subscription services.	188452
Web Activity report shows no data. Occurs when checking the Web Activity report for the firewall and it shows no data because the Content filter has been disabled.	186295

SonicPoint

Resolved Issue	Issue ID
VAP settings do not appear at the Group level in GMS. Occurs when you go to **Wireless > Virtual Access Point** to update settings at the Group level.	188459

Tree Control

Resolved Issue	Issue ID
The right-click on a device feature in TreeControl does not function correctly. Occurs after upgrading to Firefox version 52.	184797

Universal Schedule

Resolved Issue	Issue ID
GMS superadmin users are not able to modify all Scheduled reports. Occurs when Scheduled reports are being added by other users.	188105
Select flow reports do not appear in the PDF of the USR. Occurs when adding USR.	184992

Workflow

Resolved Issue	Issue ID
Unable to modify address objects using GMS with Workflow enabled. Occurs when the change order is created, but no tasks are being created.	189243

Known Issues

The following is a list of issues known to exist at the time of the GMS 8.4 release.

Console Panel

Known Issue	Issue ID
Tenant web services APIs are shown in the web services status page. Tenant web services APIs are always shown in the web services status page. These APIs should be hidden for on-premise installations. Technically there are no tenant concepts in on-premise cases.	191744
Viewing the Disk Space Utilization status alert shows the Threshold as “unknown.” Occurs only with the Disk Space Utilization Status alert that is available in the Console panel.	191735

Event Management

Known Issue	Issue ID
Email alerts do not appear when a tunnel goes down or is recovering. Occurs on a smaller set of customer bases, where there is a corner case of traps getting lost or are not being processed by the monitoring manager service. A restart of the service keeps them going until the next time the service (specifically the trap manager thread) stalls.	191386

GMS

Known Issue	Issue ID
Performing a firmware upgrade on the unit while using the **Login To Unit** feature of GMS fails. Occurs when using the **Login To unit** feature, not while directly logging in to the firewall through a separate window.	191868

Policies Panel

Known Issue	Issue ID
In the SSOagent/Terminal service agent/Radius accounting client, the screens are still displaying the Partition column. Occurs when the authentication partitions are disabled.	192971
The FloorPlan view reveals there are no SonicPoints present even after they have been added. Occurs during the MSSQL setup.	192960
The **Enable Link State Propagation** checkbox should be removed from the VLAN Interface Settings page. Occurs for the WAN zone interface when the IP assignment selected in the “wire mode (2 port wire)” and the wire mode type is “Bypass (via internal switch/relay).”	192958
Adding a VLAN interface in the Wired mode should only display VLAN interfaces that are not configured.	192942
The User Accounting section is not available at the unit or group levels. The support for this feature is not present in 8.4, but will be available in a subsequent release.	191311
The forward and reverse inheritance features do not function correctly. Occurs when trying to apply Group membership or VPN Access settings to Local Users.	185227
Task creation for Forward Inheritance is not functioning correctly. Occurs when a range mismatch for the maximum URL cache range exists.	185084

Policies Panel (Continued)

Known Issue	Issue ID
Forward Inheritance a the group level is not functioning correctly for **Policies > Capture ATP > Settings**. Occurs when adding new address objects to exclude from Capture ATP.	183968
The Inheritance preview of a Route Policy does not list dependent address objects. Occurs during the Inheritance task execution.	183910
Deleting or modifying a Network Monitor Profile does not function correctly. Occurs at the Group level for firmware released earlier than 6.2.6.	183901
The **OK** button does not function correctly for the “Client CF Enforcement list” and “Excluded from Client CF Enforcement List” options in **Policies > Security Services > Client CF Enforcement**. Occurs when editing a Client CF Enforcement list.	183761
The Forward Inheritance feature for an external switch configuration appears to be functioning correctly, but the **Console > Log > View Log** message indicates the task has failed. Occurs after successfully adding and then deleting a switch from the group unit.	183530

Reports Panel

Known Issue	Issue ID
The Unit Details in **Flows > General > Status** are blank. Occurs when accessing the expected Unit Details data.	184238

Summarizer

Known Issue	Issue ID
Unit Up/Down emails start appearing in your Inbox at a fixed time daily as per the schedule, once the Optimization begins. Occurs only during the Optimization window.	191353

Universal Schedule

Known Issue	Issue ID
Select added reports do not appear in the Universal Scheduled Report PDF. Occurs when adding Universal Scheduled Reports.	184992

Workflow

Known Issue	Issue ID
In **Policies > Flow Activity > External Collector**, the color does not change to yellow when modifying System Logs. Occurs when choosing a reporting format.	183918
Text box color codes are not implemented for changes to the Maximum Rule Count in Access Rules. Occurs when editing and approving the maximum rule count.	183908

Platform Compatibility

The SonicWall GMS 8.4 release can be hosted in two deployment scenarios as follows:

- Microsoft Windows Server Software
- VMware ESXi Virtual Appliance

Deployment Considerations:

- Before selecting a platform to use for your GMS deployment, use the Capacity Calculator. This helps you set up the correct GMS system for your deployment.

