



Dell SonicWALL™ Global Management System (GMS) 8.0

Release notes

June 2015


These release notes provide information about the Dell SonicWALL™ Global Management System (GMS) 8.0 release.

- [About Dell SonicWALL GMS 8.0](#)
- [New features](#)
- [Resolved issues](#)
- [Known issues](#)
- [Platform compatibility](#)
- [Upgrading to GMS 8.0](#)
- [Technical support resources](#)
- [About Dell](#)



About Dell SonicWALL GMS 8.0

GMS 8.0 is a major release, with new features and functionality. See [New features](#).

Dell SonicWALL GMS can be used in a variety of roles in a wide range of networks. Network administrators can use Dell SonicWALL GMS in a *Management Console role* in an Enterprise network containing a single Dell 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.

 **NOTE:** All fixes in the 7.2 Service Packs (SP1, SP2, SP3, and SP4) are included in this 8.0 release.

Before upgrading to GMS 8.0

-  **CAUTION:** If you have an UMA EM5000 appliance or a Windows 32-bit GMS Server currently in your deployment, you must migrate them first to a Windows 64-bit GMS server or decommission these systems, before upgrading to v8.0.
-  **CAUTION:** If you are upgrading to GMS v8.0 and still have CDP appliances under management, those appliances will automatically be removed from GMS after the upgrade.

See the [Upgrading to GMS 8.0](#) section for more information.

New features

This section describes the new features included in the GMS 8.0 release:

- **Change Order Management and Work Flow**—GMS 8.0 introduces a workflow automation feature that assures the correctness and the compliance of policy changes by enforcing a process for configuring, comparing, validating, reviewing and approving policies prior to deployment. The approval groups are user-configurable for adherence to company security policy. All policy changes are logged in an auditable form that ensures the firewall complies with regulatory requirements. This feature provides the ability to infer what would end up on the unit as part of a task and then validate that configuration based on what is presently on the unit and what is then going to be pushed to the unit. The changes can then be optionally approved by a set of users before they get deployed, through the WorkFlow mechanism. All granular details of any changes made are historically preserved to help with compliance, audit trailing, and troubleshooting.
- **Java Applet Replacement**—The TreeControl application (that displays all managed appliances) and the User Management application (**Console > Management > Users**) have now been replaced with non-Java versions. All Java applets in the front-end have been removed, except for NetMonitor and the "Login to Unit" feature from TreeControl.
- **SonicOS Support**—New features in SonicOS 6.2 are supported.
- **Portuguese Support**—The Login screen now includes version information and indicates Brazilian Portuguese support.
- **Access Rules**—The Access Rules screen now allows users to update Address Objects, Address Groups, Service Objects, and Service Groups all from the same Access Rules screen instead of jumping to separate screens to carry out these operations.
- **Reporting**
 - **Report Database Rebuild Utility**—The Reporting Database Rebuild Utility allows you to submit a request to rebuild any specific month's report table if it were to become corrupt.
 - **Report Data Optimization**—In previous versions, report data optimization exported sorted report data into a file and reloaded that data back to the report database. In GMS 8.0, instead of using a file to upload the data, a temporary table is created that exports and reimports that data, leading to better performance.
 - **Botnet Reports**—Botnet reporting is added to the Reports panel and includes four report types: Attempts, Targets, Initiators, and Timeline.
 - **Geo IP Reports**—Geo IP reports contain information on blocked traffic that is based on the traffic's country of origin or destination. Geo IP Reporting is added to the Reports panel and includes four report types: Attempts, Targets, Initiators, and Timeline.
 - **MAC Address in Reporting**—This feature shows the Media Access Control (MAC) address on the report page. This adds detail to the current device-specific information in the report panel and the PDF report. New columns "Initiator MAC" and "Responder MAC" are added to the following reports:
 - Data Usage > Initiators
 - Data Usage > Responders
 - Data Usage > Details
 - User Activity > Details
 - Web Activity > Initiators
 - **Enhanced Reporting Database**—The Reporting Database has been upgraded to a newer version that offers better performance and higher reliability.
 - **Distributed Universal Scheduled Report**—PDF report generation is now distributed and uses an engine that can make better use of your CPU and RAM resources, resulting in faster delivery of scheduled reports with larger volumes and more rows of data.
- **CSV File Import for IPS Signatures**—You can import configurations of your IPS signatures (such as Block vs. Logged, and so on) from a spreadsheet in CSV format.

