

SonicWall® Global Management System 9.3

Release Notes

October 2020

These release notes provide information about the SonicWall® Global Management System (GMS) 9.3 release.

Topics:

- [About SonicWall GMS 9.3](#)
- [System Requirements](#)
- [Resolved Issues](#)
- [Known Issues](#)
- [Product Licensing](#)
- [SonicWall Support](#)

About SonicWall GMS 9.3

SonicWall GMS 9.3 release provides new features and functionality, and fixes a number of known issues from previous releases. Refer to [Resolved Issues](#) for additional information.

SonicWall GMS 9.3 is a Web-based application that can configure and manage multiple SonicWall appliances and monitor non-SonicWall appliances from a central location. GMS can be used in a variety of roles in a wide range of networks. Network administrators can use GMS in a Management Console role in a network containing a single SonicWall firewall or an enterprise-level network comprised of many firewalls.

GMS 9.3 is easy to install and configure. You can add appliances to GMS management and then monitor the system using the Intelligent Platform Monitor (IPM) functionality.

GMS 9.3 can be deployed either as a single server deployment or as a distributed deployment. You can upgrade from GMS versions 8.7 or 9.2 to version 9.3 or perform a fresh installation of GMS 9.3. Upgrades are described in this document. To install a new GMS configuration, upgrade to GMS 9.3, refer to the *GMS 9.3 Getting Started Guide*.

System Requirements

For syslog-based deployments, you can also use the Capacity Planning Tool at <https://www.sonicwall.com/en-us/products/firewalls/management-and-reporting/global-management-system> to determine the specific hardware requirements for your deployment.

System Requirement	Minimum Requirements
SonicWall GMS Virtual Appliance	<ul style="list-style-type: none">• A CPU greater than quad core level• 16 GB RAM (more is recommended for increased performance)• 40 GB, 250 GB, or 950 GB available disk space (depending on number of devices)• thick provisioning <p>NOTE: GMS is not supported as a VMware virtual machine running in a cloud service, such as Amazon Web Services EC2.</p>
Hard Drive	<ul style="list-style-type: none">• Spindle Speed: 10,000 RPM or higher• Cache: 64 MB or higher• Transfer rate: 600 MBs or higher• Average Latency: 4 microseconds or lower
Java	<ul style="list-style-type: none">• Java 8.0 plug-in
Browser	<ul style="list-style-type: none">• Google Chrome 42.0 and higher (recommended browser for dashboard real-time graphics display)• Mozilla Firefox 37.0 and higher• Microsoft Edge 41 or higher• Microsoft Internet Explorer 10.0 and higher <p>NOTE: Internet Explorer version 10.0 in Metro interfaces of Windows 8 is currently not supported.</p> <p>NOTE: When using Internet Explorer, turn off Compatibility Mode when accessing the GMS management interface.</p> <p>NOTE: Internet Explorer is not supported for Angular-based flow reports.</p>
Network	<ul style="list-style-type: none">• access to the Internet• either:<ul style="list-style-type: none">• an IP address automatically assigned through DHCP• a static IP address

SonicWall Appliances Supported for GMS Management

- i** **NOTE:** GMS 9.3 does not support legacy SonicWall appliances, including:
- Firewall appliances running firmware earlier than SonicOS 5.0
 - CSM Series
 - CDP Series

SonicWall GMS 9.3 supports the following SonicWall appliances and firmware versions:

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: <ul style="list-style-type: none">• 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://sonicwall.com/support 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
SOHO	SonicOS 5.9.1.3 or newer 5.9 versions
SOHO Wireless	SonicOS 6.2.6 or newer
SOHO 250 and 250 Wireless	SonicOS 6.5.4.1 or newer
Email Security/Anti-Spam	
Email Security Series	Email Security 7.2 or newer (management only)
Secure Mobile Access	
SMA 1000 Series	SMA 10.7.2 or newer
SMA/SRA/SSL-VPN Series	SSL-VPN 2.0 or newer (management) SSL-VPN 2.1 or newer (management and reporting)

Notes:

- GMS 9.3 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.

GMS Virtual Appliance Supported Platforms

SonicWall GMS 9.3 can be installed as a virtual appliance. The elements of basic VMware structure must be implemented prior to deploying the SonicWall GMS Virtual Appliance. The GMS Virtual Appliance runs on the VMware ESXi 6.5 platform.

Non-SonicWall Appliance Support

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

Resolved Issues

The following issues are resolved in this release.