CAUTION: SonicWall recommends that you take steps to minimize abrupt shutdowns of the server hosting GMS, as this can cause corruption of the Reporting database, potentially leading to loss of data for the current month. A possible solution includes using an Uninterrupted Power Supply (UPS).

Before installing GMS 8.4, ensure that your system meets the minimum hardware and software requirements described in the following sections:

Supported Platforms

The SonicWall GMS supports the following Microsoft Windows operating systems:

- Windows Server 2016 (English and Japanese language versions)
- Windows Server 2012 Standard 64-bit
- Windows Server 2012 R2 Standard 64-bit (English and Japanese language versions)
- Windows Server 2012 R2 Datacenter

These Windows systems can either run in physical standalone hardware platforms, or as a Windows Server virtual machine over Hyper-V or ESXi.

TIP: For best performance and scalability, it is recommended to use a 64-bit Windows operating system. Bundled databases run in 64-bit mode on 64-bit Windows operating systems. All listed operating systems are supported in both virtualized and non-virtualized environments. In a Hyper-V virtualized environment, Windows Server is a guest operating system running on Hyper-V. GMS is then installed on the Windows Server virtual machine that is layered over Hyper-V.

NOTE: GMS is not supported on MS-Windows Server virtual machines running in cloud services, such as Microsoft Azure and Amazon Web Services EC2.

Unsupported Platforms

The following platforms have been dropped from support:

- CDP management and reporting
- UMA EM5000 as part of the GMS deployment
- Windows 32-bit as part of the GMS deployment
- Firewalls with firmware older than SonicOS 5.0
- Gen4 or older Firewalls

Hardware Requirements

Use the Capacity Calculator to determine the hardware requirements for your deployment.

NOTE: A Windows 64-bit operating system with at least 16GB of RAM is highly recommended for better performance of reporting modules. For more information, read the "Capacity Planning and Performance Tuning" appendix in the *SonicWall GMS Administration Guide*.

Hard Drive HDD Specifications

The following hard drive HDD specifications are required when using GMS Software on Windows Server or a GMS Virtual Appliance:

Hardware Requirements

Requirement	Details
Spindle Speed	10,000 RPM or higher
Cache	64 MB or higher
Transfer rate	600 MBs or higher
Average latency	4 microseconds or lower

GMS Virtual Appliance Supported Platforms

The elements of basic VMware structure must be implemented prior to deploying the SonicWall GMS Virtual Appliance. The GMS Virtual Appliance runs on the following VMware platforms:

- ESXi 6.5, 6.0, and 5.5

  NOTE: For fresh installations of GMS 8.4 VM, ESXi 6.5 is required.

Virtual Appliance Deployment Requirements

Consider the following before deploying the GMS Virtual Appliance:

- GMS management is not supported on Apple MacOS.
- All modules are 64-bit.
- Using the Flow Server Agent role requires a minimum of:
  - Quad Core
  - 16GB of memory
  - 300GB available disk space

Use the Capacity Calculator to determine the hardware requirements for your deployment.

The performance of GMS Virtual Appliance depends on the underlying hardware. It is highly recommended to dedicate all the resources that are allocated to the Virtual Appliance, especially the hard-disk (datastore). In environments with high volumes of syslogs or AppFlow (IPFIX), you will need to dedicate local datastores to the GMS Virtual Appliance.

Read the "Capacity Planning and Performance Tuning" appendix in the *SonicWall GMS Administration Guide*.

Browser Requirements

SonicWall GMS uses advanced browser technologies such as HTML5, which are supported in most recent browsers. SonicWall recommends using the latest Chrome, Firefox, Internet Explorer, or Safari browsers for administration of the SonicWall GMS.

This release supports the following Web browsers:

- Chrome 42.0 or higher (recommended browser for dashboard real-time graphics display)
- Firefox 37.0 or higher
- Internet Explorer 11.0 or higher (do not use compatibility mode)

NOTE: Internet Explorer version 10.0 in Metro interfaces of Windows 8 is not currently supported.

NOTE: Turn off Compatibility Mode when accessing the GMS management interface with Internet Explorer. For more information, see the Knowledge Base article located at: https://support.sonicwall.com/sonicwall-gms/kb/sw14003

Mobile device browsers are not recommended for SonicWall GMS system administration.

