SonicWall® Global Management System 8.6

Release Notes

July 2018

These release notes provide information about the SonicWall® Global Management System (GMS) 8.6 release.

Topics:

- About GMS 8.6
- New Features
- Resolved Issues
- Known Issues
- Platform Compatibility
- Upgrading to GMS 8.6
- Product Licensing
- SonicWall Support

About GMS 8.6

SonicWall® Global Management System(GMS) is a Web-based application that can configure and manage thousands of SonicWall firewall appliances and monitor non-SonicWall appliances from a central location. GMS can be used as a Management Console in an enterprise network containing a single SonicWall E-Class NSA or SuperMassive. GMS can also be used as a Remote Management System for managing multiple unit deployments for enterprise and service provider networks consisting of hundreds and thousands of firewalls, Email Security appliances, and Secure Mobile Access (SMA) appliances.

GMS enables administrators to monitor the status of and apply configurations to all managed SonicWall appliances, groups of SonicWall appliances, or individual SonicWall appliances. GMS also provides centralized management of scheduling and pushing firmware updates to multiple appliances and to apply configuration backups of appliances at regular intervals. GMS has monitoring features so you can view the current status of SonicWall appliances and non-SonicWall appliances, pending tasks, and log messages. It also provides graphical reporting of Firewall, SMA, and Email Security (ES) appliance and network activities for the SonicWall appliances.

A wide range of informative real-time and historical reports can be generated to provide insight into usage trends and security events. Network administrators can also configure multiple site VPNs for SonicWall appliances. From the GMS user interface (UI), you can add VPN licenses to SonicWall appliances, configure VPN settings, and enable or disable remote-client access for each network.

GMS 8.6 is a new feature release that includes a number of resolved and known issues. Refer to New Features, Resolved Issues and Known Issues for additional information.

ⓘ **NOTE:** GMS can be deployed a number of different ways, and numerous requirements apply. Refer to Platform Compatibility for detailed information.

New Features

GMS 8.6 releases several new features including:

- Allow Login to the Web Interface from a List of Allowed IP/Subnets
- Permanent Account Lockout
- Search Feature Added to Specific Screens
- Password Complexity Enforcement
- Sandwich/Clustering
- Support for SonicOS 6.5.2

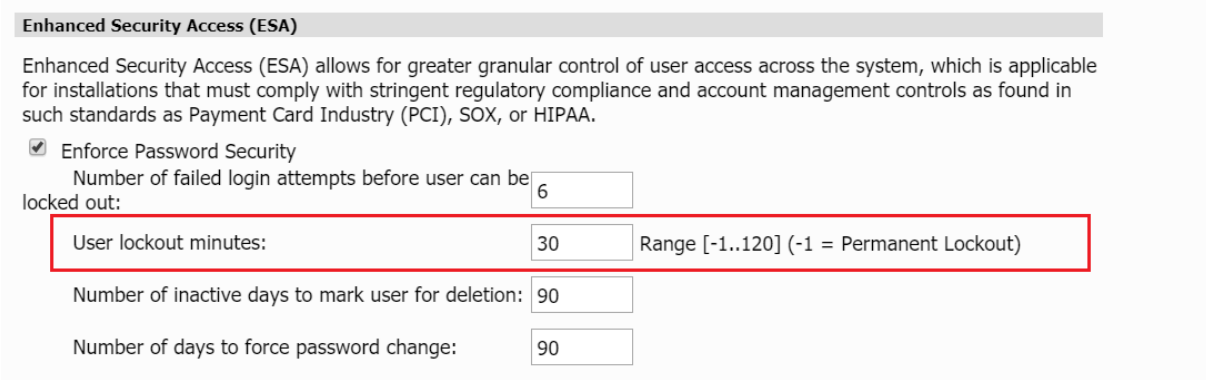
Allow Login to the Web Interface from a List of Allowed IP/Subnets

Administrators are granted access to specific address ranges. As an administrator, you can also provide admin access to those specific IP address ranges to other users in your network. This access can be used only at the site IP locations indicated, and is not transferable to other locations that are not set with the same access.

- The absence of list entries allows users to login without IP enforcement.
- IPv4 and IPv6 versions are supported.

Permanent Account Lockout

Ability to permanently lock users out of GMS is an enhancement to the temporary lockout feature of previous versions. The changes for this feature apply to the **Console > Management > Settings** screen's "Enhanced Security Access (ESA)" section. The User Lockout feature is usually controlled in minutes. By entering a "-1" value in this field, a permanent account lockout can be enforced.



Enhanced Security Access (ESA)

Enhanced Security Access (ESA) allows for greater granular control of user access across the system, which is applicable for installations that must comply with stringent regulatory compliance and account management controls as found in such standards as Payment Card Industry (PCI), SOX, or HIPAA.

