Release Notes

Management and Reporting

Dell SonicWALL GMS 7.2 Release Notes

Contents

Platform Compatibility

The Dell SonicWALL GMS 7.2 release can be hosted in three deployment scenarios as follows:

- Microsoft Windows Server Software
- VMware ESX/ESXi Virtual Appliance
- UMA EM5000 Universal Management Appliance

Deployment Considerations:

- Before selecting a platform to use for your GMS deployment, please use the Capacity Calculator 2. This helps you setup the correct GMS system for your deployment.
- It is highly recommended that steps are taken 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).

Microsoft Windows Server Operating Systems

The Dell SonicWALL GMS supports the following Microsoft Windows operating systems:

- Windows Server 2012 Standard 64-bit
- Windows Server 2008 SBS R2 64-bit
- Windows Server 2008 R2 Standard 64-bit
- Windows Server 2008 SP2 64-bit
- Windows Server 2003 32-bit and 64-bit (SP2)

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.

Hardware for Windows Server

Use the Capacity Calculator 2 to determine the hardware requirements for your deployment.

Note: A Windows 64-bit operating system with at least 8-GB of RAM is highly recommended for better performance of reporting modules. Please read the “Capacity Planning and Performance Tuning” appendix in the *GMS Administrator’s Guide*.

Hard Drive HDD Specifications

The following hard drive HDD specifications are required when using GMS software:

- **Spindle Speed** : 7200 and higher
- **Cache**: 64MB and higher
- **Transfer rate**: 600 MB/s or higher
- **Average Latency**: 4 ms 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, and 5.1
- ESXi 4.0 Update 1 (Build 208167 and newer)
- ESX 4.1
- ESX 4.0 Update 1 (Build 208167 and newer)

Virtual Appliance Deployment Considerations

Please 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
  - 16 GB of memory
  - 300 HDD

GMS Virtual Appliance Hardware Resource Requirements

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.

Starting with GMS 7.1 the Virtual Appliances are 64-bit, which take advantage of additional RAM available to it. A minimum of 4 GB RAM is required. However, at least 8 GB of RAM is highly recommended for better performance of reporting modules. Please read the “Capacity Planning and Performance Tuning” appendix in the *GMS Administrator’s Guide*.

Hard Drive HDD Specifications

The following hard drive HDD specifications are required when using the GMS Virtual Appliance:

- **Spindle Speed** : 7200 and higher
- **Cache**: 64MB and higher
- **Transfer rate**: 600 MB/s or higher
- **Average Latency**: 4 ms or lower

UMA EM5000 Requirements

The GMS 7.2 release is supported on the Dell SonicWALL UMA EM5000 Universal Management Appliance. The 3.1 GB of RAM on the UMA EM5000 is sufficient memory to run GMS 7.2.

MySQL Requirements

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

Java Support

Download and install the latest version of the Java 7 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

Dell SonicWALL GMS 7.2 supports the following Dell SonicWALL appliances and firmware versions:

Dell SonicWALL Platforms	Dell SonicWALL Firmware Version
Firewall / Network Security	
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 7.2: • Multi-blade 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 Enhanced 5.0 or newer
TZ Series	SonicOS Enhanced 3.2 or newer SonicOS Standard 3.1 or newer
PRO Series	SonicOS Enhanced 3.2 or newer
CSM Series	SonicOS CF 2.0 or newer
Email Security/ Anti-Spam	
Email Security Series	Email Security 7.2 or newer (management only)

Secure Remote Access	
SMB SSL-VPN Series	SonicOS SSL-VPN 2.0 or newer (management) SonicOS SSL-VPN 2.1 or newer (reporting)
E-Class SRA Series	SRA 9.0 or newer
Backup and Recovery	
CDP Series	CDP 2.3 or newer (management) CDP 5.1 or newer (reporting)

Notes:

- GMS 7.2 supports Dell SonicWALL firewall App Control policy management and App Control reporting support. Please 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 release will be supported in an upcoming release of GMS.
- Legacy SonicWALL XPRS/XPRS2, SonicWALL SOHO2, SonicWALL Tele2, and SonicWALL Pro/Pro-VX models are not supported for Dell SonicWALL GMS management. Appliances running SonicWALL legacy firmware including SonicOS Standard 1.x and SonicWALL legacy firmware 6.x.x.x are not supported for GMS management.

