

SonicWall™ Global Management System (GMS) 8.3

Release Notes

March 2017

These release notes provide information about the SonicWall™ Global Management System (GMS) 8.3 release.

Topics:

- [About SonicWall GMS 8.3](#)
- [New Features](#)
- [Resolved Issues](#)
- [Known Issues](#)
- [Platform Compatibility](#)
- [Upgrading to GMS 8.3](#)
- [Product Licensing](#)
- [SonicWall Support](#)

About SonicWall GMS 8.3

SonicWall GMS 8.3 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 8.3 release.

Topics:

- [High Availability](#)
- [PPPoE Unnumbered Interface Support](#)
- [Vendor OUI Detection and Logging](#)
- [Dell Networking X-Series Switch Integration Features](#)
- [DPI-SSH](#)

- Support for pcapNG
- TSR FTP for Periodic Backup
- Custom Lists for Geo-IP and Botnet
- SIP UDP Fragmentation Fixes
- System Logs on AppFlow Server via IPFIX
- NAT64: Stateful NAT from IPv6 Client to IPv4 Server
- DNS Proxy
- FQDN Routing
- Maximum Routes Doubled
- Maximum Zone to Zone Access Rules Increased
- Flow Reporting using IPFIX Extension Version 2
- Syslog Server Profiling
- IPv6 Support
- DPI-SSL Increased Connection Counts and Enhancements
- Open Authentication Social Login
- Updated SonicPoint Firmware
- SonicPoint Radius Accounting
- 31-Bit Network
- Threat API
- Biometric Authentication
- VPN Auto Provisioning

High Availability

GMS 8.3 introduces two new features in the area of High Availability:

- **HA support with Dynamic WAN interfaces**

In GMS 8.3, PPPoE can be enabled on interfaces in HA Active/Standby mode.

After the active unit connects to the PPPoE server, it synchronizes the PPPoE session ID and server name to the idle unit.

During a failover, the active unit terminates the PPPoE HA connection on the client side by timing out. The secondary unit then terminates the original connection on the server side and starts a new PPPoE connection.

When High Availability is enabled and one interface is configured as PPPoE Unnumbered, the following settings are required:

In the **High Availability > Settings** screen:

- Select **Enable Virtual MAC**
- Clear **Enable Preempt Mode**

In the **High Availability > Monitoring** screen:

- Select **Enable Physical/Link Monitoring**
- Set the **Primary** and **Secondary** IP address fields to 0.0.0.0

- Clear all other checkboxes

- **HA Stateful Synchronization support for DHCP**

DHCP can now be enabled on interfaces in HA mode. This feature is supported in both Active/Standby (non-stateful) and Stateful Synchronization mode.

Only the active unit can get a DHCP lease. It synchronizes the DHCP IP address along with the DNS and gateway addresses to the idle unit. The DHCP client ID is also synchronized, allowing this feature to work even without enabling Virtual MAC.

During a failover, the active unit releases the DHCP lease and the secondary unit renews the DHCP lease using the existing DHCP IP address and client ID as it becomes the active unit. The IP address does not change, and network traffic, including VPN tunnel traffic, continues to pass.

If the active unit does not have an IP address when failover occurs, the secondary unit starts a new DHCP discover.

PPPoE Unnumbered Interface Support

A PPPoE Unnumbered interface allows you to manage a range of IP addresses with only a single PPPoE connection. The Internet Service Provider (ISP) provides multiple static IP addresses that can be allocated within a subnet. The first address is designated as the network address, and the last one as the broadcast address.

Start by configuring the PPPoE client settings on a WAN interface:

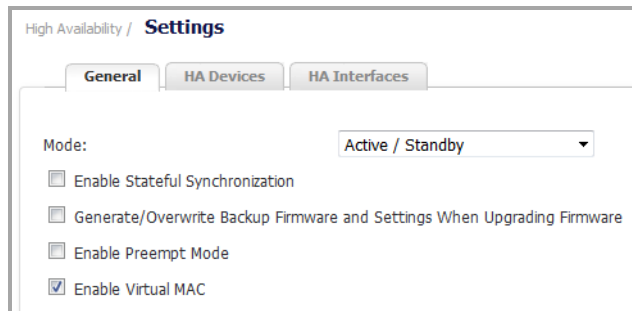
The Unnumbered PPPoE interface is configured on a different interface:

- 1 For **Zone**, select **LAN**, **DMZ**, or create a new zone.
- 2 For **Mode / IP Assignment**, select **IP Unnumbered**.
- 3 For **IP Address**, enter the address provided by your ISP. Usually it is the second IP address assigned by the provider. The subnet mask is also assigned by the ISP.

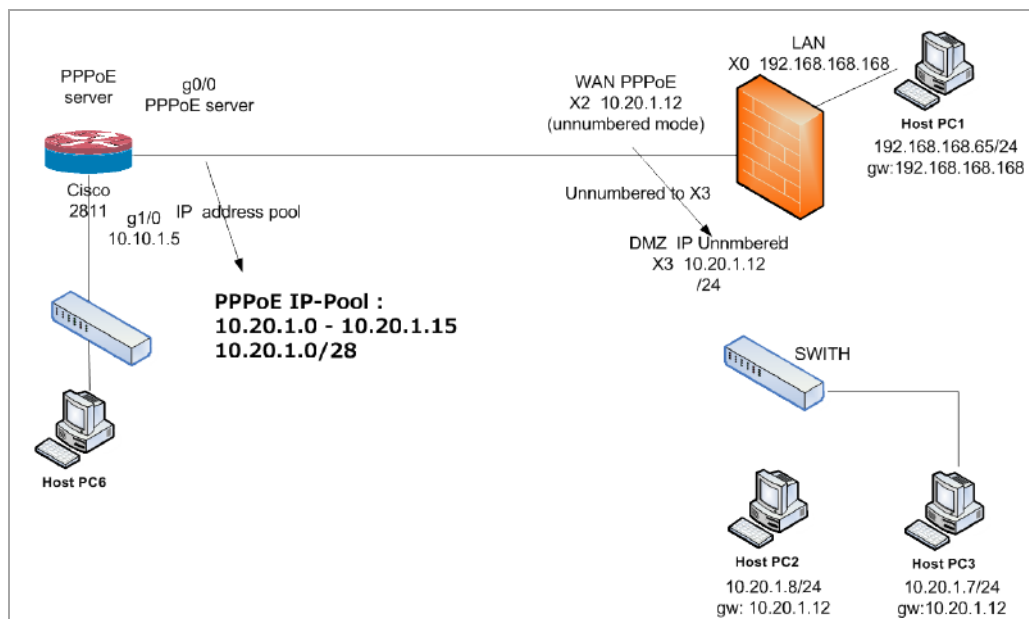
Notes:

- The default MTU of PPPoE is 1492.
- To change X3 to another mode when X2 unnumbered to X3 is configured, first terminate the relationship with X2 by changing X2 to another mode. Otherwise, if you change the IP address or mask of interface X3, it causes X3 to reconnect to the PPPoE server.
- If X3 is set as unnumbered interface, other interfaces cannot connect to X3 using an L2 Bridge.

If High Availability is enabled, **High Availability > Settings** is configured as shown below with Unnumbered PPPoE:



A sample network topology is shown below:



In this topology, X2 is the PPPoE unnumbered interface and X3 is an unnumbered interface.

X2	WAN	Default LB Group	10.20.1.12	255.255.255.240	PPPoE	Disconnect	1 Gbps Full Duplex	Unnumber to X3
X3	DMZ		10.20.1.12	255.255.255.240	Unnumber		1 Gbps Full Duplex	Be X2 Unnumbered
X4	DMZ				PortShield to X3		1 Gbps Full Duplex	
X5	DMZ				PortShield to X3		No link	

GMS adds two routes:

6	Any	X3 Subnet	Any	0.0.0.0	X3	20
7	Any	X0 Subnet	Any	0.0.0.0	X0	20
8	Any	X1 Subnet	Any	0.0.0.0	X1	20
9	X1 IP	Any	Any	X1 Default Gateway	X1	20
10	X2 IP	Any	Any	X2 Default Gateway	X2	20
11	X3 Subnet	Any	Any	0.0.0.0	X2	20

GMS also adds two NAT policies:

<input type="checkbox"/> 18	X3 Subnet	Original	Any	Original	Any	Original	X3	X2
<input type="checkbox"/> 19	Any	Original	X3 Subnet	Original	Any	Original	X2	X3
<input type="checkbox"/> 20	Any	Original	10.20.1.3	192.168.168.65	Any	Original	X2	Any

A manually added NAT policy would have settings such as:

NAT Policy Settings

Original Source: Any

Translated Source: Original

Original Destination: 10.20.1.3

Translated Destination: 192.168.168.65

Original Service: Any

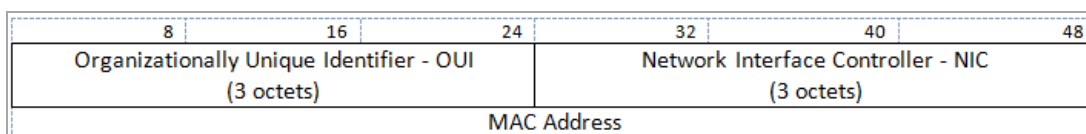
Translated Service: Original

Inbound Interface: X2

Outbound Interface: Any

Vendor OUI Detection and Logging

Every wired or wireless networking device has a 48-bit MAC address assigned by their hardware manufacturers. An organizationally unique identifier (OUI) is a 24-bit number that uniquely identifies a vendor, manufacturer, or other organization globally or worldwide. The first three octets of the MAC address are the OUI.



In GMS 8.3, this information is used to provide a **Vendor** column in the following tables:

- Dashboard > Connections Monitor
- Dashboard > Log Monitor
- Dashboard > AppFlow Monitor
- Network > ARP
- Network > Neighbor Discovery
- Network > MAC-IP Anti-spoof
- Network > DHCP Server
- Network > IP Helper
- Switching > L2 Discovery
- Switching > Link Aggregation
- VPN > DHCP over VPN
- Wireless > Status

- Wireless > IDS
- SonicPoint > Station Status
- SonicPoint > RF Analysis
- SonicPoint > IDS

Dell Networking X-Series Switch Integration Features

GMS 8.3 provides several enhancements and new features for Dell Networking X-Series integration:

- **PortShield and High Availability**

Dell Networking X-Series integration previously supported GMS PortShield functionality in HA mode using Dedicated Uplink(s). In GMS 8.3, support for PortShield functionality in HA mode is available using Common Uplink.

In this configuration, a link between the active/standby firewall and the X-Series switch serves as a common uplink to carry all the PortShield traffic. In this configuration firewall interfaces which serve as PortShield hosts should be connected to a separate switch and not the same X-Series switch connected to the active and standby units. This is to avoid looping of packets for the same PortShield VLAN. The PortShield members can be connected to ports on the X-Series switch which is controlled by the active/standby firewall.