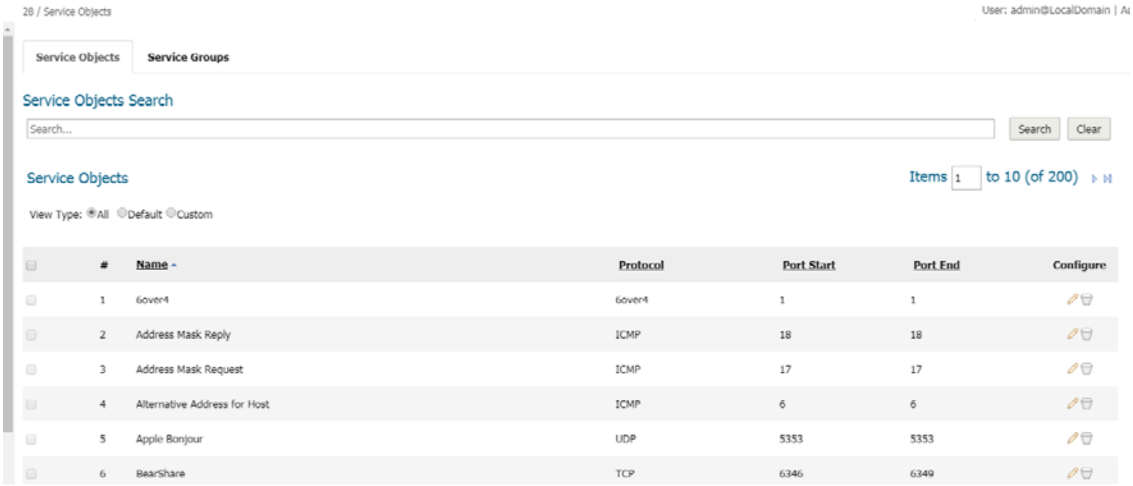
☑ Enforce Password Security

Number of failed login attempts before user can be locked out:	6	
User lockout minutes:	30	Range [-1..120] (-1 = Permanent Lockout)
Number of inactive days to mark user for deletion:	90	
Number of days to force password change:	90	

Search Feature Added to Specific Screens

This enhancement allows you to search any record or present field on the pages listed below. The details of the Search capability are limited only to string searches. All properties of Service Objects are checked and compared with matches to your string filtering requirements.

- Objects > Service Objects



Service Objects Search

Search...

Service Objects

Items 1 to 10 (of 200)

View Type: ● All ○ Default ○ Custom

□	#	Name	Protocol	Port Start	Port End	Configure
□	1	6over4	6over4	1	1	✎ 🗑
□	2	Address Mask Reply	ICMP	18	18	✎ 🗑
□	3	Address Mask Request	ICMP	17	17	✎ 🗑
□	4	Alternative Address for Host	ICMP	6	6	✎ 🗑
□	5	Apple Bonjour	UDP	5353	5353	✎ 🗑
□	6	BearShare	TCP	6346	6349	✎ 🗑

- Network > DNS Proxy
- Objects > Dynamic Address Objects
- Rules > Content Filter Policies
- Objects > Content Filter Objects
- Objects > Bandwidth Objects
- Objects > Match Objects
- Objects > Action Objects
- Objects > Email Address Objects
- Rules > Route Policies
- Network > VLAN Translation
- Network > Zones
- Network > DNS Security
- Rules > Application Control
- Network > Neighbor Discovery
- Network > DNS screen
- Network > DDNS
- Network > MAC-IP Anti-Spoof
- Network > IP Helper
- Rules > NAT Policies

Password Complexity Enforcement

Enforcing complexity on passwords is consistently listed as a requirement for security audits. As part of GMS 8.6, the following password complexities are enforced for GMS users.

Password should be created based on the following rules:

1. At least seven characters in length
2. A maximum length of 15 characters are allowed.
3. Passwords must include characters from at least two (2) of these groupings: alpha, numeric, and special characters.
4. The last five passwords used cannot be repeated.
5. New passwords must not contain a sequence of three (3) or more characters from the previous password.
6. Passwords must not be the same as the UserID with which they are associated.

Additionally, the following rules are also applicable:

1. You should change your passwords every 90 days.
2. Password parameters are set to require that new passwords cannot be the same as the four previously used passwords.
3. User accounts are temporarily locked-out after six invalid access attempts.

   Once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account.
4. The system/session idle time-out features have been set to 15 minutes or less.
5. Passwords are protected with strong cryptography during transmission and storage.