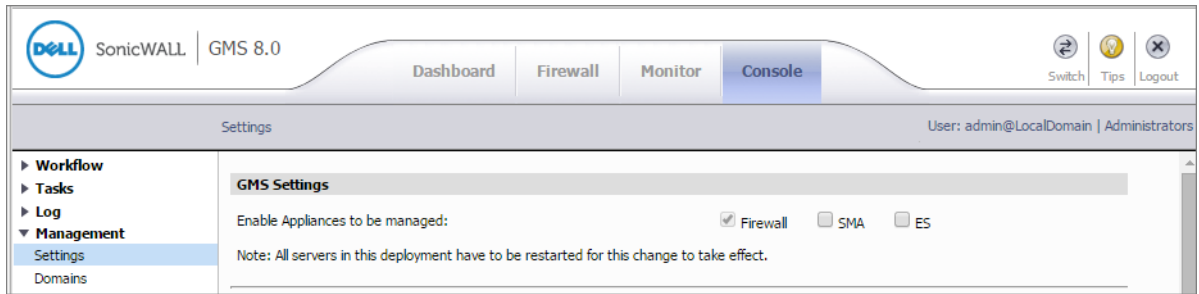
- **Enhanced USR Template Manager**—In addition to the PCI Report template, HIPAA and SOX templates are added to Universal Scheduled Reports as an aid for compliance audits.
- **Signature Details**—You can view the details of any signature matched with the new “Show Signature details” or “Show Spyware Signature details” right-click options.
- **Update at Unit-And-One-Level-Up Permission**—The “Update At Unit and One Level Up” option is an addition to the existing screen permissions for users and user types, which now include:
 - None
 - View Only
 - Update at Unit Level Only
 - Update at Unit and One Level Up
 - Update at All Levels

The new permission is especially useful in the management of firewalls that are distributed geographically and where each location uses high availability (HA) or a handful of firewalls with similar policies and configurations, and where technicians are allocated to those geographic locations to make such changes.

In these deployments, technicians are given permission to make changes to the firewall at the Unit and Group levels, as long as that Group level is just one level higher than the firewall level, as it would be on an immediate parent node on a firewall or unit node. Technicians for these deployments do not normally have full permissions at the higher level nodes; however, they can have full permissions at the unit and the unit’s parent node levels.

- **USR-Customizing Sorting Option in PDF**—Provides additional sorting options for Scheduled PDF reports.
- **Improved Inheritance Filters**—In earlier versions of GMS, when a screen was selected for inheritance, GMS automatically selected dependent screens so that a comprehensive list of interdependent screens was included in the filter. For instance, selecting an Access Rule screen for inheritance would automatically select dependent screens such as Zones, Address Objects, Service Objects, and so on. This was not only confusing, but it also led to undesirable end results. To inherit a few rules, GMS inherited all Zones, Address Objects, and Service Objects even when they did not need to be inherited. In GMS 8.0, the filters have been enhanced to address these limitations: selecting a filter does not additionally select the dependent screens, which minimizes confusion. Instead, GMS automatically determines which objects are needed to be inherited, and inherits only those dependent objects instead of all the objects from dependent screens. If you are upgrading from a version prior to GMS 8.0, your old filters will remain intact - to take advantage of this more intuitive approach in GMS 8.0, you will need to re-create your filters.
- **Log Analyzer**—The Firewall > Reports > Analyzers > Log Analyzer page has been updated with an out-of-the-box default view.
- **TLS Support in Emails**—Provides support for Microsoft Office 365 and Gmail.
- **Packet Data Viewer for Signature Alerts**—Provides the functionality to view the data packets that triggered the Intrusion event eliminating the need to use external utilities such as Wireshark, and so on. This advanced functionality allows you to further fine-tune the security policy for your network.
- **Granular Configuration of Syslog Filters**
 - GMS Super admin user can now enable or disable the default syslog filters defined by GMS and Analyzer products. This gives greater control to the kind of syslogs that the customer wants to store and report against.
 - Comment field has been added to describe the filter and the also the creator. Comments possible for Syslog filters.
- **Number of Syslogs collected per file**—This advanced configuration parameter for fine tuning the GMS deployment for performance is now exposed in the user interface. The default configuration is set to 100,000 syslogs per file.
- **Support for Firewall’s Native Backup/Restore Functionality**—In GMS 8.0, you can now perform a System Backup of the firmware image on a firewall, if the firewall supports this functionality. Using GMS 8.0, you can also boot such firewalls using their System Backup image. This functionality is provided in GMS 8.0 in the Policies Panel > Register/Upgrades > Firmware Upgrade screen, in the “System Backup” section.
- **All Windows Modules of GMS 8.0 are now 64-bit**—Provides better usage of system resources and better performance.