NOTE: If using Chrome version 42 and newer to access GMS 7.2 and older, you will need to enable NPAPI support in Chrome, which by default has been disabled starting with version 42.

Microsoft SQL Server Requirements

The following SQL Server versions are supported:

- SQL Server 2014
- SQL Server 2012

NOTE: For SQL Server deployments in countries in which English is not the default language, set the default language to English in the Login Properties of the GMS database user in the SQL Server configuration.

NOTE: A database user with "DB Creator" privileges must be provided to GMS during the Role Configuration process of any GMS Server.

Java Support

NOTE: Java is required only when you are using Net Monitor.

Download and install the latest version of the Java 8 plug-in on any system that accesses the GMS management interface. This can be downloaded from:

www.java.com

or

http://www.oracle.com/technetwork/java/javase/downloads/index.html

SonicWall Appliances Supported for GMS Management

NOTE: GMS 8.4 does not support legacy SonicWall appliances, including:

- Firewall appliances running firmware earlier than SonicOS 5.0
- CSM Series
- CDP Series

SonicWall GMS 8.4 supports the following SonicWall appliances and firmware versions:

Component Requirements

SonicWall Platforms	SonicWall Firmware Version
Network Security Appliance	
SuperMassive 10000 Series	SonicOS 6.0 or newer **NOTE**: Only partial policy management and reporting support is currently available. The following SuperMassive specific features are not supported for centralized policy management in GMS: • Multi-blade Comprehensive Anti-Spam Service (CASS) • High Availability/Clustering • Support for Management Interface • Flow Reporting Configurations • Multi-blade VPN • Advanced Switching • Restart: SonicOS versus Chassis Contact your SonicWall Sales representative through https://support.sonicwall.com/ for more information.
SuperMassive 9000 Series	SonicOS 6.1 or newer
NSA Series	SonicOS 5.0 or newer
TZ Series and TZ Wireless	SonicOS 5.0 or newer
SonicWall SOHO and SOHO Wireless	SonicOS 6.2.6 or newer
Email Security/Anti-Spam	
Email Security Series	Email Security 7.2 or newer (management only)
Secure Mobile Access	
SMA 6200/7200	SMA 10.7.2 or newer
SRA/SSL-VPN Series	SSL-VPN 2.0 or newer (management) SSL-VPN 2.1 or newer (management and reporting)
E-Class SRA Series	E-Class SRA 9.0 or newer

Notes:

- GMS 8.4 supports SonicWall firewall App Control policy management and App Control reporting support. Refer to the SonicOS documentation for information on the supported SonicOS firmware versions.
- Appliances running firmware newer than this GMS release can still be managed and reports can still be generated. However, the new features in the firmware will be supported in an upcoming release of GMS.

Non-SonicWall Appliance Support

SonicWall GMS provides monitoring support for non-SonicWall TCP/IP and SNMP-enabled devices and applications.

Upgrading to GMS 8.4

This section provides procedures for upgrading an existing SonicWall GMS 8.3 or newer installation to GMS 8.4.

See the associated Knowledge Base articles #213012 and #213411 at https://support.sonicwall.com/sonicwall-gms/kb for more information.

GMS can be configured for a single server or in a distributed environment on multiple servers. GMS 8.4 can be installed as a fresh install or as an upgrade from GMS 8.3. If you wish to perform a fresh install of GMS 8.4, refer to the *GMS Getting Started Guide* that relates to your GMS deployment.

Consider the following before upgrading to GMS 8.4:

- You must disable the User Account Control (UAC) feature on Windows before running the GMS installer. In addition, disable Windows Firewall or your personal firewall before running this installer.
- For appliances under management using a GMS Management Tunnel or Existing Tunnel, make sure that HTTPS management is allowed from the GMS servers. This is because GMS 8.4 logs into the appliances using HTTPS only.
- The scheduled reports created in GMS 8.0 continue to work properly after upgrading to 8.4. However, the Legacy reports created in GMS 6.0 or earlier versions are not migrated. For more information on viewing legacy reports, refer to the *GMS Administration Guide*.
- When performing a fresh installation of GMS on Windows, the installer prompts for an IPv6 address of the server if it detects an IPv6 network.

In a distributed environment, shut down all GMS servers except the one that is running the database. GMS servers with the **SonicWall Universal Management Suite - Database** service should be upgraded first, and then you can upgrade the other servers. You must upgrade all GMS servers in your deployment to the same version of GMS. You cannot have some servers running version 8.4 and others running 8.3.

NOTE: DO NOT start/stop the SonicWall Universal Management Suite - Database service manually, before or after upgrading to 8.4. After the upgrade, the **SonicWall Universal Management Suite – Database** service will be down until the MySQL upgrade process has completed as well. Login to the /appliance UI to track the progress.