Sandwich/Clustering

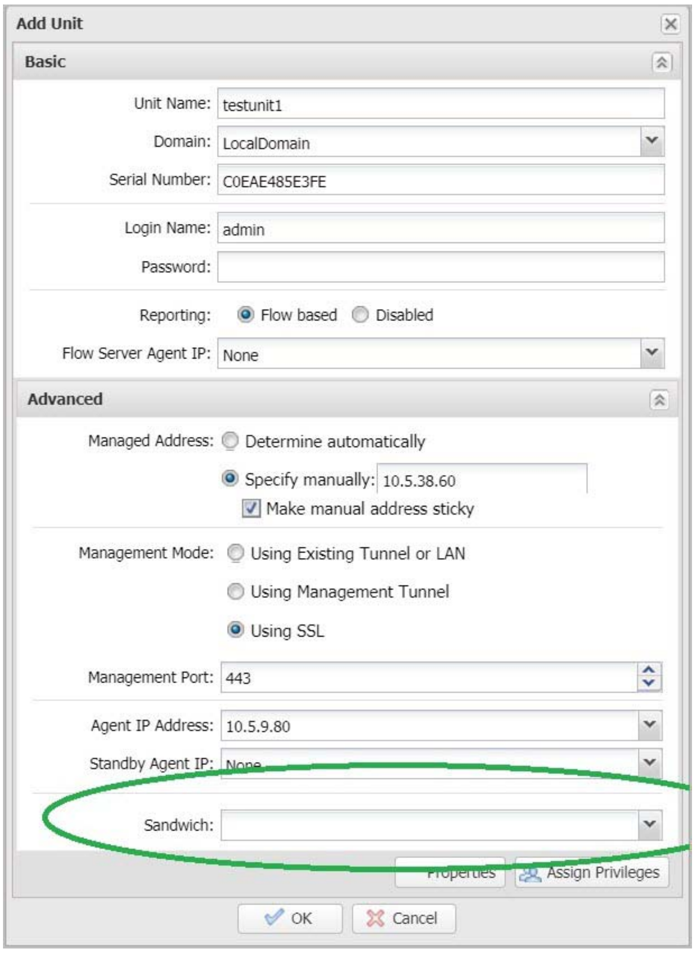
Support for Firewall Sandwich deployments is included within GMS. The ability to cluster nodes and represent them based on individual firewalls and also at the same time show them as a group of nodes.

There is no field or param in the prefs file of the firewall that indicates if the unit is part of a sandwich. It is up to the GMS user to classify units as part of a sandwich unit. This can be done during the “Add unit” or “Modify unit” operations.

After a specific unit has been marked as part of a sandwich, it appears in the respective sandwich group when the sandwich view has been selected, or in any view that has a *sandwich* custom category.

Creating a Sandwich

A sandwich can be created while adding or modifying a unit.



Add Unit

Basic

Unit Name: testunit1

Domain: LocalDomain

Serial Number: C0EAE485E3FE

Login Name: admin

Password:

Reporting: ● Flow based ○ Disabled

Flow Server Agent IP: None

Advanced

Managed Address: ○ Determine automatically

● Specify manually: 10.5.38.60

☑ Make manual address sticky

Management Mode: ○ Using Existing Tunnel or LAN

○ Using Management Tunnel

● Using SSL

Management Port: 443

Agent IP Address: 10.5.9.80

Standby Agent IP: None

Sandwich:

The sandwich drop down in Add/modify unit dialogs is editable.

To create a new sandwich and assign it to a unit type, enter the sandwich name in the drop-down text field and click **Save**.

If an existing sandwich is selected from the drop-down menu, the unit is mapped to that sandwich group.

In the Add Unit dialog, the sandwich drop-down is only present in the Advanced mode. The Sandwich custom category group is neither editable nor deletable. Therefore, it is hidden from the modify properties and Custom groups applications. The default sandwich group is available for all the existing and newly added domains.

Support for SonicOS 6.5.2

Support for the new features in SonicOS 6.5.2 was added to GMS 8.6.

Topics:

- **Decryption Services Features** - Numerous features have been added to GMS DPI-SSL and DPI-SSH decryption services including:
  - DPI-SSL Granular Control
  - Support for DPI-SSL Dynamic White List
  - Access Rules-Based DPI-SSL Control
  - TLS Certificate Status Request Extension