- High-level User Interface Changes



- Secure Remote Access (SRA) has been renamed to Secure Mobile Access (SMA).
- The CDP tab is removed.
- SRA and ES tabs are no longer shown by default, but can be activated on Console > Management > Settings.
- **Discontinued View Attributes**—The following Attributes can no longer be used to create your Views - these have been discontinued because these were associated with older firewalls or discontinued features:
 - Enable Anti-Virus Client Automated Enforcement
 - Network Type
 - PKI Status
 - VPN Present
 - Instance Name
- New Diagnostics > Cluster Status screen

Features changed or removed in GMS 8.0

- Screen Groups and Screens Removed
 - WGS Screen Group
 - WGS > Settings
 - WGS > URL Allow List
 - WGS > IP Deny List
 - WGS > Custom Log
 - WGS > External Authentication
 - WGS > Profiles
 - Application Filters Screen Group
 - Application Filters > Settings
 - Application Filters > Category Sets
 - Application Filters > Ports
 - Network > Settings
 - Network > Switch Ports
 - System > Licensed Nodes
 - Log > Log Settings
 - Content Filter > CFL Filter List
 - Content Filter > CFS Standard
 - Firewall > Services
 - Firewall > Rules
 - Users > ULA Settings
 - Network > Intranet
 - Network > Routing
 - Network > RIP
 - Network > DMZ Addresses
 - Network > One-to-One NAT
 - Network > Ethernet
 - DHCP > Setup
 - VPN > Configure
 - VPN > ULA Settings

- Web Filters > Settings
- Web Filters > Policies
- Web Filters > Custom Categories
- Web Filters > Miscellaneous
- Web Filters > Custom Block Page
- Policies > Policy List
- Users > HTTP URL ULA
- Security Services > Email Filter
- Hardware Failover > Monitoring
- Screens renamed
 - Log > "Enhanced Log Settings" renamed to "Log Settings"
 - Log > "Enhanced Log Categories" renamed to "Log Categories"
 - Content Filter > "Websense" renamed to "Websense Enterprise"
 - Network > "Routing (ENH)" renamed to "Routing"
 - Network > "RIP (ENH)" renamed to "RIP"
 - Screen group "Hardware Failover" renamed to "High Availability"
 - VPN > "Configure 2.0" renamed to "Configure"
- Changes to sections within screens
 - The "Add User" section of the **Users > Settings** screen has been removed from GMS.
 - In the **Firewall > Policies > Content Filter > Custom List** screen, the Timing (Filter List/URL Keywords/Custom Sites) section has been removed from the screen.
 - In the **Firewall > Policies > Wireless > IDS** screen, the SonicOS Standard references (visible at group/global levels) has been removed.
 - In the **Console > Tasks > Default Tasks** screen, the task titled "Setup minimal Syslog Categories for reporting Gen 3 Units" has been removed and the remaining tasks for Gen 3 have been renamed and have no reference to Gen 3, such as "Setup minimal Syslog Categories for reporting."
- Console Management screen ordering changes
- Firewall Access Rules screen renamed to HTML5
- Packet Viewer Functionality in Log Viewer

Resolved issues

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

Table 1. Appliance resolved issues

Resolved issue	Issue ID
GMS does not allow enough backup copies. Occurs when using the Auto Export Tool, backup copies are limited to 10 copies.	153246