Resolved Issue	Issue ID
After navigating to Management > Policy Panel > Log Settings the Auditing Records page is missing.	MAR-22122
On a system that has been updated from GMS 8.7 to 9.3, adding units with the reporting option set to Syslog/Disabled makes the few flow related tabs in the various panel look like they are loading data.	MAR-21955
Invalid IPS settings are seen when previewing settings to be applied by forwarding an inheritance task.	MAR-21784
The checkbox to enable authentication partitioning is visible for GEN7 TZ 470w in GMS but it is unsupported in the UTM.	MAR-21723
When a Workflow Change Audit report is requested and opened, the initial description under the section title refers to Network Traffic instead of the changes that he is pulling in the report.	MAR-21624
The customer is unable to view IPv4 access rules under the Group level on the GMS 8.7 for WAN to WAN access rule.	MAR-21530
Multiple issues for Scheduled Reports were identified.	MAR-19170
On the appliances added under GMS, Random Address objects are chosen under exclusion.	MAR-17502
Web Server crashes nearly every day.	MAR-13620
Units that were acquired through Zero Touch were showing as down.	MAR-13007
The MySonicWall synchronization task fails with the error Register/Update unit with MySonicWall.com .	MAR-12971
Web Service crashes intermittently on the Console server	MAR-11756
Scheduled reports page numbers don't match up.	MAR-11602
Multiple Unit Locally Changed alerts are sent for some devices managed by GMS .	MAR-11158
GMS does not show HA active status icon when the firewall is connected to a SonicPoint access point.	MAR-10132
While trying to configured the firewall access rule, all the rules from various zones, except the default zones, cannot be seen on the firewall.	MAR-9913
On GMS 8.7 systems, customers are unable to modify or delete any user added with an underscore (_) in the username.	MAR-9864
Client is unable to dynamically adjust column width on the main GMS displays for both 9.x and 8.7 versions.	MAR-9767
The Update Manager service is intermittently failing and the preferences backup tasks are not being created.	MAR-9581
The log analyzer page does not display properly when showing page 3 and later.	MAR-5852
Scheduled reports are running at the wrong time.	MAR-5542

Additional References

The following ticket numbers indicate resolved tickets that were opened by customers:

MAR-22138, MAR-21784, MAR-21624, MAR-21597, MAR-21595, MAR-21530, MAR-20609, MAR-17502, MAR-17192, MAR-16657, MAR-16555, MAR-15728, MAR-14877, MAR-14701, MAR-14588, MAR-14059, MAR-13620, MAR-456, MAR-13135, MAR-13134, MAR-13010, MAR-13007, MAR-12971, MAR-12308, MAR-12283, MAR-12046, MAR-11819, MAR-11756, MAR-11753, MAR-11653, MAR-11602, MAR-11342, MAR-11158, MAR-10553, MAR-10389, MAR-10382, MAR-10358, MAR-10136, MAR-9915

MAR-9913, MAR-9864, MAR9767, MAR-9581, MAR-9582, MAR-9501, MAR-9138, MAR-8539, MAR-8470, MAR-8353, MAR-8275, MAR-8214, MAR-7367, MAR-6193, MAR-5852, MAR-5542, MAR-4898, and MAR-4774.

Known Issues

The following is a list of issues known to exist at the time of the GMS 9.3 release.

Known Issue	Issue ID
When configuring VLAN on Interfaces page, an error is seen in Group level. The same configuration can be done in the unit and in the firewall.	MAR-22381
The Switch Controller cannot reboot the switch via GMS interface (via the Physical View > VLAN View).	MAR-22369
Switch Controller >Physical View > Add Switch : Not able to add the switch manually. The following error appears in the logs: Task execution failure: Add New Extended Switch: SWS14-48 (PoE Alert Usage Threshold configured on the Extended Switch: Data is incorrectly formatted: PoE Traps configured on the Extended Switch: Data is incorrectly formatted: PoE Power Limit Mode configured on the Extended Switch.	MAR-22348
The Syslog Report list is not available while creating Scheduled Reports.	MAR-22295
The External IDS page is showing that licensing is required even though it is licensed and synchronized with MySonicWall. If license is not done, the External IDS page itself does not appear, and after several synchronization, it still shows as not licensed. However, on the UTM we can see it as licensed and available. In Group level the configuration shows a successful commit and configurations are pushed to the UTM.	MAR-22238
The VLAN cannot be configure on the switch interface using the Switch Controller > Overview page.	MAR-22150
Management Policy Panel > Security Services > Client AV Enforcement : This page is missing subcategories for Enable Alert Message from Firewalls to Capture Client Endpoint Devices . These subcategories are present in the firewalls but is missing in GMS.	MAR-22134
Multiple options are missing while creating the interface tunnel for IPv6.	MAR-22028
Capture ATP Connectivity Test shows as Failed in GMS, while it succeeds in UTM.	MAR-21895
Client AV enforcement is showing as not licensed in GMS, even when verified on the devices.	MAR-21893
When using LDAP to retrieve user group information, the page is missing the Settings icon which is used to navigate to LDAP for configuration in User settings.	MAR-21871
Download this entry for Dynamic external objects fails and shows the error Download Dynamic Group Data for NewFTP1 .	MAR-21845
The Management mode is defined as Manual even when the device is added in ZT mode.	MAR-21673
Navigating to Physical View of the Switch Controller throws error No switches found . When this occurs, make sure you are connected to the network and/or that the firewall is reachable.	MAR-18928
On clicking the Edit button, the entries of a switch user should show its actual value. By design the current password is not fetched to the screen for security reasons.	MAR-14962

Product Licensing

The SonicWall GMS Virtual Appliance comes with a base license to manage either 5, 10, or 25 nodes. You can purchase additional licenses on MySonicWall. For more information on licensing additional nodes, visit: <https://www.sonicwall.com/en-us/support/contact-support/licensing-assistance>.

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.

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 and participate in the Community forum discussions at <https://community.sonicwall.com/technology-and-support>.
- 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>.

About This Document

Legend



NOTE: A NOTE icon indicates supporting information.



IMPORTANT: An IMPORTANT icon indicates supporting information that may need a little extra attention.



TIP: A TIP indicates helpful information.



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



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

GMS Release Notes
Updated - November 2020
Software Version - 9.3
232-005540-00 Rev A

Copyright © 2020 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit <https://www.sonicwall.com/legal>.