    - Support for Local CRL
    - Enhanced DPI-SSL Certificate Verification
    - Support for ECDSA-Related Ciphers
    - DPI-SSL and CFS HTTPS Content Filtering now Work Independently
    - Blocking of SSH X11 Forwarding
    - Retaining Original Port Numbers in Decrypted Packets
    - Decluttering of Split DNS
    - DNS Host Name Lookup over TCP for FQDN - Option added
- **SonicWave Features**
    - Protected Management Frames (IEEE802.11w)
    - SonicWave RRM And WNM Support (IEEE802.k and IEEE802.v)
    - Secure Fast Roaming (IEEE802.11r) for SonicWave
    - KRACK Detection (WIPS)
    - +Advanced LTE Modem Support
    - Firmware Management Support
    - Load Balancing among Multiple 3G/4G Modems
    - RSSI Threshold Support
    - RADIUS Server Authentication Cache
    - SonicWave low power mode support
    - Renaming of the SonicPoint tab
- **N-Series Switches Support**
    - About N-Series Switches
    - Configuring the N-Series Switch
    - Provisioning an N-Series Switch as an Extended Switch
    - Significance of Uplink Interfaces
    - Provisioning an N-Series Switch
    - Configuring an Extended Switch in PortShield
- **Advanced Support in Radius Accounting Single-Sign-On** - Single-Sign-On by RADIUS Accounting allows the SonicWall to automatically log users in or out based on RADIUS accounting messages from executed tasks.
- **App-Based Routing** - App-Based Routing is a kind of PBF (policy-based forwarding) rule that allows traffic to take an alternative path from the next hop specified in the route table and is typically used to specify an egress interface for security or performance reasons.
- **Capture ATP Blocking Behavior** - GMS now allows customized blocking behavior for Capture ATP to exclude certain traffic or file types from blocking file downloads until a verdict is reached. This applies to HTTP/S file downloads only.
- **DNS Sinkhole Support** - A DNS sinkhole, also known as a sinkhole server, internet sinkhole, or BlackholeDNS, is a DNS server that gives out false information to prevent the use of the domain names it represents. DNS sinkholes are effective at detecting and blocking malicious traffic, and used to combat bots and other unwanted traffic.
- **LAN Bypass** - In the NSa 6650, SM 9250, SM 6450, and SM 9650 platforms, the hardware (LAN) bypass mode is enabled in both Wire Mode and L2 Bridging. The main functionality of the LAN Bypass feature, when enabled:

- Pass traffic in between the LBP-capable interfaces while rebooting.
- Even when the firewall is powered off, pass traffic in between those LBP-capable Interfaces.

For the NSa 9250, NSa 9450, and NSa 9650 platforms, the LAN Bypass feature is available between interfaces X26 and X27. For the NSa 6650, the feature is available between X0 and X1.

- **Firmware Backup on Secondary Storage Devices** - For all NS*a* Series security appliances that have secondary storage devices, GMS now supports the ability to take a firmware and configuration settings file backup (firmware snapshot) if the system limit permits.
- **Dynamic Address Group List** - GMS supports the ability to maintain a list of dynamic address groups within the firewall, as well as making use of the dynamic address group in an access rule or policy.
- **Global Search Enhancements** - The Global Search function now performs a dynamic search for configuration objects, such as objects and rules, as well as management interface pages. Page-search results contain links to main pages that are part of menu items. Object and rule search results display the names of corresponding object/rule, and the matching details are listed as part of the description.
- **High Availability Heartbeat over MGMT Interface** - GMS appliances now allow heartbeats to be exchanged between an HA pair across the MGMT interface in addition to the HA control interface.
- **Dynamic Botnet HTTP Authentication** - The implementation of SonicOS 6.5.0 did not allow the security appliance to accept URLs that are password protected. The primary reason is that the security appliance does not maintain the state of the transaction when performing a HTTP GET. Because of this, the transaction needs to happen in single shot. However, with password-protected sites, the server returns a HTTP 404 error and the user is prompted with a username/password dialog (when using from a regular browser). With GMS 8.6, username and passwords for HTP URLs in the dynamic Botnet configuration are accepted, and the information is transmitted in the HTTP header so the GET request has the required information.
- **LHM RESTful API** - Lightweight Hotspot Messaging (LHM) defines the method and syntax for communications between a SonicWall wireless access device (such as a SOHO W, TZ-series W, or a SonicPoint with a governing SonicWall security appliance) and an Authentication Back-End (ABE) for authenticating Hotspot users and providing them parametrically bound network access.

  A RESTful API is an application program interface (API) that uses HTTP requests to GET, PUT, POST and DELETE data. A RESTful API, also referred to as a RESTful web service, is based on representational state transfer (REST) technology, an architectural style and approach to communications often used in web services development.
- **URI List Groups** - GMS 8.6 supports URI list groups for ease of management of allowed and forbidden lists or for Websense exclusion. You can assign multiple URI list objects to one group, and refer that group directly within other modules. The URI list group supports nested inclusion, which means one group can contains other groups. A URI list group can be used anywhere a URI list object can be used. You can configure a URI list group from the management interface or the CLI.
- **Quota Control for all Users** - The quota control for users feature provides quota control based on the user’s account. The quota can be specified as a session lifetime, or a transmit and/or receive traffic limit. With a cyclic quota, a user can not access the internet upon meeting the account quota until the next cycle (day, week, or month) begins. If the quota cycle is Non Cyclic, the user is unable to access the internet upon meeting the quota.
- **Flexible Storage Module Support** - All NSa Series platforms support the built-in storage module. This module is a storage device like the Built-in storage module and is used to read/write data to it. The Flexible storage module is a shared device than can be used by multiple security appliances provided it is successfully activated on each security appliance. In the Flexible storage module, a top-level directory is created with the security appliance serial number as the directory name. All applications create sub-directories inside this top-level directory and store their data there.