Table 2. Application Control resolved issues

Resolved issue	Issue ID
Blocking advanced application control at the application level in GMS does not function correctly. Occurs when an application is modified, the entry is made to the Applications Table but the row is updated based on values in the preferences file.	159608

Table 3. Event Management resolved issues

Resolved issue	Issue ID
UP or DOWN unit status alerts are sent after a server restart. Occurs when a service is restarted on all units managed by a Scheduler that was also restarted.	158550

Table 4. Policies Panel resolved issues

Resolved issue	Issue ID
Zone information fails to synchronize. Occurs when the length of the custom header/footer specified in Guest Services has exceeded 55 characters.	157612
Local administrative rights are lost for the firewall. Occurs when creating local groups in GMS.	153378

Table 5. SNMP resolved issues

Resolved issue	Issue ID
GMS is sending an incorrect SNMP alert; "Alert: Element "% Current Connections" is greater than 95" even though the connection shows less than that on the firewall. Occurs when the agent is started with intervals prefilled with a zero.	149658

Table 6. Tree Control resolved issues

Resolved issue	Issue ID
The Modify Unit window is not shown and the Login to Unit window is not working correctly. Occurs when the pipe character is present in the unit password.	156664

Table 7. Unit Acquisition resolved issues

Resolved issue	Issue ID
Unable to open the Email Security tab in GMS (Management > User Interface) and an incorrect error message appears. Occurs when version certificates are in conflict.	157575

Table 8. Universal Scheduler resolved issues

Resolved issue	Issue ID
USR permissions cannot be assigned to any user (including other administrators). Occurs when creating a group level report by the default administrator.	151203

Known issues

The following is a list of issues known to exist at the time of the GMS 8.0 release.

Table 9. Reporting known issues

Known issue	Issue ID
The Top Threats SRA Signatures, Classification, and Severity columns are shown with the same threat IDs instead of displaying different names, classes, and severity levels. Occurs when selecting Policies > WAF > Threats Prevented.	160842

Table 10. Policies panel known issues

Known issue	Issue ID
In System > Tools > Inherit Settings at Unit (IPv4), the Reverse Inheritance option fails from unit to group and all other units. Occurs when using the VPN filter for reverse inheritance.	161370
GMS returns errors during OSPF v2 Inheritance configuration. Occurs when configuring the OSPF v2 for Inheritance with the "Enable Auto Cost" check box selected.	160665
The Trusted DHCP Relay Agent List settings fail to reverse inheritance to other units in a specific group. Occurs when selecting the Enable Trusted DHCP Relay Agent List option in Firewall > Policies > DHCP > Trusted Agents.	160443

Table 11. User interface known issues

Known issue	Issue ID
Landing page shows the error message "Loading, please wait..." or goes white without explanation. Occurs when a user with insufficient permissions or privileges logs in to GMS.	161161

Table 12. Workflow known issues

Known issue	Issue ID
Changing a Guest Services profile fails when clicking the Configuration icon in Firewall > Policies > Users > Guest Services. Occurs when the Task Description contains a single quote character.	157921
The Super Admin can disable Workflow without following the correct process. Occurs when the Super Admin disables the Workflow feature without an approved change order going through Workflow.	157537
Change Order related audit logs should not be deleted. Occurs when the Delete Log Messages Older Than action is performed from the Console > Configuration screen.	154789
GMS incorrectly displays the "Upgrade process completed" message. Occurs when exiting the Workflow free trial activation screen.	152932
On the Console > Workflow > Change Orders page, the Change Order on Approval option can unexpectedly change to the Not Approved state. Occurs when using Internet Explorer 11.	150018

Platform compatibility

The Dell SonicWALL GMS 8.0 release can be hosted in two deployment scenarios as follows:

- Microsoft Windows Server Software
- VMware ESX/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: Dell 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 8.0, 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](#)
- [MySQL requirements](#)
- [Microsoft SQL server requirements](#)
- [Java support](#)
- [Dell SonicWALL appliances supported for GMS management](#)

Supported platforms

The Dell 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
- Windows Server 2008 R2 Datacenter
- Windows Server 2008 SBS R2 64-bit
- Windows Server 2008 R2 Standard 64-bit
- Windows Server 2008 SP2 64-bit
- Windows Server 2003 64-bit (SP2)

The above Windows systems can either run in physical standalone hardware platforms, or as a virtual machine under Hyper-V or ESXi.



