Dell™ SonicWALL™ Global Management System (GMS) 8.2

Release notes

December 2016

These release notes provide information about the Dell™ SonicWALL™ Global Management System (GMS) 8.2 release.

About Dell SonicWALL GMS 8.2

The GMS 8.2 release provides new features and functionality, and fixes a number of known issues from previous releases. See New features, Resolved issues, and Known issues.

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.

Pre-8.2 Upgrade Preparation

> **NOTE:** The process of upgrading from GMS 8.1 to GMS 8.2 requires following a set of steps as there are dependencies on the files installed. You CANNOT upgrade directly from GMS 8.1 to GMS 8.2. The correct upgrade path is **GMS 8.1** > **8.1 Service Pack 1** > **Hotfix 173751** > **Hotfix 168044** > **8.2**.
>
> - You should plan to perform a backup to GMS between each Hotfix update.
> - GMS requires a mandatory restart between each update.
> - Apply each Hotfix in the upgrade path on all systems in the distributed deployment before upgrading to 8.2.
> - See Upgrading to GMS 8.2 for complete upgrade details.
>
> The GMS 8.0/8.1 database is reporting problems when managing SonicWALL firewalls running SonicOS 6.2.6. The problems appear as an inability to access database reports because of database corruption caused by SYSLOG anomalies in SonicOS 6.2.6. These problems are resolved in GMS 8.2 and syslog reports are generated as normal.
>
> See the associated Knowledge Base articles #213012 and #213411 at https://support.software.dell.com/kb-product-select for more information.

The reporting database engine changed from a MySQL engine to a Postgres engine called Rv2 (Reporting Database version 2) for data storage. This change has minimum impact on the Reporting functionality with the exception of some additional user input required prior to the upgrade. By default, all reporting data automatically migrates from the 8.1 data format (MySQL storage) to the 8.2 data format (Postgres storage). Data migration is a time-consuming process depending on the amount of data stored within the system. The following Knowledge Base article and the GMS/Analyzer 8.2 Installation FAQ document posted in MySonicWALL Downloads at https://support.sonicwall.com/sonicwall-gms/kb/187302 provide the latest migration information.

Basically, there are three options you can choose from for data migration:

1. **Migrate the Data**. No action is required.
2. **Migrate the Data** but choose the number of months to migrate. This option requires the customer to open the KB and follow its instructions to set the “Do you want to migrate the data for the following months:” drop-down to “Yes,” and then set the number of months to migrate from the second drop-down.
3. **Do Not Migrate the Data**. This option requires the customer to open the KB and follow its instructions to set the “Do you want to migrate the data for the following months:” drop-down to “No.”

New features

This section describes the new features included in the GMS 8.2 release.

Topics:

- Enhanced Flow Reporting Agent
- MySQL 5.7 upgrade
- SonicOS support
- Open Java Development Kit and Tomcat 8 upgrade
- Apache Flex BlazeDS XXE
- Geo map support in GMS with a proxy
- Data deletion
- Optimized code for performance

- Email Security and GMS integration
- Applications report

Enhanced Flow Reporting Agent

The Flow Reporting Agent introduced in GMS 7.1 has been enhanced with a new Real-Time Viewer with drag and drop customization, a new Real-Time Report screen with one-click filtering, a new Top Flows Dashboard with one-click View By buttons, a new Flow Reports screen with five additional flow attribute tabs, a new Flow Analytics screen with powerful correlation and pivoting features, and an all-new Session Viewer for deep drill-downs of individual sessions and packets.

MySQL 5.7 upgrade

The 5.0 MySQL server has been replaced with a newer version of the MySQL Community server 5.7.15. During a GMS fresh installation, the SGMS database is created with the new MySQL server. For GMS upgrade installations, existing data is migrated to the newer MySQL server using the MySQL upgrade process.

SonicOS support

SonicOS Enhanced versions 6.2.6 and above are supported, including Content Filter Objects like the CFS 4.0 policy screen changes, and SonicPoint enhancements like Capture ATP policy configuration. SonicOS 6.2.6 also supports a new checkbox in the VPN Policy add dialog, Advanced tab: Allow Advanced Routing. It is available on the Advanced tab only when you select Tunnel Interface as the Policy Type on the General tab.