- **Single Point of Management over Common Uplink for VLAN Traffic**

Dell Networking X-Series integration previously supported VLANs in a Dedicated Uplink configuration. In GMS 8.3, VLANs are also supported with Common Uplink. This allows a single link between the firewall and the X-Series switch to carry management traffic of the firewall managing the X-Series switch plus PortShield traffic for the *Interface Disambiguation via VLAN (IDV)* VLANs corresponding to the firewall interfaces plus traffic for the VLAN sub-interfaces present under the Common Uplink interface.

NOTE: Overlapping VLANs cannot exist under appliance interfaces configured as dedicated uplinks or common uplinks to the same switch. This is because the VLAN space is global on the X-Series switch.

NOTE: PortShield of Extended Switch Interfaces to Common Uplink Interfaces without selecting any VLANs for access/trunk configuration is not supported.

- **Increase X-Series Switch Maximum to Four**

In previous GMS releases, a SonicWall firewall could be provisioned for a maximum of two X-Series switches. In GMS 8.3, a maximum of four X-Series switches is supported. All four X-Series switches must be directly connected to the firewall appliance. Daisy-chaining of X-Series switches is not yet supported.

- **Support for SonicWall NSA and SuperMassive**

In GMS 8.3, support for the X-Series solution is extended to include SonicWall NSA and SuperMassive appliances, with the exception of the NSA 2600. The following SonicWall platforms are now supported:

- | | | |
|---------------------|------------|--------------------------|
| • SuperMassive 9600 | • NSA 6600 | • TZ600 |
| • SuperMassive 9400 | • NSA 5600 | • TZ500 / TZ500 Wireless |
| • SuperMassive 9200 | • NSA 4600 | • TZ400 / TZ400 Wireless |
| | • NSA 3600 | • TZ300 / TZ300 Wireless |

DPI-SSH

GMS 8.3 introduces the DPI-SSH feature. DPI-SSH inspects the data traversing the firewall in an SSH tunnel.

SSH, or Secure Shell, is a cryptographic network protocol for secure network communication and services between two networked computers. It connects, via a secure channel over an insecure network, a server and a client running SSH server and SSH client programs, respectively. SSH is not only a shell, but acts as a secure channel. It can provide different services over this tunnel, including shell, file transfer or X11 forwarding.

GMS supports SSH2. SSH1 sessions will not be intercepted and inspected. If the SSH1 banner message contains a non-conforming SSH version number, it will be treated as a bad protocol and dropped.

DPI, or Deep Packet Inspection, examines the data part (and possibly also the header) of a packet as it passes the SonicWall firewall. It searches for protocol non-compliance, viruses, spam, intrusions, or defined criteria to decide whether the packet may pass.

DPI-SSH decrypts incoming SSH packets and sends them to the DPI module for inspection. After completion of DPI inspection, it re-encrypts the packet again and sends the packet to the destination. If the data/packet does not pass the DPI inspection, DPI-SSH resets the connection.

DPI-SSH provides inclusion/exclusion criteria to inspect or bypass certain kinds of traffic. The SonicOS administrator can modify the criteria on the **DPI-SSH > Configure** screen.

DPI-SSH supports both route mode and wire mode. For wire mode, DPI-SSH is only supported in the secure (active DPI of inline traffic) mode. For route mode, there is no limitation.

DPI-SSH supports the following clients:

- SSH client for Cygwin
- Putty
- secureCRT
- SSH on Ubuntu
- SSH on centos
- SFTP client for Cygwin
- SCP on Cygwin
- Winscp

DPI-SSH supports the following servers:

- SSH server on Fedora
- SSH server on Ubuntu

DPI-SSH supports the following key exchange algorithms:

- Diffie-hellman-group1-sha1
- Diffie-hellman-group14-sha1
- ecdh-sha2-nistp256

Notes:

- If there is already an SSH server key stored in the local machine, it must be deleted. For example, if you already SSH to a server, and the server DSS key is saved, the SSH session will fail if the DSS key is not deleted from the local file.
- The ssh-keygen utility cannot be used to bypass the password.
- Putty uses GSSAPI. This option is for SSH2 only, which provides stronger encrypted authentication. It stores a local token or secret in the local client and server for the first time communication. It exchanges messages and operations before DPI-SSH starts, so DPI-SSH has no knowledge about whatever was exchanged before, including GSSAPI token. DPI-SSH will fail with the GSSAPI option enabled.

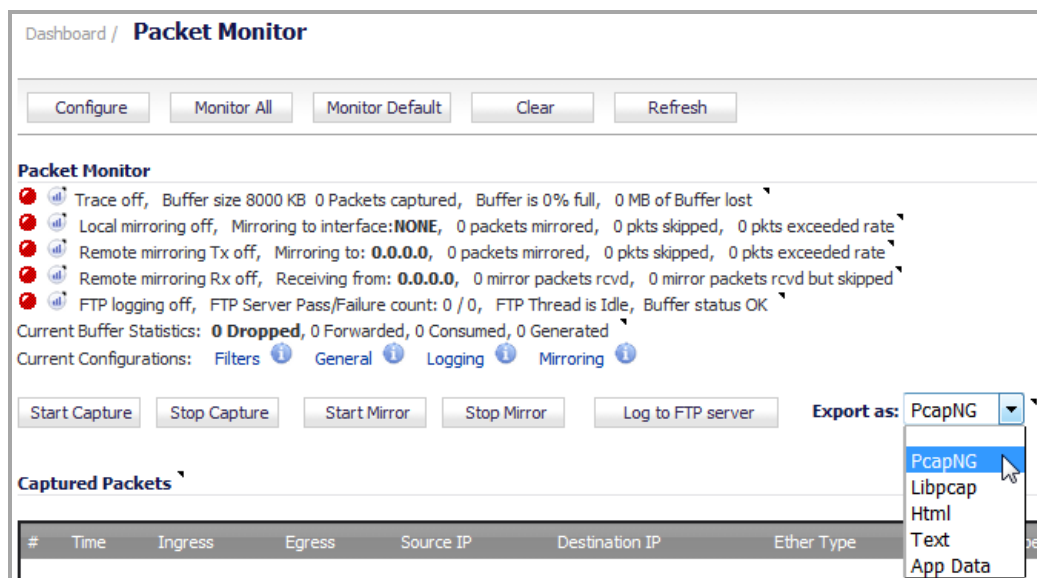
- On the client side, either the SSH 2.x or 1.x client can be used if DPI-SSH is enabled. However, clients with different version numbers cannot be used at the same time.
- Gateway Anti-Spyware and Application Firewall inspections are not supported even if these options are selected in the **DPI-SSH > Configure** screen.

Support for pcapNG

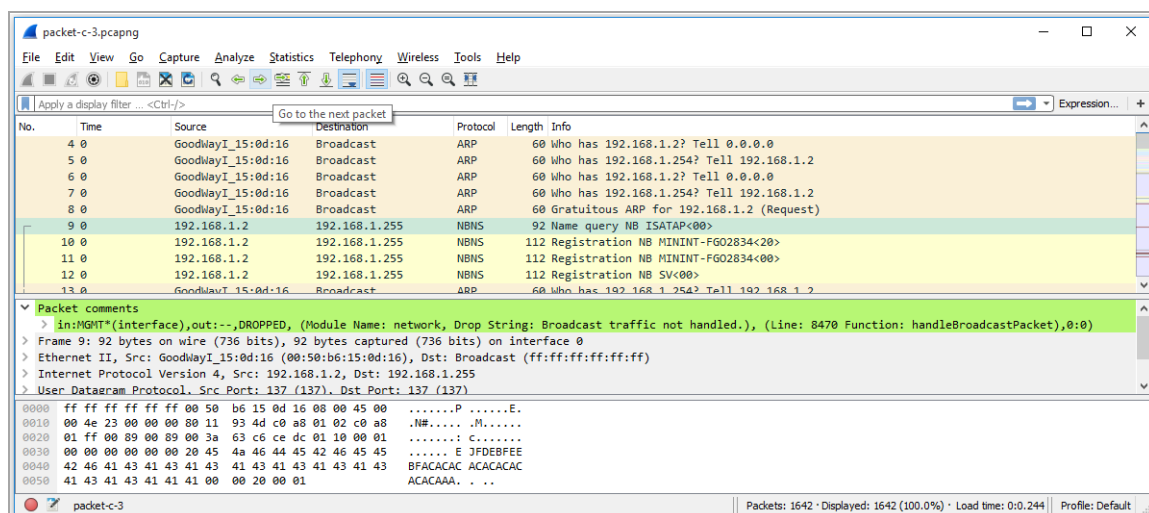
GMS 8.3 provides an option to export the pcapNG file on the packet monitor user interface. The pcapNG file can be directly opened by Wireshark and the new “Packet comments” section is displayed.

In previous releases, packet monitor export supports pcap, but the administrator must export pcap, HTML and text to find out the line number, in-interface, out-interface, and the function name which acted on the packet. This data is now available by exporting a single pcapNG file.

The **Dashboard > Packet Monitor** screen provides a new option to export the pcapNG file.



When the file is opened in Wireshark, the new Packet comments section is displayed.



TSR FTP for Periodic Backup

This feature allows administrators to send the configuration settings (prefs) and tech support report (TSR) to a specified FTP server. Admins can configure a schedule for periodic backup of this information to the FTP server.

To enable scheduled prefs and TSR backups:

- 1 Navigate to the **System > Settings** page.
- 2 Click the **Send by FTP** button. The **Schedule Reports** page displays.



The screenshot shows a window titled "Schedule Reports". At the top left is a "Set Schedule" button. Below it is a section titled "Actions" with two checkboxes: "Send Tech Report by FTP" and "Send Settings by FTP". Underneath are four input fields: "FTP Server:" with the value "0.0.0.0", "User name:" with "admin", "Password:" with "password", and "Directory:" with "reports". At the bottom are "Apply" and "Cancel" buttons.

- 3 Select **Send Tech Report by FTP** to send TSR.
- 4 Select **Send Settings by FTP** to send prefs.
- 5 Enter the required information for the FTP server.
- 6 Click **Set Schedule** to define a start schedule.
- 7 Click **OK** and then click **Apply**.