TIP: 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.

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 *Dell 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:

Table 13. 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 Dell SonicWALL GMS Virtual Appliance. The GMS Virtual Appliance runs on the following VMware platforms:

- ESXi 4.1, 5.0, 5.1 and 5.5
- ESXi 4.0 Update 1 (Build 208167 and newer)
- ESX 4.1
- ESX 4.0 Update 1 (Build 208167 and newer)

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 *Dell SonicWALL GMS Administration Guide*.

Browser requirements



Dell SonicWALL GMS uses advanced browser technologies such as HTML5, which are supported in most recent browsers. Dell SonicWALL recommends using the latest Chrome, Firefox, Internet Explorer, or Safari browsers for administration of the Dell 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 10.0 or higher (do not use compatibility mode)

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

i **NOTE:** Turn off Compatibility Mode when accessing the GMS management interface with Internet Explorer.

Mobile device browsers are not recommended for Dell SonicWALL GMS system administration.

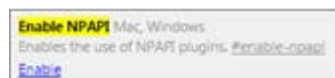
i **NOTE:** If using Chrome version 42 and newer to access GMS 7.2 and older, you will need to enable NPAPI support in Chrome, which by default has been disabled starting with version 42.

To enable NPAPI support, complete the following steps:

- 1 In your URL bar, enter:

```
chrome://flags/#enable-npapi
```

- 2 Click **Enable** for the **Enable NPAPI** configuration option:



- 3 Click **Relaunch Now**, which now appears at the bottom of the configuration page.



MySQL requirements

GMS automatically installs MySQL as part of the base installation package. Separately installed instances of MySQL are not supported with GMS.

Microsoft SQL server requirements

The following SQL Server versions are supported:

- SQL Server 2012
- SQL Server 2008
- SQL Server 2005

i **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.

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

Java support

i **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 7 or 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>

Dell SonicWALL appliances supported for GMS management

i **NOTE:** GMS 8.0 does not support legacy SonicWALL appliances, including:

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

Dell SonicWALL GMS 8.0 supports the following Dell SonicWALL appliances and firmware versions:

Table 14. Component requirements

Dell SonicWALL platforms	Dell SonicWALL firmware version
Network security appliance	
SuperMassive 10000 Series	SonicOS 6.0 or newer
	i 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 8.0: <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 Dell SonicWALL Sales representative for more information.

SuperMassive 9000 Series	SonicOS 6.1 or newer
NSA Series	SonicOS 5.0 or newer
TZ Series	SonicOS 5.0 or newer
Email Security/Anti-Spam	
Email Security Series	Email Security 7.2 or newer (management only)
Secure Mobile Access	
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
SMA 6200/7200	SMA 10.7.2 or newer

Notes:

- GMS 8.0 supports Dell 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-Dell SonicWALL appliance support

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

Upgrading to GMS 8.0

This section provides procedures for upgrading an existing Dell SonicWALL GMS 7.2 or newer installation to GMS 8.0. GMS can be configured for a single server or in a distributed environment on multiple servers. GMS 8.0 can be installed as a fresh install or as an upgrade from GMS 7.2. If you wish to perform a fresh install of GMS 8.0, refer to the *GMS Getting Started Guide* that relates to your GMS deployment.

Consider the following before upgrading to GMS 8.0:

- 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 Dell 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 8.0 logs into the appliances using HTTPS only.

- The scheduled reports created in GMS 7.2 continue to work properly after upgrading to 8.0. 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, stop all GMS services on all GMS servers before performing an upgrade. You must upgrade all GMS servers in your deployment to the same version of GMS. You cannot have some servers running version 8.0 and others running 7.2.

Upgrading procedure

To upgrade to GMS 8.0, complete the following steps:

- 1 Navigate to www.mysonicwall.com.
- 2 Download the GMS 8.0 software.
- 3 After the file has downloaded, double-click the 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 Once the installer has completed, reboot the system to complete the installation.