SonicOS 6.2.6.0 includes two important new features that are supported by GMS 8.2:

- Capture Advanced Threat Protection (Capture ATP) See About Capture ATP
- Content Filtering Service 4.0 (CFS 4.0) See About CFS 4.0

About Capture ATP

Capture Advanced Threat Protection (ATP) is an add-on security service to the firewall, similar to Gateway Anti-Virus (GAV). Capture ATP helps a firewall identify whether a file contains a zero-day virus by transmitting a suspicious file to the Cloud where the Capture ATP service analyzes the file to determine if it contains a virus. Capture ATP then sends the results to the firewall. This is done in real time while the file is being processed by the firewall.

The **Capture ATP > Status** page displays a graph chart that shows the percentages of benign and malicious files discovered, as well as the total number of files analyzed. It also displays a log table that shows the results of individual files submitted for analysis.

Capture ATP must be configured on each firewall individually. After the Capture ATP service license is activated, you can enable Capture ATP on the **Capture ATP > Settings** page.

Capture ATP can also analyze files that you upload for analysis from the **Capture ATP > Status** page. After the files are analyzed they are listed in the table on the **Status** page. You can click on any file in the log table on the **Status** page and see the results from the detailed analysis of that file.

Note that Capture ATP is only supported on the following appliances using SonicOS 6.2.6.0 or newer. The smaller TZ appliances and the SOHO wireless appliance do not support Capture ATP.

- SuperMassive 9600
- SuperMassive 9400
- SuperMassive 9200
- NSA 6600
- NSA 5600
- NSA 4600
- NSA 3600
- NSA 2600
- TZ600
- TZ500 and TZ500 Wireless

About CFS 4.0

Content Filtering Service (CFS) 4.0 has been redesigned to improve performance and ease of use. The workflow was redesigned and more accurate filtering options have been provided. Refer to *SonicOS 6.2.6 Content Filtering Service (CFS) 4.0 Feature Guide* for more details. For information about upgrading from an older version of CFS, see the *SonicOS 6.2.6 CFS 4.0 Upgrade Guide*.

Topics:

- CFS workflow
- CFS settings
- New CFS policy design
- CFS custom categories
- New objects in CFS 4.0
- CFS log entries
- Websense support in CFS 4.0
- Deprecated CFS 3.0 features
- Comparison of CFS 3.0 to CFS 4.0

CFS workflow

When processing packets, CFS follows this workflow:

1. A packet arrives and is examined by CFS.
2. CFS checks it against the configured exclusion addresses, and allows it through if a match if found.
3. CFS checks its policies and finds the first policy which matches the following conditions in the packet:
    - Source Zone
    - Destination Zone
    - Address Object
    - Users/Group
    - Schedule
    - Enabled state
4. CFS uses the CFS Profile defined in the matching policy to do the filtering, and returns the corresponding operation for this packet.
5. CFS performs the action defined in the CFS Action Object of the matching policy.
6. If no CFS Policy is matched, the packet is passed through without any action by CFS.

CFS settings

The following global settings are used in CFS 4.0:

- Global settings
  - **Max URI Caches (entries)** — Defines the maximum number of cached URI entries. Cached URI entries save the URI rating results, so that SonicOS does not need to ask the backend server for the rating of a known URI. In CFS 3.0, the cache size had a maximum; in CFS 4.0 the maximum is changed to the entry count.
  - **Enable Content Filtering Service** — This option can be cleared to bypass CFS for all packets. By default, it is selected.
  - **Enable HTTPS content filtering** — When enabled, CFS first attempts to get the ServerName from the client "hello". If that fails, CFS attempts to get the CommonName from the SSL certificate and then get the rating. If both attempts fail to get the ServerName/CommonName, CFS uses the IP address for the rating.
  - **Blocked if CFS Server is Unavailable** — If the CFS server cannot provide the rating request within the specified duration (5 seconds by default), this option defines whether to allow or deny the request.
- CFS Exclusions
  - **Exclude Administrator** — When enabled, content filtering is bypassed for all requests from an account with administrator privileges.
  - **Excluded address** — Content filtering is bypassed for all requests from address objects selected in the **Excluded address** list.
- Custom Category
  - **Enable CFS Custom Category** — Allows the administrator to customize the ratings for specific URIs. When CFS checks the ratings for a URI, it first checks the user ratings and then checks the CFS backend server for the ratings.
- Advanced Settings
  - **Enable Smart Filtering for Embedded URL** — When enabled, detects the embedded URL inside Google Translate (Https://translate.google.com) and filters the embedded URL too. Requires that client DPI-SSL be enabled also.