Non-Dell SonicWALL Appliance Support

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

Browser Support

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 18.0 and higher (recommended browser for dashboard real-time graphics display)
- Firefox 16.0 and higher
- Internet Explorer 8.0 and higher (do not use compatibility mode)

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

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

Enhancements in GMS 7.2

The following enhancements are included in the GMS 7.2 firmware release:

- **IPv6 Support** — IPv6 is supported in GMS 7.2, allowing the user to:
    - Install GMS in an IPv6 network environment. GMS can now access various Network Elements using IPv6 addresses, such as: Firewalls, SMTP servers, RADIUS/LDAP Authentication Servers, SNMP Managers, WebServices, etc.
    - Access GMS web interfaces on an IPv6 network.
    - Use these products to manage IPv6 features of Firewalls.
    - Generate IPv6 based reports.
    - Monitor Network Elements using IPv6 addresses.
- **Summarizer IPv6 and Enhanced Syslogs** — Syslog tags used by Summarizer for IPv6 and enhanced syslogs are supported.
- **Federated Management & Reporting**— An easy way to create, modify, or delete a policy directly from the Reports panel. While viewing a report, right-click on a column that supports this feature, then select "Configure Policy". The corresponding policy screen displays, allowing the user to configure the policy without having to navigate to the Policy panel.
- **Intrusion Reporting Enhancements** — Two new reports are added at root level to the Intrusion reports:
    - Reports > Intrusions > Details
    - Reports > Intrusions > Alerts
- **Log Analyzer Enhancements** — The Log Analyzer interface is customizable to allow expansion and easy distribution of columns for ease of navigation.
- **Scheduled Reports Permission Management** — In GMS 7.1, scheduled reports created by an end user can only be viewed and configured by the creator and Administrator. GMS 7.2 gives the scheduled report creator the ability to manage permissions of the scheduled reports so other users in the deployment can view and configure the report. This feature is available to users within the LocalDomain ONLY.
- **Syslogs sent by appliances that are not under Reporting or Management** — Some of the units which are no longer managed by GMS send syslogs that create NMM files which impact performance. In GMS 7.2, the user will be notified if this occurs and they can make the unit stop sending syslog messages.
- **Firewall Login Enhancements** — This feature allows the GMS Administrator or equivalent to manage Firewalls using a non-admin user with sufficient privileges to manage. Based on the user type, Local User or Remote User, the user credentials would be used by GMS to manage, monitor, and report.
- **Sticky Managed Address Mode** — This feature allows the GMS Administrator to manage a unit using a Static IP Address under any management mode. The sticky flag ensures the static address specified is not overwritten with the IP address obtained from the syslog packet's header as it was happening in previous versions. As a result, the interface used to manage the unit can be different from the one used for sending syslogs to GMS.
- **Application Level Data Archiving and Aging** — In GMS 7.1 data was not deleted from the application table e.g. logs and meta data tables, causing the number of rows to grow quickly in the tables, affecting overall performance of the application. In GMS 7.2 the console logs and application meta data tables are aged and archived to fix this issue.
- **Localization** — Support for the Korean language is included in GMS 7.2.
- **Disable archiving of syslogs to File System** — Added the option to disable storing of archived syslogs.
- **Import LDAP Users and User Groups** — LDAP user groups can be imported on Dell SonicWALL appliances via GMS.