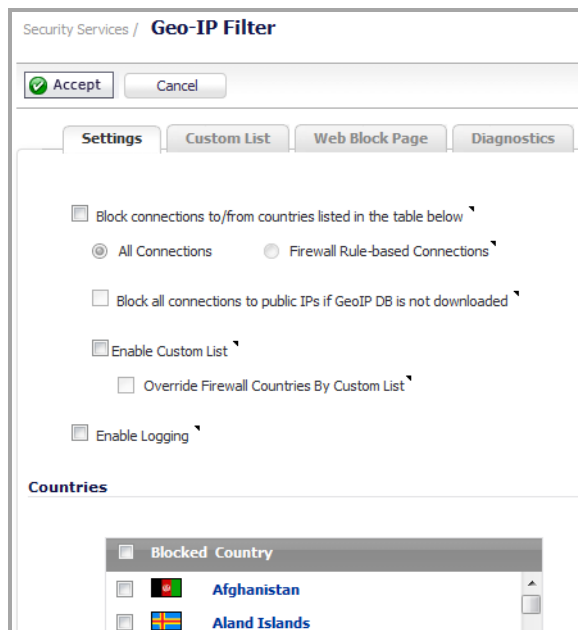
Custom Lists for Geo-IP and Botnet

GMS 8.3 provides new options to configure a custom country list for Geo-IP Filter and a custom botnet list for Botnet Filter.

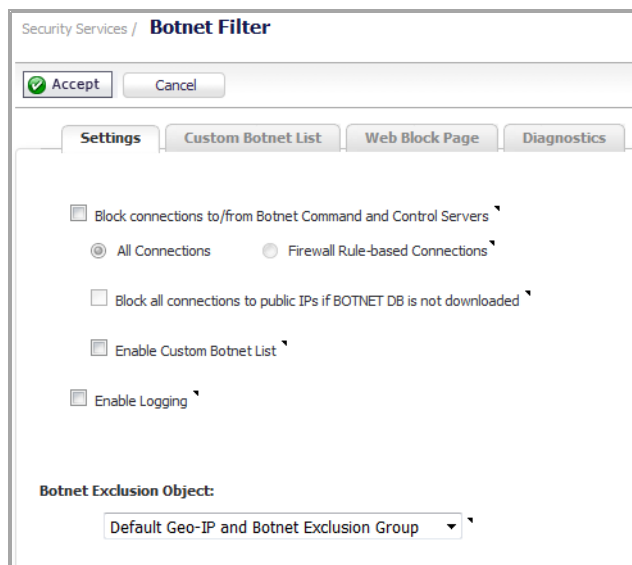
An IP address can be associated with a wrong country. This kind of misclassification can cause incorrect/unwanted filtering of an IP address. Having a custom country list can solve this problem. The custom country list overrides the firewall country associated with a particular IP address.

Similarly, an IP address can be wrongly marked as botnet. A custom botnet list can override the botnet tag for a particular IP address.

The **Security Services > Geo-IP Filter** page is changed for this new feature, and has four tabs with various configuration settings on each.



The **Security Services > Botnet Filter** page is similarly changed for this new feature, also with four tabs.



SIP UDP Fragmentation Fixes

In previous releases, the SIP transformation design and implementation does not handle fragmented SIP packets transported in UDP mode. A SIP/UDP signaling packet is fragmented when the SIP payload length is greater than the maximum MTU size of the network minus the size of the SIP packet headers. For example, for a commonly accepted maximum MTU size of 1514 bytes, if the SIP signaling packet payload length exceeds 1472 bytes, the SIP packet is dropped by GMS.

In GMS 8.3, SIP/UDP payload length is not restricted by the underlying MTU size on the network. This support is completely transparent to users. No configuration is required.

System Logs on AppFlow Server via IPFIX

In GMS 8.3, system logs can be sent to an external server via IPFIX packets and then saved into the database on the disk. The logs only include the ones which are reported WITHOUT connection cache. Users can edit the configuration in the **Log > Settings** page to indicate which log events should be sent.

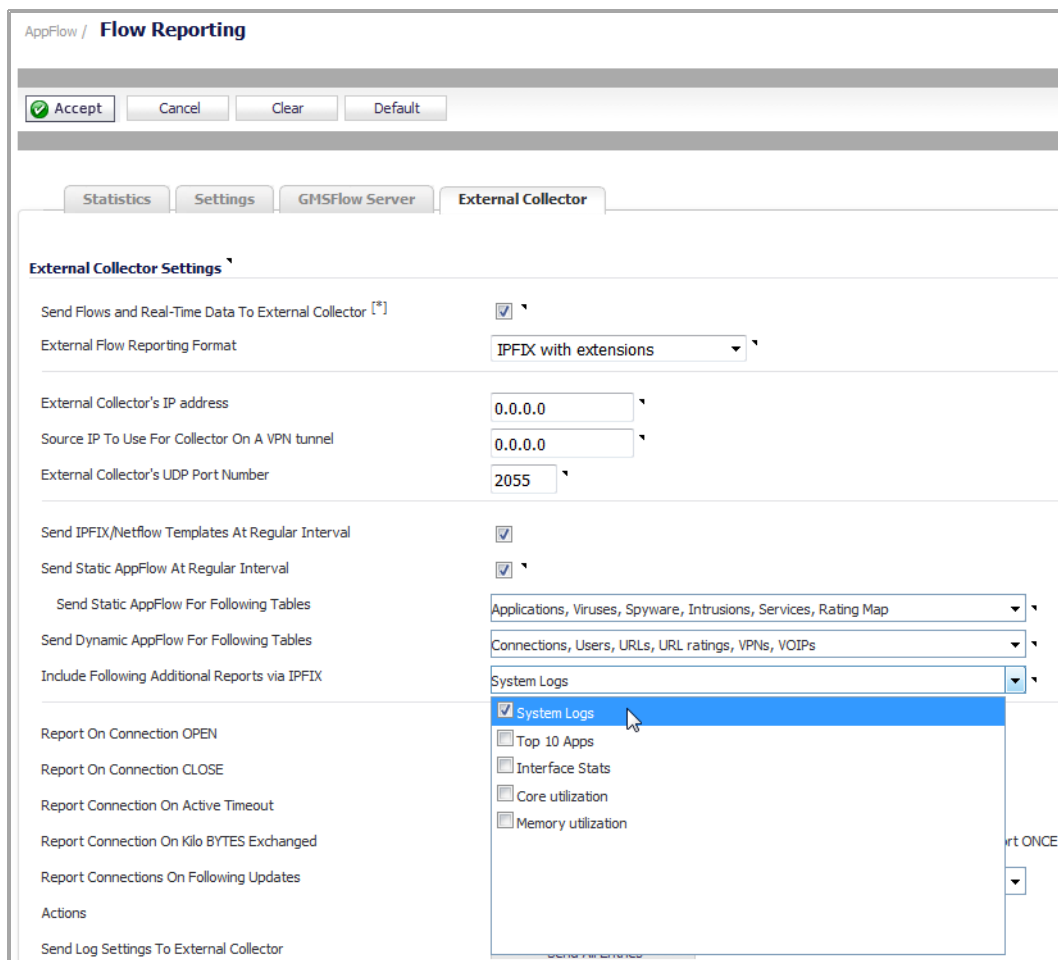
System logs include events that are typically not dependent on traffic flowing through the firewall. Such events are mostly flow (session/connection) related events.

System logs typically include, but are not limited to:

- Interface state change
- Fan failure
- User authentication
- HA failover and failback
- Tunnel negotiations
- System events such as configuration changes

Configuration options for this feature are on these pages:

- **AppFlow > Flow Reporting > External Collector** tab:



An important step is send log properties and some fields of log settings to the external collector. Make sure the connection between GMS and the external collector server is ready before clicking the **Send All Entries** button to send the settings.

Click the button again to sync the settings in the following cases:

- GMS is upgraded with some NEW added log events.
- The connection between GMS and the external server has been down for some time and log settings might have been edited in the period.
- **AppFlow > Flow Reporting > GMSFlow Server** tab:
Enable Logs in the **Include Following Additional Reports via IPFIX** drop-down list.
Click the **Synchronize Log Settings** button when ready.
- **AppFlow > Flow Reporting > AppFlow Server** tab:
Enable Logs in the **Include Following Additional Reports via IPFIX** drop-down list.
Click the **Synchronize Log Settings** button when ready.

NAT64: Stateful NAT from IPv6 Client to IPv4 Server

As a NAT64 translator, GMS 8.3 allows an IPv6-only client from any zone to initiate communications to an IPv4-only server with proper route configuration. It maps IPv6 addresses to IPv4 addresses so that IPv6 traffic changes to IPv4 traffic and vice versa. IPv6 address pools (represented as Address Objects) and IPv4 address pools are created to allow the mapping. An IP/ICMP translation algorithm is implemented to translate packet headers between IPv6 and IPv4. The IPv4 addresses of IPv4 hosts are translated to and from IPv6 addresses by using an IPv6 prefix configured in GMS. A DNS64 server is configured in the IPv6-only client, which creates AAAA records (IPv6 records) with A records (IPv4 records). GMS does not act as a DNS64 server.

This feature provides a way for administrators to configure a NAT64 policy in the same way as a regular NAT policy. In the policy, by configuring translated destination to Original in a 6to4 policy, GMS automatically translates IPv4-converted IPv6 addresses to IPv4 addresses. When adding a policy from the **Network > NAT Policies** page, select **NAT64 Only** for the **IP Version** field.

SONICWALL Network Security Appliance

General

NAT Policy Settings

IPv6 Original Source: --Select an address object --

Translated IPv4 Source: --Select an address object --

Pref64: --Select an address object --

Translated Destination: Embedded IPv4 Address

Original Service: ICMP UDP TCP

Translated Service: Original

Inbound Interface: Any

Outbound Interface: Any

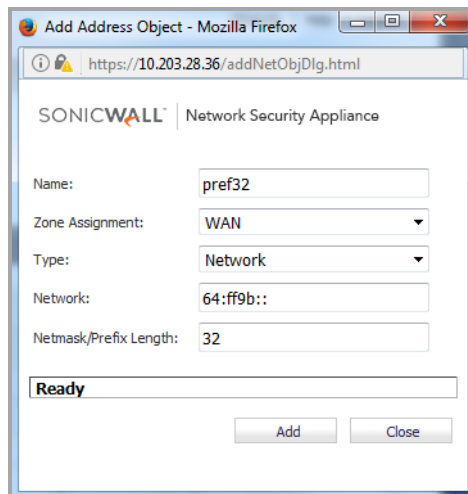
Comment:

IP Version: IPv4 Only IPv6 Only NAT64 Only

Enable NAT Policy

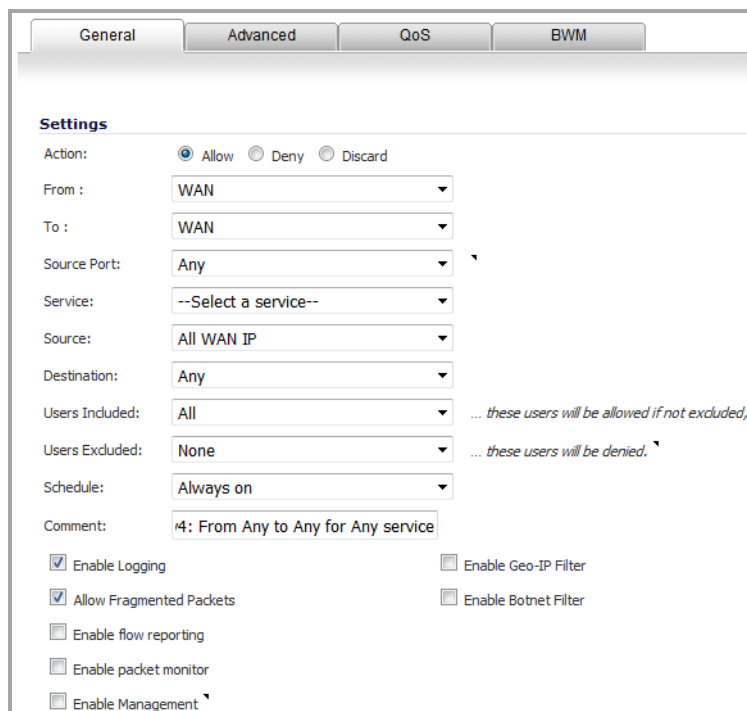
Create a reflexive policy

In GMS, an Address Object of Network type can be configured to represent all addresses with *pref64::/n* to represent all IPv6 client which can do NAT64. *Pref64::/n* defines a source network which can go from an IPv6-only client through NAT64 to an IPv4-only client.