  With the availability of two storage modules, Built-in and Flexible, you now have a choice to use for features. The switching of storage at run time may not be available for all features, and thus it may involve a reboot. For example, for the Log Monitor feature, to switch the storage device from one to the other involves a reboot. For logging, the option to choose the storage device is available in the **Log Settings > Base Setup** page; by default, the Built-in storage module is used if both modules are available.

- **TACACS+ Support** - GMS 8.6 now supports TACACS+ (Terminal Access Controller Access-Control System latest generation) for user authentication. The main characteristics of TACACS+ are:
  - Provides separate authentication, authorization and accounting (AAA) services.
  - Uses TCP for its transport.
  - Entire TACACS+ body may be protected by the encryption.
- **Enhanced User Login Reporting** - GMS 8.6 now supports reporting this information on the **MONITOR | Current Status > System Status** page.
- **Manual Priority Support for Access Rules** - A manual option has been added to the Access Rules priority drop-down.
- **SSO Support in Access Rules** - A new field has been added that is supported at Group level and inheritance. The field is visible in the UI only when the “Enable SSO agent authentication” option in U**sers > Settings > Configure SSO** screen is enabled. By default, the field is disabled.
- **WeChat Support** - GMS 8.6 now supports WeChat, a very popular social app in China.
- **AWS Logs** - Establishes the availability of console log reporting for Amazon web services (AWS).
- **VLAN Enhancements for LAG** - Link Aggregation (LAG) allows you to inter-connect devices with two or more links between them in such a way that the multiple links are combined into one larger virtual pipe that can carry a higher combined bandwidth. As multiple links are present between two devices, if one link fails, the traffic is seamlessly transferred through other links without disruption. With multiple links being present, traffic also can be load balanced in such a way to achieve even distribution.

  With this enhancement;
  - LAG will not have to be dismantled or removed before the VLAN is added/deleted. The configuring will allow you to add the VLAN to an existing LAG or delete the VLAN from an existing LAG without disrupting the current traffic related to the LAG or other VLANs configured on the LAG.
  - VLAN can be added to/deleted from any member of the LAG and it will get applied to all the other members of the LAG automatically without the need to explicitly add to/delete from other members of the LAG.

For more detailed information about new SonicOS 6.5.2 features, refer to the *SonicOS 6.5.2.0 Release Notes*.

Resolved Issues

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

Change Order Management

Resolved Issue	Issue ID
Change Compliance Reports are sometimes empty.	202743

Inheritance

Resolved Issue	Issue ID
An invalid “Max Rule Count is not in the valid range of [0 .. 5000]” error message appears for Forward/Reverse Inheritance of the maximum rule count.	207835
Forward Inheritance of FQDN address objects fails for devices with older firmware.	198045
Running inheritance on a firewall containing two similarly named objects (but are differentiated by capitol letters) will not move one of the objects to the Group Level.	196614

Policies Panel

Resolved Issue	Issue ID
Modifying the maximum rule count cause and error at the Group and Global levels.	207831
Many of the default zones are missing in the GMS upgrade setup.	206213
“Mesh Network Support” is available for SonicOS 6.5.2.24n and above but was removed from the UTM for 6.5.2.0.24n.	206204
Reverse inheritance of address group fails to move all VLAN objects.	203934
Add support for the **Enable DNS host name lookup over TCP for FQDN** feature under IPv4/v6 DNS settings.	203424
Missing the **Drop TCP SYN packet with data** setting for the firewall settings on the Flood Protection page.	203362
In Access Rules, the maximum rule count (minimum and maximum values) for the NSA 6600 have changed and should be updated in the GMS user interface.	203048
Deleting Scheduled Reports does not function correctly.	202842
The Allow Unauthenticated VPN AP Client Access drop-down is not being updated.	202822
The VPN AP Client ID is not being updated.	202818
In the **Botnet Filter > Dynamic Botnet List Server** tab, an invalid error message displays when the password contains special characters.	202804
There is a synchronization issue for Wireless VAP/VAP Profiles. GMS does not show all profiles in the user interface.	202754
In Route Policies, adding a probe should enable the **Disable route when probe succeeds** option and activate the **Probe default state is UP** check box.	202728
App Control Advanced: Clicking the Category should change the value in View Styles.	202589
In the DHCP over VPN feature, there is a value mismatch for the **Obtain using DHCP through this SA** option in GMS and the UTM.	202570
In the DHCP over VPN feature, the **Send DHCP requests to the server addresses listed below** option should be disabled when the **Use Internal DHCP Server** option is enabled.	202543
The RADIUS accounting test for Connectivity does not return the expected result but instead returns HTML code.	202480
Updating the RADIUS accounting server returns a task execution failure.	202450
On **Switching > LLDP Profile**, task creation fails with “Object does not exist” error when performing a **Delete** operation.	200296
The Content Filter Policies screen shows license is unavailable even though **Content Filtering: Premium Edition** is licensed.	200282
Synchronize Now is not working for **AWS Configuration > AWS Objects**.	200241
Anti-Spyware signatures are not getting displayed in GMS user interface.	199343
Test Connection Button should be available on AWS Configuration page.	199239
Modifying a route policy based on **Name** field creates new policy instead of a modification.	199065
In **Wireless > Settings**, the regulatory domain on the GMS user interface does not match the one in the UTM regulatory domain.	193012
The unit’s up/down status alerts were sent even after heartbeat messages were received.	185710