- **Reverse DNS Support** — This feature enhances the quality of data by performing a reverse lookup on the private IPs (LAN Side) with a missing hostname sent by the firewall. The reverse lookup is performed by logging into the DNS server on the LAN side of the firewall. This functionality requires the GMS to be installed on the LAN side of the firewall, to be able to access the DNS Server.
- **SonicOS Support** — SonicOS 5.9 and SonicOS 6.x and higher firmware versions are supported to work with GMS 7.2. Future SonicOS firmware versions that are released after GMS 7.2 can still be managed and reports can still be generated. However, the new features in the firmware release will be supported in an upcoming release of GMS. The following SonicOS enhancements are added:
    - **NTP Server Support** — Added options for adding and editing NTP Servers in the System > Time screen.
    - **Rapid Spanning Tree Support** — Added a new screen under Switching called Rapid Spanning Tree which offers force version, bridge priority, hello time, and forward delay options.
    - **VLAN Trunk Switching** — Added a new screen is under Switching called VLAN Trunking. The two fields: Starting VLAN ID and Ending VLAN ID are used to display reserved VLAN information and are read-only fields.
    - **Rate Control Switching** — Added a new screen called Rate Control under the Switching screen group. The Rate Control table shows the name, ingress limit mode, ingress rate, egress rate, and flow control.
    - **Layer 2 QoS Switching** — A new screen called Layer 2 QoS was added in the Switching group. The DSCP Remap table shows 64 priority levels with default value of “normal”. The Reset control brings each priority to its default value.
    - **Port Security Switching** — A new screen called Port Security was added to the Switching group. This screen offers these filters: By Default, Trunk Ports are not displayed, LAG LACP enabled ports are also excluded, VLAN interfaces are also not displayed.
    - **User Settings Enhancements** — Added several new options in the Users > Settings page, available at unit and group level.
    - **Anti-Spam Settings** — Three new fields are added to the Anti-Spam > Settings page: Probe Timeout, Use Destination Mail Server Private Address as Junk Store Address, Junk Store IP Address.
    - **Security Services Enhancements** — Added several new options in the Geo-IP Filter, Botnet Filter, Inheritance Preview Dialog, Gateway Anti-Virus, Intrusion Prevention, and Anti-Spyware screens.
    - **3G/4G/Modem > Connection Profile Enhancements** — A new option called Force PAP Authentication is added to the 3G/4G/Modem > Connection Profiles page.
    - **Wireless Enhancements** — Several enhancements are added to the Settings, Security, and Virtual Access Point screens.
    - **Administrative Enhancements** — New options are added to the System > Administrator page.
    - **CFS Enhancements** — New Fields are added to the Content Filter > Settings and Websense pages.
    - **NTLM tab in Users > Settings** — A new NTLM tab is added in the Single Sign On Authentication Configuration window.
    - **Per-Zone Enforcement Settings** — New fields are added to the User > Settings > SSO Configuration > Enforcement tab.
    - **Web Block Page Enhancements** — A new Customize Web Block Page Settings section available in the Security Services > Botnet Filter page.

Known Issues

This section contains a list of known issues in the GMS 7.2 release.

Policies

Symptom	Condition / Workaround	Issue
An LDAP Schema name may not fully display in the **LDAP Schema** drop-down menu.	Occurs when **LDAP + Local Users** settings are configured and a schema is selected from the **LDAP Schema** drop-down menu that contains a large amount of characters.	139615
No content is displayed in the Email Security (ES) pane of the GMS user interface.	Occurs when adding an Email Security device to GMS, then navigating to the ES pane of the GMS user interface.	137816
The wrong interface is displayed at Group level for a Route Policy.	Occurs when creating a Route Policy at Unit level, then performing a Reverse Inheritance from Unit to Group level.	136743
The LDAP Schema settings do not match in the GMS and Firewall user interfaces.	Occurs when configuring the LDAP Server settings, then navigating to the **Schema** tab and clicking the **Update** button	136192
A Mirror interface configured via GMS displays in the Firewall's user interface, but not in the GMS user interface.	Occurs when configuring a Mirror interface in the GMS **Diagnostics > Packet Monitor** screen.	134936

Reports

Symptom	Condition / Workaround	Issue
The **Reports > Flow Activity > Real-Time Viewer** screen displays the wrong date/time of the Flow Server and no reports.	Occurs when using an Internet Explorer (IE) Web browser.	139699
The wrong report is highlighted in the Reports panel.	Occurs when loading a custom report. You should be directed to the **Reports > Custom Reports** screen. *Example*: Go to the **Reports > Data Usage > Initiators** screen. Click the **Load Custom Report** drop-down and select a custom report. Observe that the custom report is generated, but the **Reports** panel still has **Data Usage** highlighted, instead of **Custom Reports**.	136747

Universal Scheduled Reports

Symptom	Condition / Workaround	Issue
A Local Domain user is able to provide user permission to a Custom Domain user that does not have units/unit permission.	Occurs when performing the following: 1. Login to GMS as the **Admin** from **LocalDomain**. 2. Add a new custom domain, then add a user that does not have units added/unit permission. 3. Go to **Universal Scheduled Reports** > **Add a Scheduled Report** or **Manage Scheduled Reports**. 4. In **Permission Management** page, observe that the user from the Custom Domain is displayed in user list that does not have units/unit permission.	134320

Resolved Issues

This section contains a list of issues resolved in GMS 7.2 release.