Upgrading Procedure

To upgrade to GMS 8.4, complete the following steps:

1. Navigate to www.mysonicwall.com.
2. Download the GMS 8.4 software.
3. After the files have downloaded, double-click the first file and follow the onscreen instructions. The Installer detects any previous installations of GMS. Click **Install** to proceed with the installation.
4. If you see a Windows Security Alert for Java, click **Unblock**. The installer displays a progress bar as the files are installed. Wait a few minutes for the installer to finish installing.
5. After the files are installed, whether or not the system has a Personal Firewall such as Windows Firewall enabled, a dialog is displayed notifying you to either disable the firewall or manually open the syslog and SNMP ports, and to ensure that these ports are open on your network gateway or firewall if you plan to

use HTTPS Management mode for managing remote appliances (instead of GMS Management Tunnel or Existing Tunnel modes). Click **OK**. Be sure to adjust the settings as recommended.

6 After the installer has completed, reboot the system to complete the installation.

Prerequisite Requirements for Deploying a GMS 8.4 Virtual Appliance on VMware ESXi

With ESXi 6.5, to protect an ESXi host against unauthorized intrusion and misuse, VMware imposes constraints on several parameters, settings, and activities.

One of the security features that impacts the deployment of GMS 8.4 appliance is:

For increased security, SHA-256 with the PKCS#1 RSA encryption signature algorithm is used for the default certificates in both:

- SonicWall GMS 8.4 Virtual Appliance firmware
- VMware ESXi 6.5

This means that new deployments of GMS 8.4 can only be deployed on servers running VMware ESXi 6.5 or higher. However, upgrades from GMS 8.3 to GMS 8.4 are supported on servers running earlier versions of ESXi.

Installing GMS 8.4 on VMware ESXi

For brand new deployments of GMS 8.4:

1 GMS 8.4 “Fresh Install” OVA

2 Minimum VMware version required is ESXi 6.5

For upgrades of existing GMS Virtual Appliances from 8.3 to 8.4:

1 Download or access to 8.3 OVA and 8.3 SP1 binaries

2 Check **Console > Diagnostics > Summarizer** for agent health information. This verification helps determine if there is a need to add an agent.

Installation procedures:

1 Upgrade all GMS console agents to 8.4 using the 8.4 “VA Upgrade” .OVA file.

2 Deployment is now running 8.4

To add a new virtual appliance GMS agent server, to a GMS distributed deployment, there are two options:

- Option i: Upgrade the ESXi server to 6.5. Add the 8.4 agent and follow normal procedures to add to the deployment.
- Option ii: Maintain an ESXi server at its current level. You will have to use the GMS 8.3 .OVA fresh Install file to add the GMS agent, then, upgrade the agent to 8.4 and follow normal procedures to add it to the distributed deployment.

Upgrading the GMS Virtual Appliance

This section provides procedures for upgrading an existing SonicWall GMS 8.3 virtual appliance or newer installation to GMS 8.4 virtual appliance.

See the associated Knowledge Base articles #213012 and #213411 at https://support.sonicwall.com/sonicwall-gms/kb for more information.

In a distributed environment, shut down all GMS servers except the one that is running the database. GMS servers with the SonicWall Universal Management Suite - Database service should be upgraded first, and then you can upgrade the other servers. You must upgrade all GMS servers in your deployment to the same version of GMS. You cannot have some servers running version 8.4 and others running 8.3.

NOTE: DO NOT start/stop the SonicWall Universal Management Suite - Database service manually, before or after upgrading to 8.4. After the upgrade, the SonicWall Universal Management Suite – Database service will be down until the MySQL upgrade process has completed as well. Login to the /appliance UI to track the progress.

For a fresh install of the GMS 8.4 64-bit Virtual Appliance, refer to the *GMS Virtual Appliance Getting Started Guide*.

To upgrade, complete the following:

1. Download the GMS 8.4 file from www.mysonicwall.com to your workstation software: **sw_gmsvp_vm_eng_8.4.xxxx.yyyy.gmsvp-updater.64bit.sh**
2. Log in to the /appliance (System) interface of the GMS server.
3. Navigate to the **System > Settings** page.
4. Click **Browse**, navigate to the location where you saved the above files, and select the first necessary file.
5. Click **Apply** to begin the firmware upgrade installation.
6. The Virtual Appliance reboots at the end of the installation process.

Product Licensing

SonicWall network security appliances must be registered on MySonicWall to enable full functionality and the benefits of SonicWall security services, firmware updates, and technical support. Log in or register for a MySonicWall account at https://mysonicwall.com.

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract and to customers who have trial versions.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View video tutorials
- Access MySonicWall
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT NOTE, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Last updated: 9/28/17

232-001333-00 Rev A