Reporting

Resolved Issue	Issue ID
When generating a Scheduled Report, the layout is broken on the Table of Contents page.	205613

User Interface

Resolved Issue	Issue ID
The **Appliance > Deployment > Settings** page displays an invalid page error.	194994

Workflow

Resolved Issue	Issue ID
Selecting both processed/unprocessed change orders and then generating a compliance report incorrectly does not return any warnings.	202400
The Workflow page takes more time to load than expected.	196734
Performing approval action fails showing “Update failed, invalid input” when comments include special characters.	183652

Known Issues

The following is a list of issues known to exist at the time of the GMS 8.6 release.

Appliance

Known Issue	Issue ID
There is an intrusion data mismatch between GMS and the UTM.	207863

Backend Communication

Known Issue	Issue ID
An error log appears after a successful execution of a task that reads, “Synchronize unit with MySonicWall.com.”	205404
Synchronizing GMS with MySonicWall isn't working.	199349

Console Panel

Known Issue	Issue ID
Secure Access: Guest users with View Only access attempt to unlock locked users, but the user interface returns an “Update Failed: Invalid Input” error message.	207363
SMA/ES options are missing under the **Console > Management > Settings** page.	203898
Selecting multiple change orders does not generate a Compliance report and there are no console logs being displayed.	202850
Interval setting for auto-added alerts: New firmware availability for CustomDomain appears as undefined.	201139
When logging in to GMS from other accounts, the “Add user Type” option does not function as expected.	199219
The wrong note is shown on the Product licenses > License summary page. The license summary being generated is from the offline license information.	199132
The **CP > Product** licenses page does not show default product licenses information.	199129

Diagnostics

Known Issue	Issue ID
The immediate IPSEC traffic appears blank after enabling some checkboxes when selecting **Start Capture** on the Monitor page.	196576

Firewall Configuration

Known Issue	Issue ID
When an address group is created and pushed out to the firewall from Globalview, the SSLVPN option on a WAN network is disabled.	191760

Inheritance

Known Issue	Issue ID
Reverse inheritance for FairNet policies do not function correctly.	207227
Instead of modifying the existing NAT policy, a new NAT policy with same name is created while reverse inheriting from the unit to the group level.	207117
When inheriting a NAT Policy/Route Policy/SA, dynamic external object groups are not created as expected.	206895
Client AV screen has issues related to Inheritance.	206160
The reverse inheritance with an optional target to a parent node and all nodes under it does not function correctly for DPI-SSL enforcement.	206087
When performing reverse inheritance, two entries with the same configuration were created at the group level.	205623
Inheritance of the SonicWave profile does not include any dependent custom schedules configured in the Radio0/Radio1 Advanced settings.	193403
Reverse inheritance fails for the Wire mode from unit to group as well as for the units managed under it.	193340
Content Filtering 4.0 policy inheritance tasks do not function as expected. Required dependent objects are not applied.	191691

Install - Upgrade

Known Issue	Issue ID
The START action failed for a flow server that is pointing to an AIOP set up.	207864
SSL-VPN devices are not being upgraded as expected through GMS.	207846
After a successful role configuration, a “Failed to Update role Settings” message appears.	207172
The Role settings were not updated during upgrade.	199060
Firmware uploaded through a GMS proxy (Login to Unit) returns an error message.	191868

Licensing

Known Issue	Issue ID
Product does not correctly associate to GMS.	195192

Management

Known Issue	Issue ID
The user interface shows the Email Security appliance login page, which is non-responsive.	207843