Upgrading the GMS virtual appliance

The GMS Virtual Appliance can be upgraded from 7.2 to 8.0, but cannot be directly upgraded from GMS versions earlier than 7.2. To upgrade the GMS Virtual Appliance from a version earlier than 7.2, you need to upgrade to major versions of GMS until you reach 7.2, then you can upgrade to GMS 8.0. For Dell SonicWALL GMS Virtual Appliance deployments, upgrading from the GMS 7.2 release to the GMS 8.0 release can be performed on the **System > Settings** page.

In a distributed environment, shut down all GMS servers except the one that is running the database. Then upgrade the Console/AIOP first and then the other servers. You must upgrade all GMS servers in your deployment to the same version of Dell SonicWALL GMS 8.0. You cannot have some servers running version 7.2 and others running 8.0.

For a fresh install of the GMS 8.0 64-bit Virtual Appliance, refer to the *GMS Virtual Appliance Getting Started Guide*.

To upgrade, complete the following:

- 1 Download the GMS 8.0 file from www.mysonicwall.com to your workstation:
- 2 `sw_gmsvp_vm_eng_8.0.xxxx.yyyy.gmsvp-updater.64bit.sh`
- 3 Log in to the /appliance (System) interface of the GMS server.
- 4 Navigate to the **System > Settings** page.
- 5 Click **Browse**, navigate to the location where you saved the above file, and select it.
- 6 Click **Apply** to begin the firmware upgrade installation.
- 7 The Virtual Appliance reboots at the end of the installation process.

Technical support resources

Technical support is available to customers who have purchased Dell software 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. In addition, the portal provides direct access to product support engineers through an online Service Request system. To access the Support Portal, go to <http://software.dell.com/support/>.

The site enables you to:

- Create, update, and manage Service Requests (cases)
- View Knowledge Base articles
- Obtain product notifications
- Download software. For trial software, go to Trial Downloads.
- View how-to videos
- Engage in community discussions
- Chat with a support engineer

Dell SonicWALL reference documentation is available on the Dell Software Support site:

<https://support.software.dell.com/sonicwall-gms/release-notes-guides>

The screenshot shows the Dell SonicWALL GMS Release Notes and Guides page. The navigation bar includes 'Software', 'Products', 'Solutions', 'Buy', 'Trials', and 'Support'. A search bar is located in the top right corner. The main content area is titled 'SonicWALL GMS - Release Notes and Guides' and features a filter section for 'Virtual Appliance' and 'All categories'. Below the filter, there are sections for 'Administration Guide', 'Best Practices', and 'Configuration Guide', each listing documents with 'pdf' links. On the right side, there are two sidebars: 'Self Service Tools' with links like 'Download New Releases', 'Knowledge Base', 'My Support', 'Product Support', 'Professional Services', 'Training & Certification', 'Technical Support Forum', and 'Video Tutorials'; and 'Featured Content' with links like 'Community Forum', 'MySonicWALL', 'Support Offerings', and 'Support Guide'.

Datasheets, white papers, and other product information are available on the Dell Software Products website:

<http://software.dell.com/products/network-security-management-reporting/>

Knowledge articles and links to related community forums and other resources are available at:

