SonicWall® Global Management System 9.0

Release Notes

January 2018

These release notes provide information about the SonicWall® Global Management System (GMS) 9.0 release.

Topics:

About SonicWall GMS 9.0

SonicWall GMS 9.0 release provides a new look and interface, new features and functionality, and fixes a number of known issues. See the New Features section.

GMS 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 an Enterprise network containing a single SonicWall NSA, TZ, or SuperMassive appliance.

GMS 9.0 is easy to install and configure. You can easily add appliances to GMS management, then use the Intelligent Platform Monitor (IPM) functionality for easy monitoring and management.

GMS can be configured for a single server deployment. It cannot be configured as a distributed deployment. GMS 9.0 must be installed as a fresh installation. You cannot upgrade to 9.0 from a previous version of GMS. To perform a fresh installation of GMS 9.0, refer to the *GMS 9.0 Virtual Appliance Getting Started Guide*.

System Requirements

You can also use the Capacity Calculator to determine the specific hardware requirements for your deployment.

System Requirement	Minimum Requirements
SonicWall GMS Virtual Appliance	• A CPU greater than quad core level • 16 GB RAM (more is recommended for increased performance) • 250 or 900 GB available disk space (depending on number of devices) • thick provisioning **NOTE:** GMS is not supported as a VMware virtual machine running in a cloud service, such as Amazon Web Services EC2.
Hard Drive	• **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	• Java 8.0 plug-in
Browser	• Google Chrome 42.0 and higher (recommended browser for dashboard real-time graphics display) • Mozilla Firefox 37.0 and higher • Microsoft Internet Explorer 10.0 and higher **NOTE:** Internet Explorer version 10.0 in Metro interfaces of Windows 8 is currently not supported. **NOTE:** When using Internet Explorer, turn off Compatibility Mode when accessing the GMS management interface. **NOTE:** Internet Explorer is not supported for Angular-based flow reports.
Network	• access to the Internet • either: • an IP address automatically assigned through DHCP • a static IP address
SonicWall Appliance and Firmware	• SonicOS 6.2 and higher

GMS Virtual Appliance Supported Platforms

SonicWall GMS 9.0 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 following VMware platforms:

- ESXi 6.5, 6.0 and 5.5

Non-SonicWall Appliance Support

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

New Features

This section indicates or describes the new features introduced in the GMS 9.0 release. All the new features in GMS 9.0 promote ease of installation and configuration, make it easier to add devices, and easier to monitor and manage them.

Topics:

- GMS User Interface Enhancements
- Simplified Installation Processes
- Policy Control from Flow Reporting and Analytics
- Add Unit Operation Status
- Intelligent Platform Monitoring and Reporting Module
- Flow-based Reporting

GMS User Interface Enhancements

Some GMS 9.0 menu items have been rearranged for a better user experience. Most of the changes are self-explanatory for those familiar with GMS 8.x.

At the top level, GMS 9.0 now shows five available views:

1. Home – This view is for the reporting dashboard and summary (only in flow-based installations)
2. Manage – This view is for managing or configuring units.
3. Reports – This view is used for detailed reporting (syslog and flow-based reporting)
4. Analytics – This view is available only for flow-based reporting
5. Notifications – In GMS 8.X, the Notification panel was shown in the Monitor view only.

Left navigation shows two views:

1. Left tree control – This view is for managing units and grouping them for reporting and management. This view is not available for the Console, Appliance, and Notifications views.
2. Middle pane – Contents of this depends on the top level items.

The right section reveals three views:

1. Drop-down menu – This is to choose the type of units to be displayed under the left tree control. You can select Firewall, Email Sec, or SMA device.
2. The right gear icon is for the Console view.
3. Left-side LEDs: Refer to the IPM section for more information.

Simplified Installation Processes

Improvements have been made to automate procedures that streamline and simplify the installation process.

Policy Control from Flow Reporting and Analytics

Policy Control provides the ability to create and manage policies from the Flow reporting screens. You can create application rules for multiple applications within the Application report.

To create an application rule:

1. Select the required applications from the Application Report page and click **Configure Policy**.
2. Select the required action from the Configure Policy modal and create the rule.