A well-known prefix, **64:ff9b::/96**, is auto created by GMS.

Packets from an IPv6 client are originally from the LAN zone, but appear to be from the WAN zone after being translated by the NAT64 policy. To prevent GMS from dropping these packets in some cases, a new WAN to WAN allow rule policy should be created, such as:



Notes:

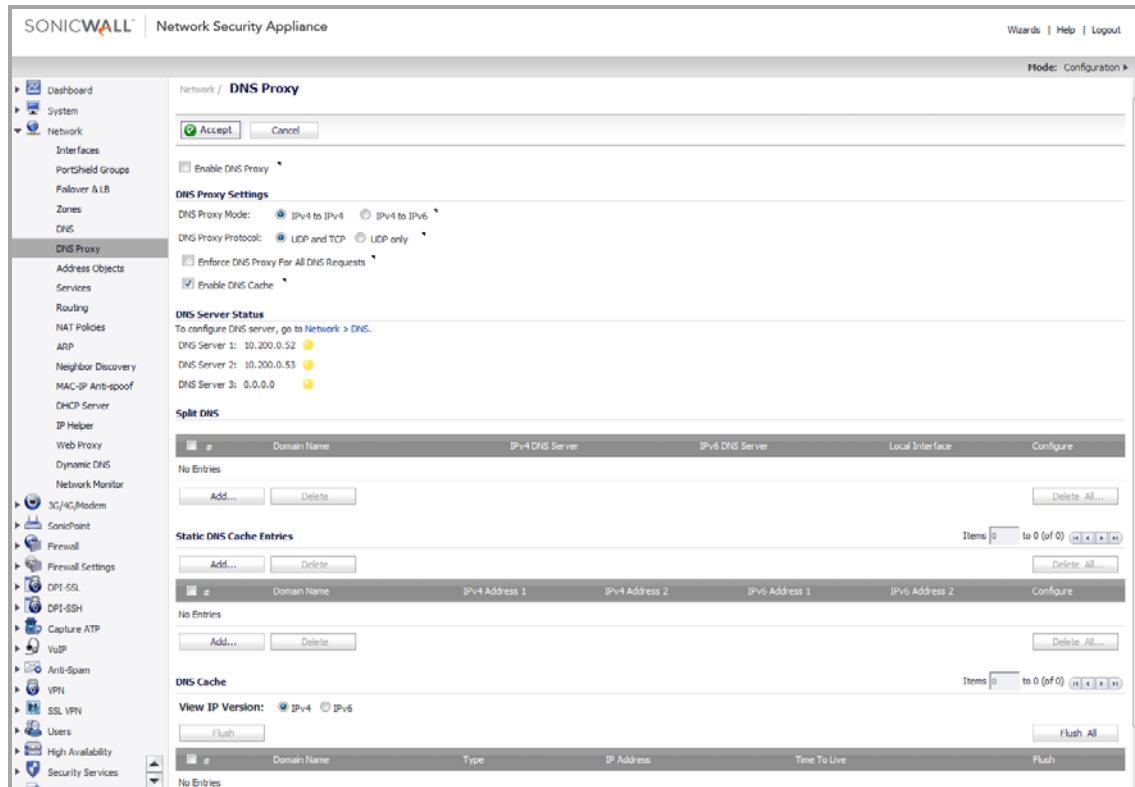
- NAT64 currently only translates unicast packets carrying TCP, UDP, and ICMP traffic.
- NAT64 currently supports FTP and TFTP application layer protocol streams. It currently does not support the H.323, MSN, Oracle, PPTP, RTSP, and RealAudio application layer protocol streams.
- NAT64 currently does not support IPv4-initiated communications to a subset of IPv6 hosts.

DNS Proxy

GMS 8.3 supports DNS proxy to allow IPv4 clients to access DNS services in a network with mixed IPv4 and IPv6.

In a normal deployment, an IPv4 interface can do name resolution on IPv4 internet, and an IPv6 interface can only do name resolution on IPv6 internet through DNS proxy.

A new page is added to the GMS web management interface, **Network > DNS Proxy**.



Select **Enable DNS Proxy** to globally enable the feature.

There are two modes for DNS proxy: **IPv4 to IPv4**, and **IPv4 to IPv6**. The default mode is IPv4 to IPv6, meaning that the firewall redirects queries from clients to upstream IPv6 DNS servers. For IPv4 to IPv4, the firewall redirects the queries to upstream IPv4 DNS servers.

Default option on DNS proxy protocol is **UDP and TCP**, which means when DNS query is sent over TCP, it will be proxied and retransmitted to outside DNS servers over TCP.

Enforce DNS Proxy For All DNS Requests is an enhanced option for DNS proxy. When the option is selected, other types of DNS queries are hooked by the DNS proxy module, including stack DNS packets sent by GMS, and forwarding DNS queries with destination address of outside DNS servers.

Interface Configuration and Allow Rules

GMS 8.3 supports the DNS proxy feature on physical interface, VLAN interface, or VLAN trunk interface, and the zone for each interface can only be LAN, DMZ or WLAN.

In the **Advanced** tab of the interface configuration page, there is a checkbox named **Enable DNS Proxy** when the interface permits configuring DNS proxy.

When DNS proxy is enabled on an interface, one Allow Rule is auto-added by GMS for UDP with the settings: From the interface to the interface, source with any and destination with the interface IP, service with DNS, and enable management. When **DNS Proxy over TCP** is enabled, another Allow Rule is auto-added.

DHCP

When DNS proxy is enabled on an interface, the device needs to push the interface IP as DNS server address to clients, so the GMS administrator needs to configure the DHCP server manually and use the interface address as the **DNS Server 1** address in the DHCP server settings on the **DNS/WINS** tab. The **Interface Pre-populate** check box in the DHCP page makes this easy to configure; if the selected interface has enabled DNS proxy, the DNS server IP is auto-added into the **DNS/WINS** page.

DNS Cache

In the **Network-> DNS Proxy** page, the DNS Cache function can be enabled by selecting the **Enable DNS Cache** checkbox; the default setting is enabled.

When enabling the function, GMS caches the answers from DNS responses during the DNS Proxy process, and will directly respond to clients if a subsequent DNS query matches the DNS cache.

There are two kinds of DNS cache: static DNS cache and dynamic DNS cache. Static DNS cache means that it can be manually created and edited by users, and never expires. Dynamic DNS cache is added automatically during the DNS proxy process, and it is displayed only in the whole DNS cache table. Its type is Dynamic, and has TTL value. Dynamic DNS cache can be flushed by the administrator.

Split DNS

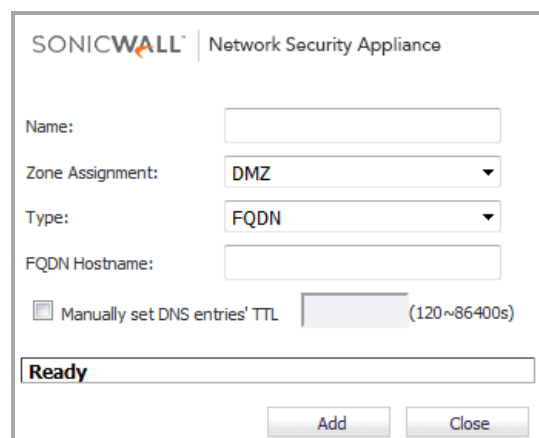
Split DNS is an enhancement for DNS proxy, which allows the administrator to configure a set of name servers and associate them to a given domain name (can be wildcard). When GMS receives a query that matches the domain name, it will be transmitted to the designated DNS server.

FQDN Routing

GMS 8.3 introduces Fully Qualified Domain Name (FQDN) support in Policy-based routing (PBR). The FQDN can be used as the source or destination of the PBR entry, and the PBR entry can be redistributed to advanced routing protocols.

Policy-based routing is a technique used to make routing decisions based on policies set by the network administrator. Policy-based routing may be based on the size of the packet, the source address, the protocol of the payload, or other information available in a packet header or payload.

The FQDN is added as an address object, which can then be used when configuring the policy. The FQDN object can contain both IPv4 and IPv6 hosts; the number of hosts in an FQDN object is variable. To configure an FQDN address object, select **FQDN** in the **Type** field and fill in the other fields.



The screenshot shows the configuration window for adding an FQDN address object in the SonicWall Network Security Appliance. The window title is "SONICWALL Network Security Appliance". The fields are as follows:

- Name:** An empty text input field.
- Zone Assignment:** A dropdown menu with "DMZ" selected.
- Type:** A dropdown menu with "FQDN" selected.
- FQDN Hostname:** An empty text input field.
- Manually set DNS entries' TTL:** A checkbox that is unchecked, followed by a text input field containing "120~86400s".
- Status:** A box containing the text "Ready".
- Buttons:** "Add" and "Close" buttons at the bottom.

Maximum Routes Doubled

This feature doubles the maximum number of static and dynamic routes supported by GMS. All platforms should maintain reasonable performance while adapting to dynamic routing changes when the maximum number of dynamic and static routes has been exploited. The GMS web management interface might respond more slowly during the adaptation period.

The TSR displays the maximum static and dynamic routes.

Maximum Zone to Zone Access Rules Increased

Previous versions of GMS do not allow the administrator to increase or decrease the Rule Table size. The Rule Table size for all the Zone-Zone pairs is fixed to a constant value based on the platform.