<https://support.software.dell.com/sonicwall-gms/>

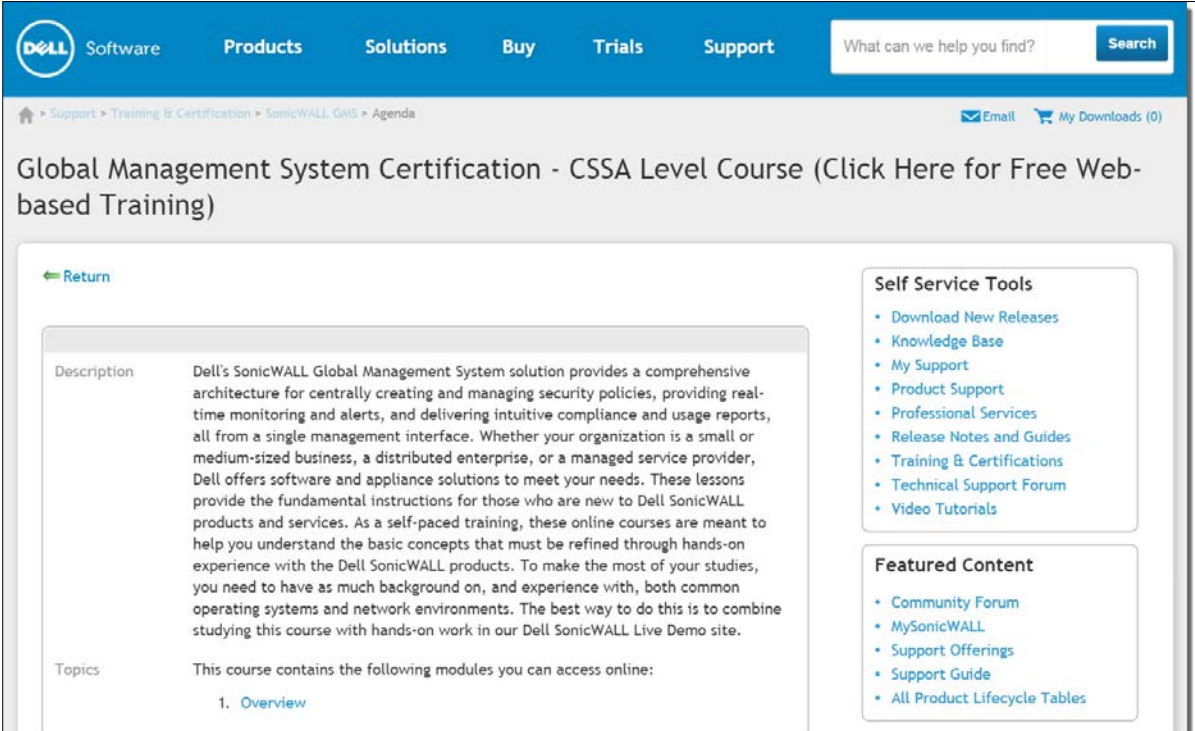
Online training materials

Dell SonicWALL Technical Training Services offers GMS software for essential security administrator certification. This Certified Dell SonicWALL Security Administrator (CSSA) course provides fundamental instructions to help you understand the basic deployment best practices for Managed Security Service Providers.

The following link provides the latest information regarding Dell SonicWALL GMS eLearning courses:

<https://support.software.dell.com/training-product-select>

Click **Find Your Course** and search for **Global Management System Certification Training**.



The screenshot shows the Dell SonicWALL support website interface. At the top, there is a navigation bar with links for Software, Products, Solutions, Buy, Trials, and Support. A search bar is located on the right side of the navigation bar. Below the navigation bar, the breadcrumb trail reads: Support > Training & Certification > SonicWALL GMS > Agenda. The main heading is "Global Management System Certification - CSSA Level Course (Click Here for Free Web-based Training)". Below the heading, there is a "Return" link. The main content area is divided into two columns. The left column contains a "Description" section with text about the course and a "Topics" section with a link to "1. Overview". The right column contains two sections: "Self Service Tools" with links for Download New Releases, Knowledge Base, My Support, Product Support, Professional Services, Release Notes and Guides, Training & Certifications, Technical Support Forum, and Video Tutorials; and "Featured Content" with links for Community Forum, MySonicWALL, Support Offerings, Support Guide, and All Product Lifecycle Tables.

About Dell

Dell listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit www.software.dell.com.

Contacting Dell

Technical support:

[Online support](#)

Product questions and sales:

(800) 306-9329

Email:

info@software.dell.com

Third-party contributions

This product contains third-party components. For third-party license information, go to: <http://software.dell.com/legal/license-agreements.aspx>. Source code information for open-source components is available at: <http://opensource.dell.com>.

© 2015 Dell Inc.
ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Dell Inc.

The information in this document is provided in connection with Dell 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 Dell products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, DELL ASSUMES 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 DELL 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 DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Dell does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Dell Inc.
Attn: LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656

Refer to our web site (software.dell.com) for regional and international office information.

Patents

For more information, go to <http://software.dell.com/legal/patents.aspx>.

Trademarks

Dell, the Dell logo, and SonicWALL are trademarks of Dell Inc. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims any proprietary interest in the marks and names of others.

Legend



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



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



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

Last updated: 6/16/2015

232-002889-00 Rev B