Appliance

Symptom	Condition / Workaround	Issue
Previously uploaded firmware cannot be deleted.	Occurs when navigating to the **System > File Manager** screen in the UMA management interface, and then attempting to delete firmware that was previously uploaded.	124891

Archived Syslogs / Backup Files

Symptom	Condition / Workaround	Issue
Decompression utilities do not work for un-zipping compressed archived syslogs files or backup files.	Occurs when un-zipping a compressed ".zip" file in a GMS Virtual Appliance or Universal Management Appliance.	132194

Event Manager

Symptom	Condition / Workaround	Issue
Cannot edit alerts that were created by another user.	Occurs when a user tries to edit an alert that was created by another user in the same user group.	129942

Firewall Configuration

Symptom	Condition / Workaround	Issue
Firewall certificates cannot be imported and the message "There are no changes made" displays in the status bar.	Occurs when importing a Firewall certificate via GMS.	137357

Inheritance

Symptom	Condition / Workaround	Issue
Inheriting GMS settings does not work on the first attempt.	Occurs when inheriting GMS settings from Group to Unit level using forward inheritance. The first attempt does not work, but the second is successful.	121819
Forward inheritance creates a bad object in the TZ appliance configuration.	Occurs when creating Access Rules and Objects at Group level and applying a forward inheritance.	124157

Logs

Symptom	Condition / Workaround	Issue
Changes to the Firewall Access Rules are not reflected in the GMS Real-Time Syslog.	Occurs when adding, editing, or deleting Access Rules via GMS on a Firewall running SonicOS 5.9.0.2 or 6.1.1.4. The changes display in the Firewall user interface, but not in the GMS user interface.	138283

Policies

Symptom	Condition / Workaround	Issue
GMS creates a new rule instead of modify the existing.	Occurs when attempting to change a rule from “Allow” to “Deny”.	132617
New Application Groups are replacing the existing ones in the Match objects list.	Occurs when “Add all Application Groups” is used and there are already groups present in the application groups list.	130707

Summarizer

Symptom	Condition / Workaround	Issue
The report summarization process becomes unresponsive and the unit must be rebooted.	Occurs when sending syslogs with extended characters.	135426

Upgrading to GMS 7.2

This section provides procedures for upgrading an existing Dell SonicWALL GMS 7.1 or newer installation to GMS 7.2. GMS can be configured for a single server or in a distributed environment on multiple servers. GMS 7.2 can be installed as a fresh install or as an upgrade from GMS 7.1. If you wish to perform a fresh install of GMS 7.2, please refer to the *GMS Getting Started Guide* that relates to your GMS deployment.

Upgrading Considerations

- The 40 GB 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 250 GB and 950 GB virtual appliances are supported in production environments. It is not possible to upgrade a 40 GB virtual appliance to a 250 GB or 950 GB virtual appliance. You need to download the 250 GB or 950 GB 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 40 GB limit, in which case Dell SonicWALL will be unable to support the 40 GB 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 7.2 logs into the appliances using HTTPS only.
- The scheduled reports created in GMS 7.1 will continue to work properly after upgrading to 7.2. However, the Legacy reports created in GMS 6.0 or earlier versions will not be migrated. For more information on viewing legacy reports, refer to the *GMS Administrator's 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.

Upgrading the GMS Software for Windows

You can use the Dell SonicWALL UMS installer to upgrade from the GMS 7.1 to the 7.2 release. For a fresh install of the GMS 7.2 Software, please refer to the *GMS Software Getting Started Guide*.

When upgrading a distributed deployment, upgrade and register the primary system first. This is usually the GMS Console system from the original deployment. All subsequent instances of GMS will use the primary system's 12 character serial number when registering as components of the deployment. Each server in the distributed deployment must be upgraded and registered individually.

If the GMS Console (Web server) is set up for HTTPS management, the upgrade to GMS will preserve the HTTPS settings for the GMS Web server.

The upgrade installer checks with the Dell SonicWALL backend to see if the GMS deployment has a valid support license. If it does not, then the upgrade discontinues. If the GMS installer detects that the Dell SonicWALL backend site is not accessible, it prompts the user to enter an Upgrade Key. If the key is valid, it allows the upgrade to continue. If the key is invalid, the installation fails.

In a distributed environment, stop all services on all GMS servers except the main database service, before performing an upgrade. You must upgrade all GMS servers in your deployment to the same version of GMS 7.2. You cannot have some servers running version 7.1 and others running 7.2.