GMS 8.3 allows flexible Rule Table size for every Zone-Zone pair. The **Firewall > Access Rules** page is refreshed and has a layout similar to the **Firewall > Address Objects** page. The selected Zone-Zone rule table size is configured on the **Firewall > Access Rules** page.

Maximum Policies

Platform	Max Size per Zone-Zone Rule Table
SuperMassive 9200/9400/9600	5000 rules
NSA 2600/3600/4600/5600/6600	2500 rules
TZ 300/400/500/600 Series	1250 rules
SOHO Wireless	250 rules

Flow Reporting using IPFIX Extension Version 2

GMS 8.3 introduces support for IPFIX with Extension v2. The flow reporting format to the GMS Flow Server (collector) in earlier SonicOS versions uses the IPFIX with Extension format (version 1) by default. In SonicOS 6.2.7, you can customize flow reporting to report in either IPFIX with Extension (v1) or IPFIX with Extension v2.

The new format uses variable length fields, which is much more memory efficient than sending static fields and will vastly reduce the amount of information transmitted over the network.

In IPFIX with Extension v2, many new fields have been added to convey more information about the firewall, and some redundant or unnecessary fields have been removed. The additional data in these new fields will enrich the GMS Flow Server's visualization capabilities. The GMS Flow Server supports the IPFIX with Extension v2 format beginning in SonicWall GMS 8.3. SonicWall GMS 8.2 or earlier releases only supported the IPFIX with Extension (v1) format.

The administrator can select **IPFIX with Extension v2** for the **GMS FS Reporting Format** option in the **AppFlow > Flow Reporting** page, **GMSFlow Server** tab. A similar option is added on the **AppFlow Server** tab. To see these fields, you must enable an internal setting. Contact SonicWall Support for information about how to enable this. See <https://support.sonicwall.com/contact-support> for Support phone numbers.

Syslog Server Profiling

This feature provides the ability to configure the settings for each Syslog server independently instead of using the global settings for all the servers. In previous releases, the events generated from all the modules in the system are reported to **all** the configured Syslog servers. Depending on the deployment, this generates a huge amount of Syslog traffic and can cause performance issues or even packet loss.

With Syslog Server Profiling, the following new functionality is available:

- Syslog messages can be sent using different settings for different Syslog servers
- There can be multiple groups of Syslog servers
- Different events can be configured to be reported to different groups of Syslog servers

All the settings in the **Log > Syslog** page except the **Enable NDPP Enforcement for Syslog Server** checkbox can now be configured for each row independently in the **Syslog Servers** table. This allows the Syslog messages to be rendered with different settings for different servers and each server can have its own Rate Limiting options.

The newly added **Enable** checkbox can be used to enable or disable sending of Syslog messages to a specific Syslog server. The settings for Enhanced Syslog and ArcSight format can also be configured individually and the corresponding buttons are shown in the **Log > Syslog** page.

All these settings can be configured from the SonicOS web interface and from the command line interface (CLI.) For convenience, the global settings can be used to configure all servers.

i | **NOTE:** The **Override Syslog Settings with Reporting Software Settings** option has been removed. Since the Syslog servers can have their own independent settings, this option is no longer needed.

Event Profile

The Event Profile is an integer and can range from 0 to 23. It can be used to combine multiple Syslog servers into a group. All Syslog servers in the group have the same Profile. There can be a maximum of 24 groups (0 to 23) and seven Syslog servers per group. Therefore, in total there can be a maximum of 168 Syslog servers.

A new column called **Event Profile** is added to the **Syslog Servers** table. This new field also belongs to the group key in addition to server name and port. So, instead of <Name, Port>, a <Name, Port, Profile> combination must be unique for each row in the **Syslog Servers** table. This allows multiple rows to have same <Name, Port> combination with different Profiles. This means one Syslog server can be part of multiple groups, if necessary.

The events in the **Log > Settings** page also have a configurable Event Profile. The Event Profile of an event can be set to any available group, causing the Syslog messages for that event to be sent only to that group of servers. If the Event Profile of an event is set to a group that does not exist in the **Syslog Servers** table, then no Syslog messages for that event are sent.

GMS

The GMS server has a fixed Syslog Facility (Local Use 0), Syslog Format (Default), and Server ID (firewall). Although the Event Profile value for GMS is set to 0 by default, all events are reported to GMS irrespective of the profile. GMS is also exempted from Rate Limiting. The newly added **Enable** checkbox does not apply. GMS can be enabled/disabled only in the **System > Administration** page and not in the **Log > Syslog** page.

When GMS is enabled, the GMS server is added to the Event Profile 0 group in the **Syslog Servers** table. It cannot be added to any other Profile groups. Therefore, only the Profile 0 group can have 8 servers in total (7 Syslog servers and 1 GMS server). All other groups can have only 7 servers. The events in the GMS group in the **Log > Settings** page have Profile 0 and cannot be changed. Other events can have a different Profile.

IPv6 Support

In GMS 8.3, IPv6 is supported on a number of additional features, as shown in this section.

SSL Control

GMS 8.3 introduces IPv6 support for SSL Control. No new options or settings have been added. Both IPv4 and IPv6 network traffic is inspected based on the settings in the **Firewall Settings > SSL Control** page.

IPv6 DPI-SSL

GMS 8.3 introduces IPv6 support for DPI-SSL. No new options or settings have been added. The settings on the **DPI-SSL > Client SSL** and **DPI-SSL > Server SSL** pages are now applied to both IPv4 and IPv6 network traffic.

IPv6 NTP

GMS 8.3 introduces support for NTP servers with IPv6 domain names or IP addresses. Administrators can now add IPv6 NTP servers in the **NTP Settings** section of the **System > Time** page.

IPv6 DNS

GMS 8.3 introduces IPv6 support for DNS.

To communicate with an IPv6 DNS server, first go to **Network > Interfaces** and configure a WAN interface with an IPv6 address, either as a static IP or through DHCPv6.

Then on the **Network > DNS** page, select the **IPv6** radio button for **View IP Version**. The display changes to allow input of IPv6 DNS server addresses, which can be entered manually or obtained dynamically from the WAN zone. Select **Prefer IPv6 DNS Servers** to make SonicOS send DNS requests to the IPv6 DNS servers first, and if that fails, send the request to the configured IPv4 DNS servers.

The **DNS Name Lookup** diagnostic tool on the **System > Diagnostics** page can be used to test the DNS servers. All four DNS diagnostic tools in previous releases are now integrated into **DNS Name Lookup**.

IPv6 MAC Address Object

GMS 8.3 introduces IPv6 support for MAC address objects. A MAC address object (AO) binds to the dynamic memory of host IP addresses. It is often used when defining access rules.

To create an IPv6 MAC AO, go to the **Network > Address Objects** page and click **Add**. Then select **MAC** in the **Type** field and enter the IPv6 MAC address in the **MAC Address** field. The configuration is basically the same as for an IPv4 MAC AO; no new options or settings have been added for configuring an IPv6 MAC AO.

IPv6 FQDN Address Object

GMS 8.3 introduces IPv6 support for FQDN address objects.

First, configure an IPv6 DNS server on the **Network > DNS** page. See [IPv6 DNS](#) for more information about this configuration.

To create an IPv6 FQDN AO, go to the **Network > Address Objects** page and click **Add**. Then select **FQDN** in the **Type** field and enter the IPv6 FQDN hostname in the **FQDN Hostname** field. The configuration is basically the same as for an IPv4 FQDN AO; no new options or settings have been added for configuring an IPv6 FQDN AO.

DPI-SSL Increased Connection Counts and Enhancements

GMS 8.3 increases the number of DPI-SSL connections available on TZ500 Series and TZ600 appliances.

In addition to the increase in connection counts, this feature provides the following enhancements for all platforms:

- Stability fixes related to race conditions
- Re-design of the initialization sequence
- Caching (both Session cache and Spoof cache) enhancements and optimizations

- Memory footprint reduction per connection leading to increased connection counts

Open Authentication Social Login

GMS 8.3 introduces support for Open Authentication Social Login.

Social Login

Also known as social sign-in, social login is a form of single sign-on using existing information from a social networking service such as Facebook, Twitter, or Google Plus to sign into a third party website instead of creating a new login account specifically for that website.

Open Authentication (OAuth)

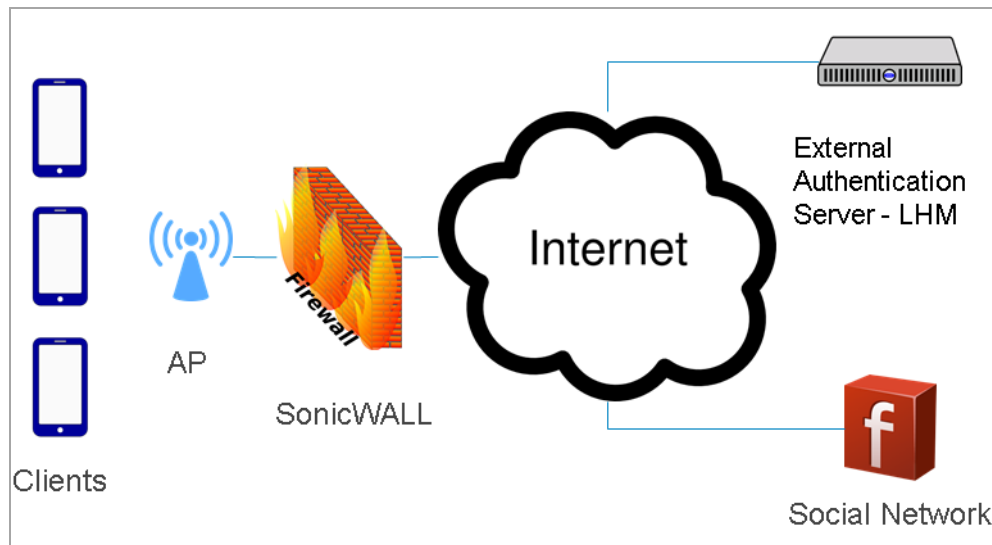
OAuth is an open standard for authorization. OAuth provides client applications a secure delegated access to server resources on behalf of a resource owner. It specifies a process for resource owners to authorize third-party access to their server resources without sharing their credentials.

OAuth Social Login is supported on SonicWall firewalls with internal wireless and SonicPoint, in the scope of wireless zone guest services. Wireless guest services are widely used in public WiFi hotspots and corporate WiFi for guests.

Facebook, Twitter, and Google Plus are supported in GMS 8.3. Within the SonicOS scope, social login is supported for wireless guests, not for GMS administrator login.

NOTE: Read the Open Authentication Social Login guidance from FaceBook/Google/Twitter and SonicWall before enabling this feature.