A task is created that allows you to immediately execute the following actions:

1. Adding new matching objects.
2. Adding Application Rules that perform user-selected action items.

Add Unit Operation Status

The **Manage | Current Status > System Status** screen provides a step-by-step update on the unit's status from the time when the unit was added to the time when the unit is acquired and operational. The status update, in addition to making sure you are aware of where you stand during the unit's acquisition, also prevents you from using the unit while the acquisition (for management and for reporting) is still in process.

Acquisition History

- GMS has the ability to show history of the acquisition processes.
- You can track all steps and understand the status at each level. Each status includes a timestamp.
- This section is available at all times, accessible with a click of a button from the **System Status** screen.

Steps include:

1. **Unit Setup**
    - Configuration accepted: Connect with your MySonicWall account and retrieve the unit's details (licenses and so on).
    - Setting up your device's parameters in GMS.
    - After your license is retrieved: The device is licensed for management and reporting.
2. **Unit Acquisition**
    - Connect to the unit through HTTPS.
        - Connect only when an IP address is specified in add unit. Wait for the unit to communicate with GMS, and if waiting for a heartbeat message, make sure the unit is configured to point to GMS. Then go to the unit's UI and enable management by GMS.
    - Communication with the unit is successful.
        - GMS synchronizes with the unit.
    - Unit reboot required when the product code is not identified.
        - This usually happens with new firewalls. GMS detects this and notifies you.
    - The acquisition is successful. The unit is ready for management by GMS.
3. **Reporting and Analytics Setup**
    - Verifying that the unit is licensed for reporting and analytics.
        - Setting up the reporting infrastructure.
    - The unit reboots in order to enable IPFIX-based flow reporting from the unit.
    - The unit is ready for operation.
        - Dashboard and report data could take up to 15 minutes to appear. Check Live Monitor to review the health of the unit.

4 **Finished**

- After the unit is successfully deployed through GMS. You can manage, view reports, dashboard data, analytics, and schedule reports.
- Click **Done** to exit the screen.

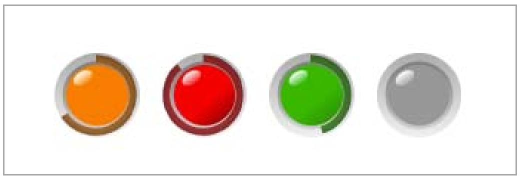
Intelligent Platform Monitoring and Reporting Module

GMS 9.0 adds monitoring tools to view the CPU, memory, and disk usage in real time and provides historical views of the system resource usage. It also automatically adapts to the available resources.

Visualization

There are four different states that the LED indicators located at the top right of the screen can display:

⬜	Initial State	The LED indicator appears gray to indicate that the IPM monitoring system has not yet received any metric information of the represented resource.
🟩	Normal State	When the represented resource utilization (%) is below the specified warning threshold, the LED indicator reflects the Normal State in green.
🟧	Warning State	When the represented resource utilization (%) is above the specified warning threshold but below the critical threshold, the LED indicator reflects the Warning State in amber color.
🟥	Critical State	When the represented resource utilization (%) is above the specified critical threshold, the LED indicator reflects the Critical State in red color.



NOTE: Flow-based setup does not allow you to add more than two or three appliances in a 250 GB flow-based installation. IPM escalates the system to the Critical State and prevents you from attempting to add more appliances. More capacity can be added through external mount, if needed to avoid the capacity limitation. More appliances can be added to 950 GB system.

Monitoring

Monitoring includes CPU usage, memory usage, and disk usage, as well as an indication of the overall system state using estimated capacity LEDs.

Estimated capacity LEDs are different from other regular resource LEDs. They do not represent a resource, but are used for presenting the system capacity allocation – a reservation or allocation status of all the monitored resources. Each managed appliance in a GMS system reserves or allocates a predefined amount of resource. So the estimated capacity LED/Informative Tooltip reflects the current resource capacity allocation status and informs you when a planned allocated resource capacity is beyond the defined thresholds. The following are the estimated capacity LED specific fields:

- **Allocated Resources** – lists the current allocated capacity (in percentage) for every resource currently monitored by IPM
- **Max. Allocation** – The highest value among the current list of allocated resources.
- **Acquired Firewalls** – the number of firewalls currently tracked by IPM for the estimated capacity allocation.

Control

You can control under what conditions the LEDs can take the green, orange or red states. These conditions can be configured from the appliance view. This view is available under **Appliance > IPM > Settings**.

The Threshold Settings screen provides you with the ability to tune the ideal threshold values for different severities (Medium - warning; High - critical) for every resource with a slider UI component.