It is highly recommended that you backup your database, GMS installation folders, and the **GMS installation folder>\conf\sgmsConfig.xml** file on all GMS servers prior to performing the GMS upgrade.

To upgrade the GMS software for Windows Server, perform the following steps:

1. Log on to your Dell SonicWALL GMS management computer as administrator (Windows). Launch the Dell SonicWALL Universal Management Suite 7.2 installer, by double-clicking the file **sw_gmsvp_win_eng_7.2.xxxx.xxxx.exe** (where "xxxx" are the exact version numbers). It may take several seconds for the InstallAnywhere self-extractor to initialize.
2. In the Introduction screen, click **Next.**
3. In the License Agreement screen, select the radio button next to **I accept the terms of the License Agreement**. Click **Next.** Wait while the installer prepares to install UMS on your system.

   Note: You must have a valid support license to upgrade your GMS.
4. Click **Install** to upgrade your installation. The Installer detects the previous installation of GMS. Click **Install** to proceed with the upgrade.
5. 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.
6. 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.
7. The final installer screen contains the path of the installation folder, and warns you that the Universal Management Suite Web page will be launched next. Click **Done**.

Upgrading the GMS Virtual Appliance

The GMS Virtual Appliance can be upgraded from 7.1 to 7.2, but cannot be directly upgraded from GMS versions earlier than 7.1. To upgrade the GMS Virtual Appliance from a version earlier than 7.1, you need to upgrade to major versions of GMS until you reach 7.1, then you can upgrade to GMS 7.2. For Dell SonicWALL GMS Virtual Appliance deployments, upgrading from the GMS 7.1 release to the GMS 7.2 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 7.2. You cannot have some servers running version 7.1 and others running 7.2.

For a fresh install of the GMS 7.2 64-bit Virtual Appliance, please refer to the *GMS Virtual Appliance Getting Started Guide*.

To upgrade, perform the following:

1. Download the respective file from the MySonicWALL.com Software Download Center to your workstation:

   sw_gmsvp_vm_eng_7.2.xxxx.yyyy.gmsvp-updater.64bit.sh
2. Log into the /appliance (System) interface of the GMS server.
3. Navigate to the **System > Settings** page.
4. Click on the **Browse** button, navigate to the location where you saved the above file, and then select it.
5. Click the **Apply** button to begin the firmware upgrade installation.

Upgrading the GMS UMA EM5000 Appliance

For the Dell SonicWALL UMA EM5000 appliance, upgrading from the GMS 7.1 release to the GMS 7.2 release can be performed on the **System > Settings** page. For a fresh install of GMS 7.2, please refer to the *GMS UMA EM5000 Getting Started Guide*.

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 Dell SonicWALL GMS 7.2. You cannot have some servers running version 7.1 and others running 7.2.

To upgrade the UMA EM5000 appliance, perform the following:

1. Download the respective file from the MySonicWALL.com Software Download Center to your workstation:
   sw_uma_em5000_eng_7.2.xxxx.xxxx.gmsvp-updater.sh
2. Log into the /appliance (System) interface of the UMA EM5000 appliance.
3. Navigate to the **System > Settings** page.
4. Click on the **Browse** button, navigate to the location where you saved the above file, and then select it.
5. Click the **Apply** button to begin the firmware upgrade installation.