External Authentication Server Topology



GMS Settings

To enable social login in GMS:

- 1 Edit the WLAN zone and click the **Guest Services** tab.
- 2 Select the **Enable Guest Services** and **Enable External Guest Authentication** checkboxes.
- 3 Click **Configure** next to the **Enable External Guest Authentication** checkbox.
- 4 In the **Social Network Login** section on the **General** tab of the popup dialog, select the **Social Network Login** checkbox and then select one or more of the **Facebook**, **Google**, or **Twitter** checkboxes.
- 5 On the **Auth Pages** tab, enter the desired page name such as **login.php** in the **Login Page** field.

6 Click **OK**.

GMS automatically creates the necessary pass network domains for allowing authentication process traffic between the authentication server and the user. The automatically added address object group is named **Default Social Login Pass Group**. This address object group is appended to the current configured pass networks, if any, or added into a new group named **Social Login Pass Group**. The **Network > Address Objects** page shows these entries.

Facebook Settings

facebook for developers | Products Docs Tools & Support News | Search | My Apps

SonicWALL H... | Basic | Advanced | Migrations

Dashboard | Settings | App Review | App Details | Roles | Open Graph | Alerts | Localize

App ID: 85780088433318 | App Secret: [Masked] Show

Display Name: SonicWALL Hotspot | Namespace: [Empty]

App Domains: amazonaws.com | Contact Email: [Redacted]

Website: Quick Start | Site URL: http://amazonaws.com/

Client OAuth Settings

Client OAuth Login
Enables the standard OAuth client token flow. Secure your application and prevent token redirect URIs are allowed with the options below. Disable globally if not used.

Web OAuth Login For...
Enables web based OAuth client login for building custom login flows. [?]

Embedded Browser OAuth Login
Enables browser control redirect uri for OAuth client login. [?]

Valid OAuth redirect URIs
http://ec2-54-149-208-253.us-west-2.compute.amazonaws.com/facebookCallback.php

Updated SonicPoint Firmware

New SonicWall-branded firmware version 9.0.1.0-10 is available for SonicPoints connected to appliances running SonicOS 6.2.7.

Supported platforms are:

- SonicPoint ACe
- SonicPoint ACi
- SonicPoint N2

Your SonicPoint is automatically provisioned with the new firmware by GMS.

SonicPoint Radius Accounting

GMS 8.3 introduces support for Radius Accounting on SonicWall firewalls with a connected SonicPoint ACe, ACi, or N2, in the scope of IEEE 802.11i Enterprise Authentication.

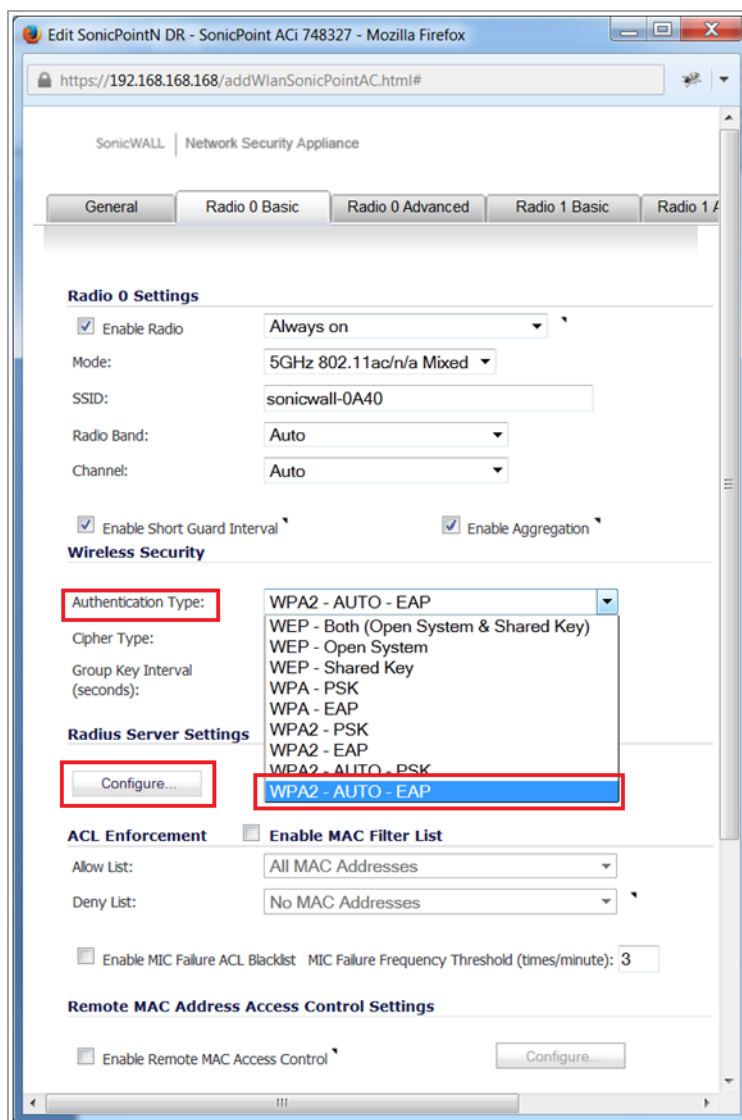
Radius Accounting uses the RADIUS protocol to deliver accounting information from a Network Access Server (NAS, a SonicPoint in our case) to the Radius Accounting Server (RAS). The GMS administrator can use the accounting information to apply various billing rules on the Radius Accounting server side, based on session duration time or traffic load being transferred for each individual user. Radius Accounting is the process of collecting and storing the information contained in the following system messages:

- Accounting-Start
- Accounting-Stop

GMS Settings

To configure Radius Accounting:

- 1 On the **SonicPoint > SonicPoints** page, click the **Configure** button for your SonicPoint.



- 2 Under **Radius Server Settings**, click **Configure**.

- 3 In the configuration dialog, enter the correct **IP**, **Port**, and **Secret** (password) for the Radius Accounting Server and Radius (Authentication) server.

NOTE: The Radius Accounting Server and Radius (Authentication) Server do not need to be located at the same IP.

- 4 Click **OK** to provision the SonicPoint ACe/ACi/N2.

Radius Server Settings

The Radius Server needs to be configured accordingly to turn on accounting support.

To configure freeradius 2.1.10 fto turn on accounting support:

- 1 Add the Radius client entry into the file `/etc/freeradius/clients.conf`:

```
Client 10.103.12.192 {
    Secret= "password"
}
```

NOTE: 10.103.12.192 is the WAN IP of the SonicWall Gateway from which the Radius Server can be reached.

- 2 Add the user information into the file `/etc/freeradius/users`:

```
user_name Cleartext-Password := "password"
```

- 3 Run the command `sudo freeradius -X` in the terminal to start freeradius.

31-Bit Network

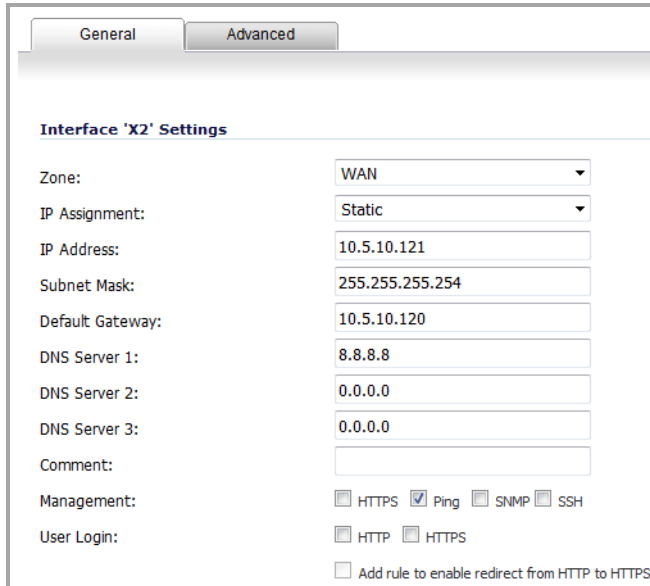
GMS 8.3 introduces support for RFC 3021, which defines the use of a 31-bit subnet mask. This mask allows only two host addresses in the subnet, with no “network” or “gateway” address and no broadcast address. Such a configuration can be used within a larger network to connect two hosts with a point-to-point link. The savings in address space resulting from this change is easily seen, each point-to-point link in a large network would consume two addresses instead of four.

In this context, the point-to-point link is not equivalent to PPP (point to point protocol). The point-to-point link using a 31-bit mask can use or not use the PPP protocol. 31-bit prefixed IPv4 addresses on a point-to-point link can also be used in the Ethernet network.

Configuring GMS

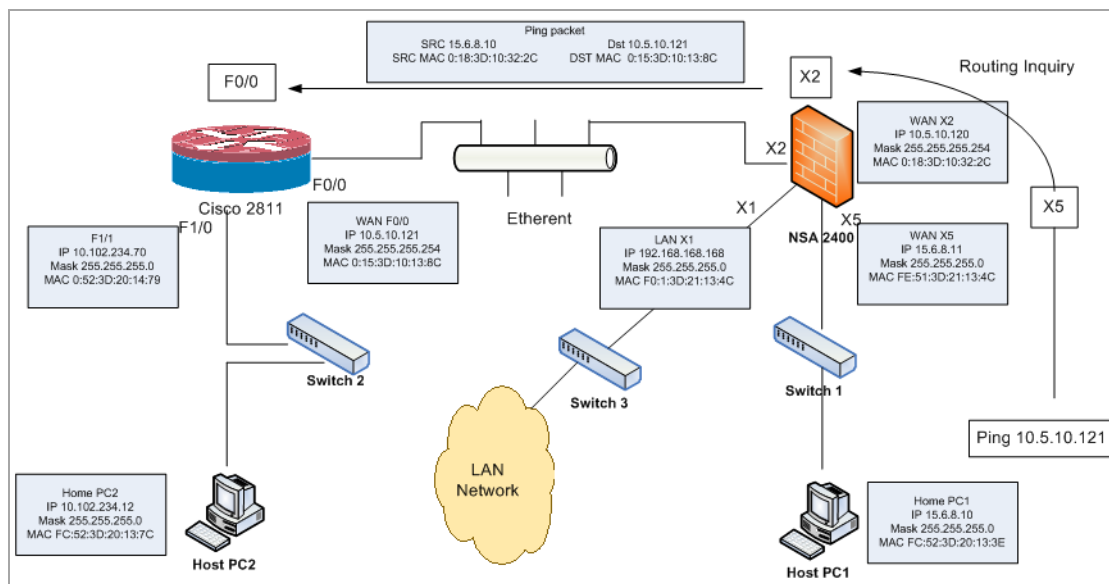
To configure an interface for a 31-bit subnet:

- 1 On the **Network > Interfaces** page, edit the desired interface.
- 2 Set the **Subnet Mask** to **255.255.255.254**.



- 3 Enter one host IP address into the **IP Address** field.
- 4 Enter the other host IP address into the **Default Gateway** field.
- 5 Set the other fields according to your network, as needed.
- 6 Click **OK**.