Policies Panel

Known Issue	Issue ID
Reverse Inheritance of a “SonicPoint Wave2 Profile” does not update the “Service Provider” and “Plan Type” options in the 3G/4G/LTE WWAN Connection profile settings.	207854
Modifying the Default CFS policy creates duplicate CFS policies at the Group level.	207819
Global level updates do not function correctly on the **RADIUS Accounting > Advanced** settings page.	207815
Deletion of user names does not function correctly at the Group level for radius accounting when using the user names field.	207814
The Portshielding Daisy Chain Switch Port to Interface is a dedicated link of the parent switch and should appear on the VLAN tab.	207786
Unable to remove the added usernames > For, With user names: field for radius accounting.	207778
Changing from WebSense to the Sonicwall Content Filtering Service does not function as expected in **Security Services > Content Filter**.	207761
Unable to add or move a TSA agent from one partition to another.	207716
Unable to add or move a single-sign-on agent from one partition to another.	207713
Adding a new local user at the group level fails under the **Users > Local Users** page.	207706
Because some L2TP interfaces cannot be added to GMS, two text boxes are missing: Gateway IP and Subnet Mask.	207366
Deleting an Address Object group at the Group/Global level does not delete the actual group. Instead, it deletes the contents of that group and then creates an empty Address Object group.	207357
Adding a new dynamic external object to the Group/Global list does not correctly add it to a Network Address Group.	207306
Searching for the name and download minutes does not list any dynamic external objects.	207173
Uploading a DPI-SSL white list to GMS returns an error message though the same file works for the UTM.	206961
Address objects based on MAC addresses created by default under the WLAN zone do not appear in GMS.	206863
The Dynamic Botnet List screen is not present in GMS.	206507
When authentication is set to “WPA2-PSK” or “WPA2-EAP,” inheritance of a Virtual Access Points profile fails at the Unit level.	206256
While adding a new zone, there is no option for wireless in the security type listbox.	206215
When authentication is set to “WPA2-PSK” or “WPA2-AUTO-PSK,” the Inheritance of a SonicPoint profile fails at the unit level.	206214
Many of the default zones are missing in the GMS upgrade setup.	206213
On the **Network > Zones** page, the task execution sync up time requires at least one minute 40 seconds to complete.	206209
When a task is pushed at the Global level, an internal server error appears while validating the data.	206208
Editing a Zone returns the “Failed to get handle for <zone_name> from Zone_Object_table” error message.	206206

Policies Panel (Continued)

Known Issue	Issue ID
Editing the “Capture Client Enforcement List” in Group UTMs creates a new “SentinelOne Client AV Enforcement List.”	206152
Test connectivity for password authentication shows no data in GMS, but the authentication is successful in the UTM.	206074
Test connectivity on the Test TACACS Settings page does not function correctly from the GMS side but is successful in the UTM.	206070
Clicking the **Users > Multi-LDAP** option returns the “LDAP is not selected as the authentication method for this node” error message.	206060
Unable to add a Sonicpoint Wave2 Profile because the **OK** button is non-responsive at the Unit level/Group level.	206018
Virtual Access Points fails at the unit level with “Virtual Access Point/Group/NAME: WPA passphrase is not valid” or “WPA Radius Server 1 secret is not valid” error messages.	205953
Dynamically created address objects should display in the GMS user interface.	205952
When editing a WAN interface and selecting the WAN assignment as DHCP on the Advanced tab, two necessary checkboxes are missing from the GMS screen.	205927
Even when TACACS+ is not selected as the authentication method for a particular node, it appears as TACACS+ being selected.	205861
GMS does not show a second TACACS+ profile when it has been added.	205848
Data mismatch of SonicPoint profiles between GMS and the UTM.	205723
The **FIREWALL | Manage | Network > Default NAT policy** (any interface-to-any interface) is not visible at the group level.	205684
Deleting the VLAN entries from the group level, deletes them at the group level, but the VLAN remains “as is” on the unit level.	196600
The Reset button for the DNS page for IPv6 configuration does not function correctly.	193412
The country code appears blank on the General tab of the Edit SonicWave Object window.	193406
Reverse inheritance from units to groups and all group members does not function as expected for Geo-IP and Botnet custom list objects.	184419

Reports Panel

Known Issue	Issue ID
The Botnet pie chart view does not show data on the Dashboard as expected.	207849
The SMA 500v does not display report data as expected.	193216

Tree Control

Known Issue	Issue ID
When Tree Control has more than 500 units, the vertical scroll bar does not appear correctly, making it impossible to view all units.	207705
Modifying a unit does not correctly populate all existing parameters for a unit after it has been moved to a sandwich group.	207003
The Import XML option does not function correctly in the GMS 8606 build.	206741

Universal Schedule

Known Issue	Issue ID
Universal Scheduled Reports (USR) report PDF files do not provide the names of the firewalls with “No Matching Reports Found.”	193449
Universal Scheduled Reports (USR) for Flow Reporting does not return PDF reports in the selected language.	193187

User Interface

Known Issue	Issue ID
Unable to login concurrently to multiple firewalls through GMS.	182279

Workflow

Known Issue	Issue ID
Adding a new VLAN (WF) appears as Modified on the View Change Order page.	196601

Platform Compatibility

The SonicWall Global Management System 8.6 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 Planning Tool at https://www.sonicwall.com/en-us/products/firewalls/management-and-reporting/global-management-system. 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 8.6, ensure that your system meets the minimum hardware and software requirements described in the following sections:

- Supported Platforms
- Unsupported Platforms
- Hardware Requirements
- Hard Drive HDD Specifications
- GMS Virtual Appliance Supported Platforms
- Virtual Appliance Deployment Requirements
- Browser Requirements
- Microsoft SQL Server Requirements
- Java Support
- SonicWall Appliances Supported for GMS Management
- Non-SonicWall Appliance Support

Supported Platforms

The SonicWall Global Management System supports the following Microsoft Windows operating systems:

- Windows Server 2016 Standard
- 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 virtual machine under Windows Server 2012 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

To determine the hardware requirements for your deployment, use the Capacity Planning Tool at https://www.sonicwall.com/en-us/products/firewalls/management-and-reporting/global-management-system.