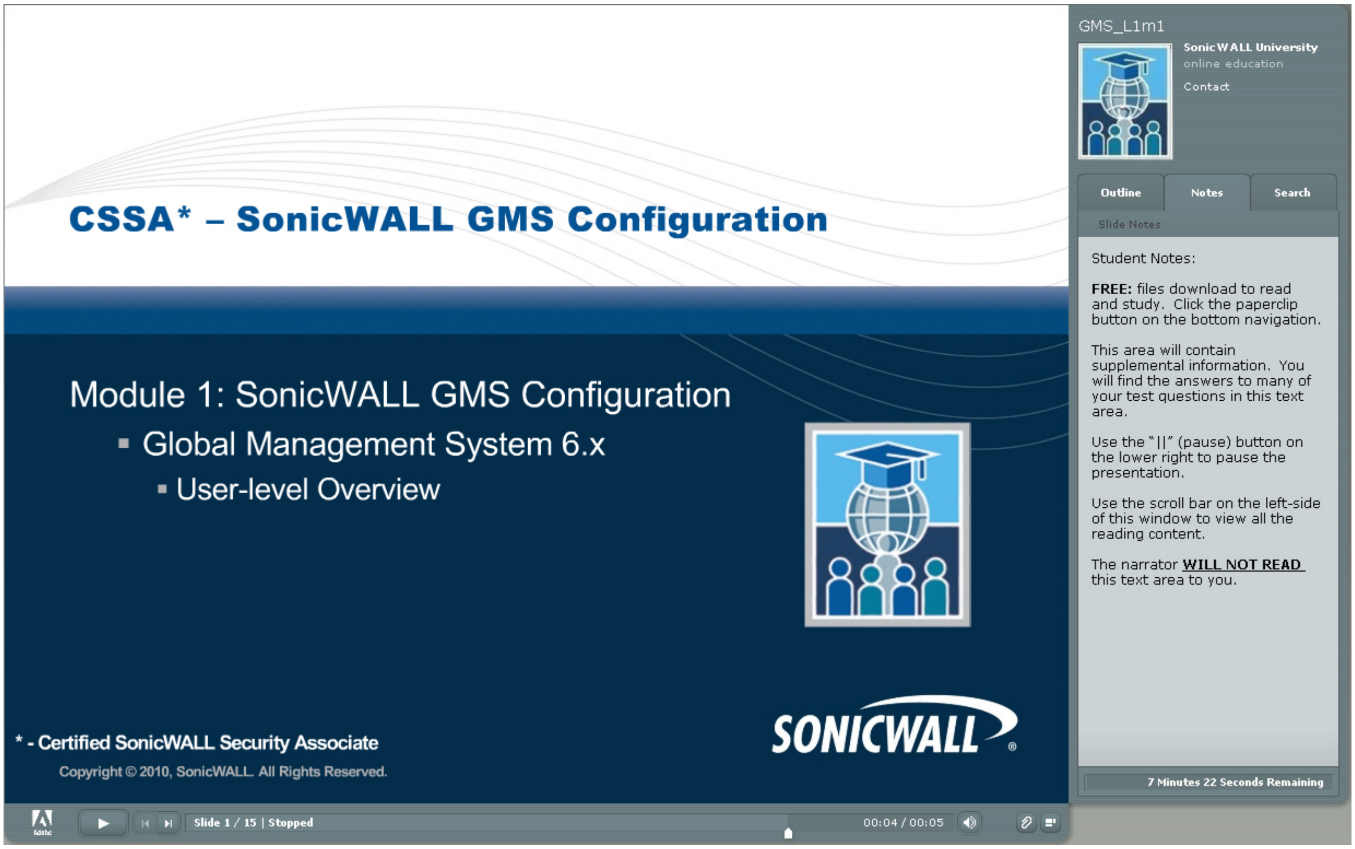
Online Training Materials

Dell SonicWALL Technical Training Services offers GMS software and UMA appliance eLearning 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:

http://www.sonicwall.com/us/support/eLearning.html#tab=technical

Click on the **Global Management System Certification Training** link.



CSSA* – SonicWALL GMS Configuration

Module 1: SonicWALL GMS Configuration
- Global Management System 6.x
  - User-level Overview

* - Certified SonicWALL Security Associate

Copyright © 2010, SonicWALL. All Rights Reserved.

Student Notes:

FREE: files download to read and study. Click the paperclip button on the bottom navigation.

This area will contain supplemental information. You will find the answers to many of your test questions in this text area.

Use the "||" (pause) button on the lower right to pause the presentation.

Use the scroll bar on the left-side of this window to view all the reading content.

The narrator **WILL NOT READ** this text area to you.