Example Network Environment



In this network environment, Host PC1 and Host PC2 can use visit each other, while hosts in the LAN network can visit Host PC2.

To configure settings for this environment:

1 For Host PC1, add two route entries:

- `Route add 10.5.10.0 mask 255.255.255.0 15.6.8.10`
- `Route add 10.102.234.0 mask 255.255.255.0 15.6.8.10`

2 For Host PC2, add two route entries:

- `Route add 10.5.10.0 mask 255.255.255.0 10.102.234.70`
- `Route add 15.6.8.0 mask 255.255.255.0 10.102.234.70`

3 On the Cisco router (F0/0):

- `interface fastEthernet 0/0`
- `ip address 10.5.10.120 255.255.255.254`

4 On the Cisco 2811, add one route entry:

```
!  
ip route 15.6.8.0 255.255.255.0 10.5.10.120  
!
```

5 On the firewall, add one route entry to enable the WAN zone data flow from X2 to X5, and X5 to X2:

```
Any 10.102.234.0 Any X2 Default Gateway X2
```

Threat API

GMS 8.3 introduces support for the Threat API feature. The GMS Threat API provides API access to SonicWall firewall services. Compared with current firewall GUI/CLI user interfaces, the Threat API is simple and makes good use of the standard HTTP protocol. With the trend toward cloud deployment, the Threat API can more easily be used than the traditional GMS GUI/CLI.

Malicious threats can originate from URLs or IP addresses. Lists of these threats can be large and change frequently. GMS can already block custom lists of URLs and IP addresses, it's just inconvenient because a human has to log in and update the lists by hand. Using an API interface makes it much easier.


The Threat list is sent to GMS using the Threat API. Threats can be added in either of the following formats:

- URLs (<https://malicious123.example.com/malware>)
- IP addresses (10.10.1.25)

Third parties can generate the threat list and pass it to the firewall using Threat API.

For IP addresses in the threat list, GMS initially creates a default Threat API Address Group and then creates an Address Object (AO) for each IP address in the threat list. The SonicOS administrator configures Firewall Access Rules that reference that Address Group and block the IP addresses.

GMS adds the URLs to its CFS Threat URI list. The GMS administrator enables Threat API Enforcement in the associated CFS Profile and configures a Content Filtering System (CFS) policy to block the URLs in the threat list.

 **NOTE:** SonicOS Threat API requires that the firewall has a Content Filtering System (CFS) license.

When a threat is blocked by CFS, the user will see a block message in their browser:



GMS Web UI Updates for Threat API

NOTE: Threat API settings are only available to the GMS administrator. By default, this is the “admin” user.

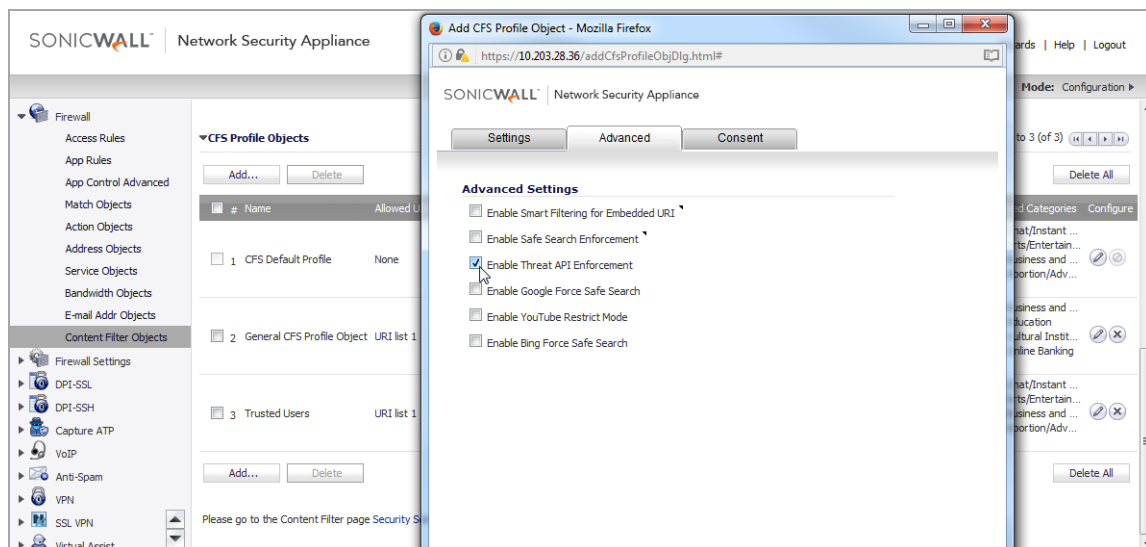
Internal Setting

A new internal setting is added for Threat API:

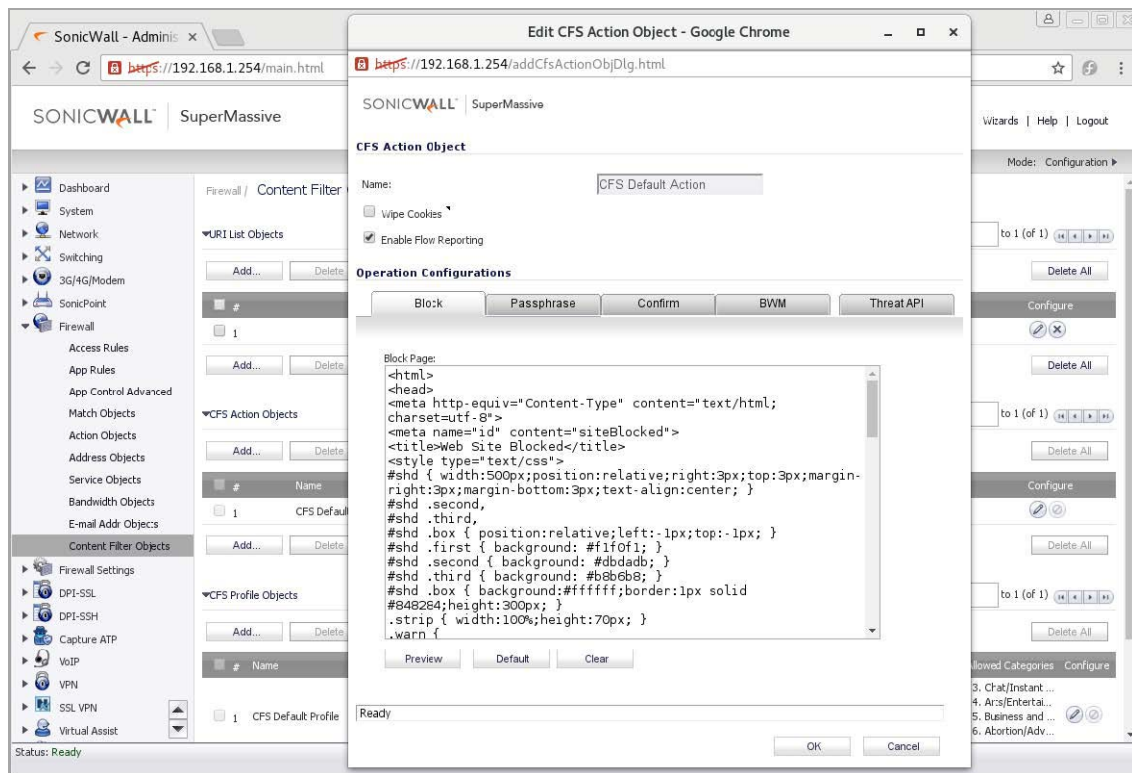
- **Enable Threat API Filtering** – Global Threat API enable/disable setting

Firewall > Content Filter Objects Settings

When adding or editing a CFS Profile Object on the **Firewall > Content Filter Objects** page, the **Advanced** tab has a new **Enable Threat API Enforcement**. After GMS receives the initial threat list and creates a Threat URI List Object, the admin adds a CFS Profile Object that references the Threat URI List Object and enables **Enable Threat API Enforcement**.



The **Firewall > Content Filter > Action Objects** page provides a way to configure a custom Threat API Block Page on a granular per CFS Action Object basis.



API Authentication

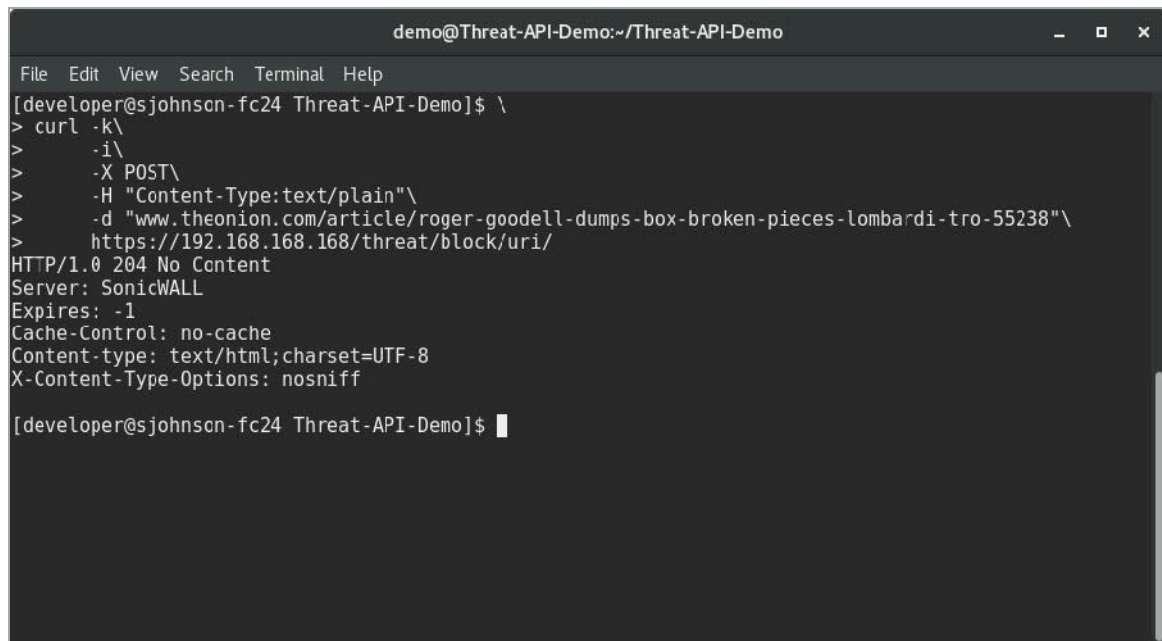
All the API commands listed below require HTTP Basic Authentication for every API call. User credentials are not stored.