ⓘ **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 Global Management System Administration Guide*.

Hard Drive HDD Specifications

The following hard drive HDD specifications are required when using GMS Software on a 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 Global Management System Virtual Appliance. The GMS Virtual Appliance runs on the following VMware platforms:

- ESXi 6.5, 6.0 and 5.5

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

To determine the hardware requirements for your deployment, use the Capacity Planning Tool at https://www.sonicwall.com/en-us/products/firewalls/management-and-reporting/global-management-system.

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 Global Management System Administration Guide*.

Browser Requirements

SonicWall Global Management System 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 Global Management System.

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
- Microsoft Edge 41 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: http://www.sonicwall.com/en-us/support/knowledge-base/170502904412584

Mobile device browsers are not recommended for SonicWall Global Management System 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 8.6 does not support legacy SonicWall appliances, including:
>
> - Firewall appliances running firmware earlier than SonicOS 5.0
> - CSM Series
> - CDP Series

SonicWall Global Management System 8.6 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://www.sonicwall.com/en-us/support for more information.

Component Requirements (Continued)

SonicWall Platforms	SonicWall Firmware Version
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	SonicOS 5.9.1.3 or newer 5.9 versions
SonicWall SOHO Wireless	SonicOS 6.2.6 or newer 6.x versions
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 8.6 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 Global Management System provides monitoring support for non-SonicWall TCP/IP and SNMP-enabled devices and applications.

Upgrading to GMS 8.6

GMS can be configured for a single server or in a distributed environment on multiple servers. GMS 8.6 can be installed as an upgrade from GMS 8.5. Consider the following before upgrading:

- 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 8.6 logs into the appliances using HTTPS only.
- The scheduled reports created in GMS 8.0 continue to work properly after upgrading to 8.6. 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 8.6 and others running 8.5.

ⓘ **NOTE:** DO NOT start/stop the **SonicWall Universal Management Suite—Database** service manually, before or after upgrading to 8.6. 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 8.6, complete the following steps:

1. Navigate to https://www.mysonicwall.com.
2. Download the GMS 8.6 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.

Prerequisites for Deploying a GMS 8.6 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. For increased security, SHA-256 with the PKCS#1 RSA encryption signature algorithm is used for the default certificates in both:

- SonicWall GMS 8.6 Virtual Appliance firmware
- VMware ESXi 6.5

This means that new deployments of GMS 8.6 can only be deployed on servers running VMware ESXi 6.5 or higher. However, upgrades from GMS 8.5 to GMS 8.6 are supported on servers running earlier versions of ESXi.

Installing GMS 8.6 on VMware ESXi

GMS 8.6 conditionally supports ESXi:

	Upgrading GMS 8.5 to GMS 8.6	Fresh installation of GMS 8.6
...on ESXi 6.0/5.5	Supported	Not supported
...on ESXi 6.5	Supported	Supported

Refer to earlier GMS guides on how to install or upgrade older versions of GMS.

Upgrading a GMS Virtual Appliance

This section provides procedures for upgrading an existing SonicWall GMS 8.5 virtual appliance or newer installation to GMS 8.6 virtual appliance.

To upgrade a GMS Virtual Appliance, complete the following:

1. Download the GMS 8.6 file from www.mysonicwall.com to your workstation software: **sw_gmsvp_all_eng_8.6.*xxxx.yyyy.<file format*>**: where ***xxxx*** is the major build number and ***yyyy*** is the minor build number.
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.

   The Virtual Appliance reboots at the end of the installation process.

Product Licensing

All instances of SonicWall Global Management System Software must be registered and licensed before use. This requirement applies to both single server deployments or distributed deployments on multiple servers, to fresh or upgraded installations, and to software installations on Windows servers or VMware Virtual Appliances. SonicWall Global Management System registration is done using the `/appliance` Universal Management Host (UMH) system interface. When installing Universal Management Suite on a server or host, a Web server is installed to provide the `/appliance` UMH system interface. The system interface is available by default after restarting the system at: https://localhost/. To complete registration, the system must have access to the Internet and you must have a MySonicWall account. The SonicWall License Manager, available on the **System > Licenses** page of the UMH system interface, allows you to log in and enter your registration information 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: 7/26/18

232-004472-00 Rev A