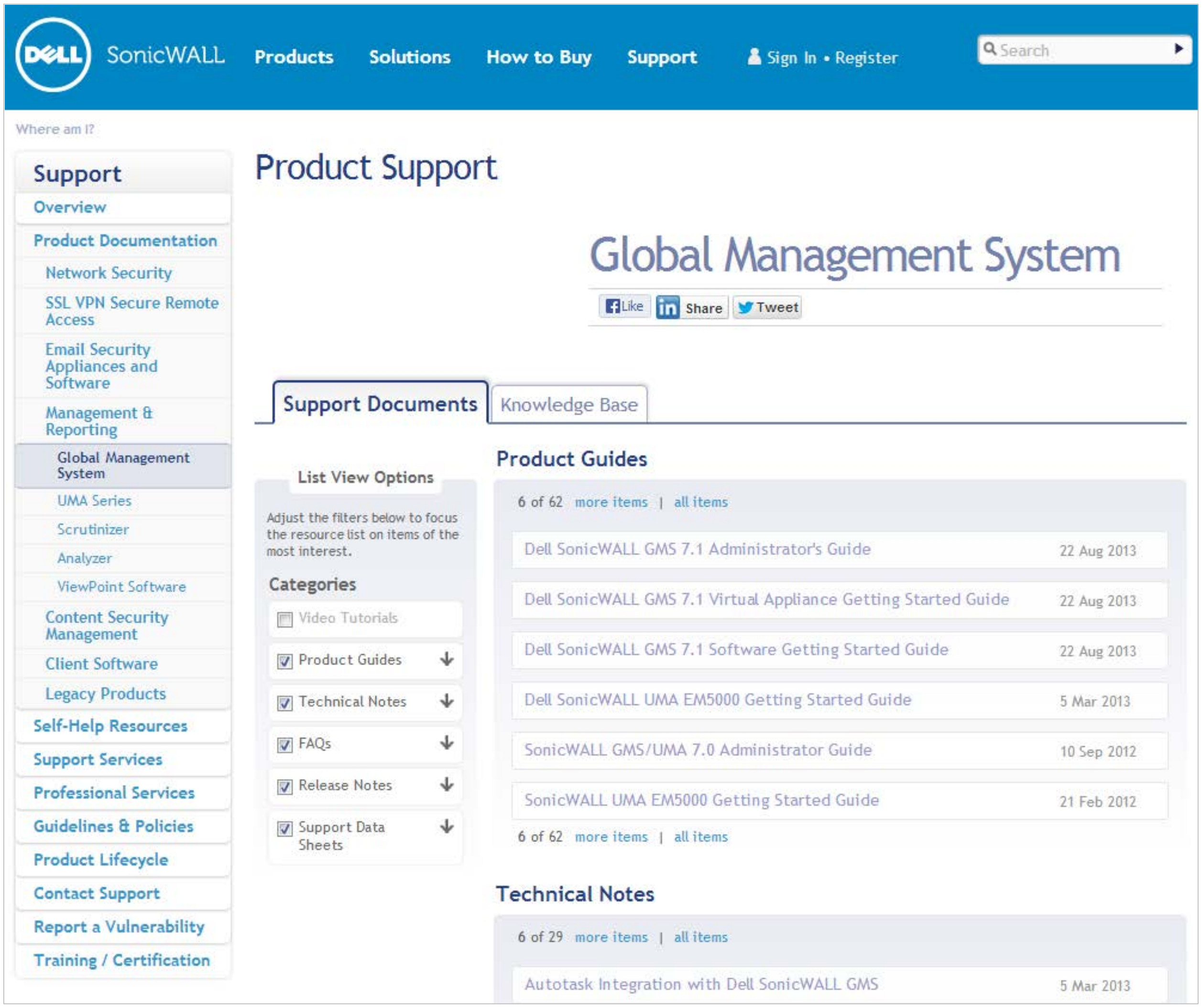
Related Technical Documentation

Dell SonicWALL reference documentation is available at the Dell SonicWALL Technical Documentation Online Library:

http://www.sonicwall.com/us/Support.html

Dell SonicWALL GMS video training is available from the GMS Development Team:

http://software.sonicwall.com/gmsvp/Dev-Training/



Product Support

Global Management System

List View Options

Adjust the filters below to focus the resource list on items of the most interest.

Categories

- ☐ Video Tutorials
- ☑ Product Guides
- ☑ Technical Notes
- ☑ FAQs
- ☑ Release Notes
- ☑ Support Data Sheets

Product Guides

6 of 62 more items | all items

Dell SonicWALL GMS 7.1 Administrator's Guide	22 Aug 2013
Dell SonicWALL GMS 7.1 Virtual Appliance Getting Started Guide	22 Aug 2013
Dell SonicWALL GMS 7.1 Software Getting Started Guide	22 Aug 2013
Dell SonicWALL UMA EM5000 Getting Started Guide	5 Mar 2013
SonicWALL GMS/UMA 7.0 Administrator Guide	10 Sep 2012
SonicWALL UMA EM5000 Getting Started Guide	21 Feb 2012

6 of 62 more items | all items

Technical Notes

6 of 29 more items | all items

Autotask Integration with Dell SonicWALL GMS	5 Mar 2013

Last updated: 12/12/2013