API Commands

- GET */threat/block/uri/* – Returns URI blocklist in a simple plain-text, 1 URI per line format.
- OPTIONS */threat/block/uri/* – Allows restricted resources on a web page to be requested from another domain outside the domain from which the first resource was served.
- POST */threat/block/uri/* – Instantiates the URI blocklist.
- DELETE */threat/block/uri/* – Clears the URI blocklist.
- GET */threat/block/ip/* – Returns host IP blocklist in a simple plain-text, 1 V4/V6 host per line format.
- OPTIONS */threat/block/ip/* – Allows restricted resources on a web page to be requested from another domain outside the domain from which the first resource was served.
- POST */threat/block/ip/* – Instantiates the host IP blocklist.
- PUT */threat/block/ip/* – Adds host(s) to the IP blocklist.
- DELETE */threat/block/ip/* – Deletes all or specified host(s) from the IP blocklist.

Threat API Examples

Example 1: A Threat API call requesting to block a URL pointing to an article:



```
demo@Threat-API-Demo:~/Threat-API-Demo
File Edit View Search Terminal Help
[developer@sjohnson-fc24 Threat-API-Demo]$ \
> curl -k\
> -i\
> -X POST\
> -H "Content-Type:text/plain"\
> -d "www.theonion.com/article/roger-goodell-dumps-box-broken-pieces-lombardi-tro-55238"\
> https://192.168.168.168/threat/block/uri/
HTTP/1.0 204 No Content
Server: SonicWALL
Expires: -1
Cache-Control: no-cache
Content-type: text/html;charset=UTF-8
X-Content-Type-Options: nosniff
[developer@sjohnson-fc24 Threat-API-Demo]$
```

Example 2: Instantiate IP & URI block lists:

```
curl -k -i -u admin:password -X POST -d "`printf "1.2.3.4\n1.2.3.5\n"`"
https://192.168.1.254/threat/block/ip/
```

Another example for this:

```
curl -k -i -u admin:password -X POST -d "`printf
"example1.com\nexample2.com\n"`" https://192.168.1.254/threat/block/uri/
```

Example 3: Update list by adding an entry to IP block list:

```
curl -k -i -u admin:password -X PUT -d "`printf "4.3.2.1\n"`"
https://192.168.1.254/threat/block/ip/
```

Example 4: Delete IP & URI entries:

```
curl -k -i -u admin:password -X DELETE -d "`printf "1.2.3.4\n1.2.3.5\n"`"
https://192.168.1.254/threat/block/ip/
```

Another example for this:

```
curl -k -i -u admin:password -X DELETE
https://192.168.1.254/threat/block/uri/
```

Biometric Authentication

GMS 8.3 introduces support for biometric authentication in conjunction with SonicWall Mobile Connect.

Mobile Connect is an app that allows users to securely access private networks from a mobile device. Mobile Connect 4.0 supports using finger touch for authentication as a substitute for username and password.

GMS 8.3 provides configuration settings on the **SSL VPN > Client Settings** page to allow this method of authentication when using Mobile Connect to connect to the firewall.

To enable biometric authentication:

- 1 On the **SSL VPN > Client Settings** page, click the **Configure** button for the **Default Device Profile**.
- 2 On the **Client Settings** tab, select **Enabled** for one or both of the following settings:
 - **Allow Touch ID on IOS devices**
 - **Allow Fingerprint Authentication on Android devices**
- 3 On the client smartphone or other mobile device, enable Touch ID (iOS) or Fingerprint Authentication (Android).

Ensure that Mobile Connect 4.0 or higher is installed on the mobile device, and configure it to connect with the firewall.

VPN Auto Provisioning

GMS 8.3 introduces the VPN Auto Provisioning feature. This feature provides automatic VPN provisioning for box-to-box hub-and-spoke configurations. The user experience is similar to that seen when using SonicWall Global VPN Client to connect from a client machine to a firewall, in which none of the complexity is visible to the user.

Minimally, only two pieces of information are required to configure a spoke appliance when using VPN Auto Provisioning:

- The peer gateway address or domain name
- The machine authentication credentials

By selecting the **Default Provisioning Key** option, machine authentication credentials can be based on a default value known to all the appliances. To increase security, user level credentials may also be required.

VPN Auto Provisioning can be used when adding a VPN Policy in the **VPN > Settings** page. In the Add dialog under **Security Policy**, select either:

- **SonicWall Auto Provisioning Client**

The screenshot shows the 'Security Policy' configuration page. It is divided into three sections: 'Authentication Method', 'SonicWall Settings', and 'User Settings'.
1. **Authentication Method:** A dropdown menu is set to 'SonicWall Auto Provisioning Client'. Below it are empty text boxes for 'Name' and 'IPsec Primary Gateway Name or Address'. The 'Authentication Method' radio buttons are set to 'Preshared Secret'.
2. **SonicWall Settings:** Includes a text box for 'VPN AP Client ID', a checkbox for 'Use Default Provisioning Key' (which is unchecked), text boxes for 'Shared Secret' and 'Confirm Shared Secret', and a checked checkbox for 'Mask Shared Secret'.
3. **User Settings:** Includes a text box for 'User Name' containing 'admin', a text box for 'User Password' with masked characters, and a checked checkbox for 'Mask User Password'.

- **SonicWall Auto Provisioning Server**

The screenshot shows a configuration window with two tabs: 'General' and 'Network'. The 'Network' tab is active. Under the 'Security Policy' section, the 'Authentication Method' dropdown is set to 'SonicWall Auto Provisioning Server'. Below it is an empty 'Name' field. The 'Authentication Method' radio buttons are set to 'Preshared Secret'. Under the 'SonicWall Settings' section, the 'VPN AP Client ID' field contains 'admin'. There is a checkbox for 'Use Default Provisioning Key' which is unchecked. The 'Shared Secret' field is masked with 12 dots. Below it is a 'Confirm Shared Secret' field which is empty, and a checked checkbox for 'Mask Shared Secret'. An 'Advanced...' button is at the bottom left.

4 Configure the other fields as needed.

Resolved Issues

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

Console panel

Resolved issue	Issue ID
Use of the inheritance filter returns a “No dependent objects found” message. Occurs when inheriting all objects within the filter.	170235

Firewall configuration

Resolved issue	Issue ID
GMS presents the default certificate instead of showing the custom certificate. Occurs when using the Login to Unit feature.	181943

Heterogenous Management

Resolved issue	Issue ID
The drill-down feature is not functioning correctly for failed login reports. Occurs when the user name contains special characters.	179204

Inheritance

Resolved issue	Issue ID
Interconnected VPN SA is being overwritten during inheritance. Occurs when creating an additional interconnected VPN SA at the group level.	183784

Policies panel

Resolved issue	Issue ID
Deleting a Wireless > Guest Services profile just schedules the task without completing it. Occurs when deleting the profile at the group level.	181627
Uploading firmware images fails in GMS. Occurs when uploading at the group level.	179637

Reporting

Resolved issue	Issue ID
Flow and Capture Reports appear to be missing. Occurs after upgrading to 8.2.	184121
Customers with larger hard drives are restricted by the 10 percent hard drive limitation for Syslog reporting. Occurs with customers who possess larger hard drives still being restricted to the spacial requirements of smaller storage drives.	152782

Tree control

Resolved issue	Issue ID
Tree Control does not load correctly. Occurs after upgrading to GMS 8.2.	181895

Universal dashboard

Resolved issue	Issue ID
The USR/UDB screen does not load correctly and the page shows up as code. Occurs when navigating in the Geo-IP map area in UDB or in the Scheduling a Report for Email area in USR.	175498

Workflow

Resolved issue	Issue ID
Interfaces created with Workflow/Change Orders do not generate the normal default objects. Occurs when creating new interfaces.	167619
Change Order creation fails. Occurs when the Change Order task description contains a single quote character.	157921

Known Issues

The following is a list of issues known to exist at the time of the GMS 8.3 release.

Policies panel

Known issue	Issue ID
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
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
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
Forward Inheritance at 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
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
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
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

Reports panel

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

Tree control

Known 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

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 8.3 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 2](#). 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 8.3, 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

Supported platforms

The SonicWall GMS supports the following Microsoft Windows operating systems:

- 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

Use the [Capacity Calculator 2](#) 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 6.0 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

Use the [Capacity Calculator 2](#) 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, or if you want to use the “Login to Unit” right-click menu of TreeControl.

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 8.3 does not support legacy SonicWall appliances, including:

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

SonicWall GMS 8.3 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: <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://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 8.3 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.

Non-SonicWall appliance support

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

Upgrading to GMS 8.3

This section provides procedures for upgrading an existing SonicWall GMS 8.2 or newer installation to GMS 8.3.

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 8.3 can be installed as a fresh install or as an upgrade from GMS 8.2. If you wish to perform a fresh install of GMS 8.3, refer to the *GMS Getting Started Guide* that relates to your GMS deployment.

Consider the following before upgrading to GMS 8.3:

- The 40GB GMS Virtual Appliance should be installed in non-production environments only. Examples of non-production environments include those for Proof of Concept (POC), pilot, and demo deployments. Only the 250GB and 950GB virtual appliances are supported in production environments. It is not possible to upgrade a 40GB virtual appliance to a 250GB or 950GB virtual appliance. You need to download the 250GB or 950GB virtual appliance if you are planning to use this software now or in the future for a production environment.
- In non-production environments, the amount of syslog data collected by the virtual appliance may exceed the 40GB limit, in which case SonicWall will be unable to support the 40GB virtual appliance.
- 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 8.3 logs into the appliances using HTTPS only.
- The scheduled reports created in GMS 8.0 continue to work properly after upgrading to 8.3. 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 8.3 and others running 8.2.

i **NOTE:** DO NOT start/stop the SonicWall Universal Management Suite - Database service manually, before or after upgrading to 8.3. 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 8.3, complete the following steps:

- 1 Navigate to www.mysonicwall.com.
- 2 Download the GMS 8.3 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.

Upgrading the GMS virtual appliance

This section provides procedures for upgrading an existing SonicWall GMS 8.2 virtual appliance or newer installation to GMS 8.3 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 8.3 and others running 8.2.

NOTE: DO NOT start/stop the SonicWall Universal Management Suite - Database service manually, before or after upgrading to 8.3. 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 8.3 64-bit Virtual Appliance, refer to the *GMS Virtual Appliance Getting Started Guide*.

To upgrade, complete the following:

- 1 Download the GMS 8.3 file from www.mysonicwall.com to your workstation software:
`sw_gmsvp_vm_eng_8.3.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 support 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://support.sonicwall.com>.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- Download software
- View video tutorials
- Collaborate with peers and experts in user forums
- Get licensing assistance
- Access MySonicWall
- Learn about SonicWall professional services
- Register for training and certification

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


Copyright © 2017 SonicWall Inc. All rights reserved.

This product is protected by U.S. and international copyright and intellectual property laws. SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.


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/>.

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: 3/31/17

232-003845-00 Rev A