When you adjust a threshold value, both the adjusted value and the **Apply** button are highlighted to inform you to confirm and apply your changes. The **Reset** button reverts the threshold value back to the last saved value.

Real-time Monitoring

Real-time monitoring of system usage can be viewed under **Appliance > IPM > Monitor**.

Historical Data

Historical data of system usage can be viewed under **Appliance > IPM > History**.

Failures

When any of the LEDs turn into a state other than normal, the corresponding controls kick in.

- **Warning State**: The Add Unit action is not available. The + icon from the tree control tool bar, the Add Unit… menu item, and the Import XML… menu item are hidden.
- **Critical State**: When the system is in the Critical State, this dialog blocks the whole content area. Although the dialog can be closed, it continues appearing every minute until the Critical State has been revoked.

Flow-based Reporting

The following is a list of locations added to include Flow-based Reporting:

- **Unit > Home > Dashboard view** - This shows the unit's system usage, traffic usage, firewalling, and threat detection statistics.
- **Unit > Home > Summary** - This shows the top ten items. The top ten is selected based on various parameters. For example, **Unit > Home > Summary > Applications**, The top ten application is selected based on the connections, data transfer, threats, and so on.
- **Unit > Home > Live Monitor** displays a real-time view of the unit. It is divided into three parts; Application usage, Interface usage, and System usage.
- The **Status** section displays various parameters related to Flow Agent configuration on the firewall.
- **Unit > Reports > Reports** - This sections displays three different views for various types of data.
    - Chart view - based on a selected y-axis against time
    - Table view
    - Timeline view
- **Units > Reports > Live Reports** - This section shows the historical data for the Application usage, the Interface usage, and the System usage of the unit.
- **Unit > Analytics > Sessions** - This section displays flow logs from the unit. It is divided into logs for:
    - Traffic
    - Threats
    - URLs
    - Blocked

Various filters can be applied to drill-down on a specific log.

- **Unit > Analytics > Monitor** - This is the *appflow monitor* for the unit. Various filters can be applied to detect who, what, and when.

Known Issues

The following is a list of issues known to exist at the time of the GMS 9.0 release.

AppFlow Server

Known Issue	Issue ID
GMS Flow Server support for SOHO units should not be available, but incorrectly shows that it is.	196578
A “Flow Server is DOWN” error message incorrectly appears in **Flow Agent > Devices**.	195526

Appliance

Known Issue	Issue ID
On new GMS installations, restoring a configuration from a Complete Backup does not function correctly.	198223
AppFlow does not function correctly after restoring a configuration from a Complete Backup.	198222

Heterogenous Management

Known Issue	Issue ID
Filtering users by Access Methods and then paginating to the next page returns a “No Matching Records Found” message.	197924
Filtering users by the number of WAF Threats Prevented returns a “No Matching Records Found” message.	197919

Installation/Upgrade

Known Issue	Issue ID
After configuring the default AppFlow-based role time settings, they cannot be updated through a Firefox browser.	195819
Configuring the Flow Server role in the Role Configuration Tool Wizard incorrectly displays the Flow Agent Paired IP configuration.	194960

Policies Panel

Known Issue	Issue ID
The Reverse Inheritance filter does not inherit all Content Filter policies from some units under the parent node.	197871
Adding new partitions resets options previously chosen on the **Users > Settings** page.	197434
The Reverse Inheritance feature for some MAC IP anti-spoof entries does not function correctly for TZ300 units.	195992
The SonicWave floor planner does not load correctly in Internet Explorer browsers.	195189

Reports Panel

Known Issue	Issue ID
The **Reports > Status** and **Home > Status** screens are showing an "HTTP Status 500 Error" on the "All in One - Flow Server" setup instead of the correct status.	195685

Tree Control

Known Issue	Issue ID
Tree control does not load correctly when Java has been enabled from techSupport.html on the front-end user interface.	197631

User Interface

Known Issue	Issue ID
In the Flow Dashboard, the shortcut for Graphs should be removed as the screen is not available in the Analytics view.	197794

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 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.

The information in this document is provided in connection with SonicWall Inc. 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 SonicWall 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 reserve the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. 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.

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/legal/eupa. Select the language based on your geographic location to see the EUPA that applies to your region.

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: 1/24/18

232-004173-00 Rev A