New CFS policy design

A CFS policy defines the filtering conditions that a packet is compared to, and CFS 4.0 provides a new policy design, different from the way policies were implemented in CFS 3.0. A default policy is provided, but you can define your own. When writing your own policies, following matching conditions can be defined:

- Name
- Source Zone
- Destination Zone
- Source Address
- Users/Group
- Schedule
- Profile
- Action

If a packet matches the conditions defined for Source Zone, Destination Zone, Address Object, Users/Groups, Schedule, and Enabled state, it is filtered according to the corresponding CFS Profile and then the CFS Action is applied. If authentication data is not available during matching for Users/Groups, no match is made for this condition. This strategy prevents performance issues, especially when Single Sign-On is in use.

Each CFS policy has a priority level and policies with higher priorities are checked first.

CFS custom categories

In CFS 4.0, CFS custom categories are handled consistently with the way ratings are handled in the CFS backend server. When adding or editing a custom category, you can select up to four categories for the URI.

Besides adding custom category entries one by one, export and import functions are also supported. One way to use this functionality is by exporting the custom category first, editing it, and then importing from that exported file.

Only the first 10,000 custom category entries in the file are imported. Invalid entries are skipped and do not count toward the maximum of 10,000 custom category entries that are supported.

New objects in CFS 4.0

Three new kinds of objects are supported in CFS 4.0:

- **URI List Objects** — Defines the URI list which can be marked as allowed or forbidden.
- **CFS Action Objects** — Defines what happens after a packet is filtered by CFS.
- **CFS Profile Objects** — Defines what kind of operation is triggered for each HTTP/HTTPS connection.

These objects are configured on the **Firewall > Content Filter Objects** page in the GMS management interface.

URI list objects

In CFS 4.0, a *URI List Object* is used for URI/domain matching. Each URI List Object contains a custom list of URIs. You can add/edit/delete a CFS URI list object on the **Firewall > Content Filter Objects** page in GMS.

Use the following guidelines when configuring URI List Objects:

- A maximum of 128 URI list objects are allowed.
- In each object, up to 5,000 URIs are supported.
- A URI is a string containing host and path. Port and other content are currently not supported.
- An IPv4 or IPv6 address string is supported as the host portion of a URI.
- The maximum length of each URI is 255 characters.
- The maximum combined length of all URIs in one URI list object is 131,072 (1024*128) including one character for each new line (carriage return) between the URIs.
- Each URI can contain up to 16 tokens. A token in URI is a string composed of the characters:

```
0-9
a-z
A-Z
$ - _ + ! ' ( ) ,
```

- The maximum length of each token is 64 characters including one character for each separator (. or /) surrounding the token.
- An asterisk (*) can be used as a wildcard representing a sequence of one or more valid tokens.

When building a policy URI List Objects can be used as either the forbidden URI list or the allowed URI list. URI List Objects can also be used by the Web Excluded Domains of Websense.

Action objects

The CFS Action Object defines what happens after a packet is filtered by CFS and specified by a CFS Policy. You can add/edit/delete a CFS Action Object on the **Firewall > Content Filter Objects** page in GMS. Within the Action Object you can define whether to block a web site, require a passphrase (password) for access, require a confirmation before proceeding to the web site, or use Bandwidth Management.

Passphrase and Confirm features only work for HTTP requests. HTTPS requests cannot be redirected to the Passphrase or Confirm page, respectively.

Profile objects

The CFS Profile Object defines the action that is triggered for each HTTP/HTTPS connection. You can add/edit/delete a CFS Profile Object on the **Firewall > Content Filter Objects** page in GMS. When setting up a new Profile Object under the new design, a domain may now be resolved to one of four ratings. From highest to lowest, the ratings are:

- Block
- Passphrase
- Confirm
- BWM (Bandwidth Management)

If the URI is not categorized into any of these ratings, then the operation is allowed.

CFS log entries

In CFS 4.0, there are only three types of log entries:

- logstrSyslogWebSiteAccessed
- logstrWebSiteBlocked
- logstrCFSAlert

These log entries start with **CFS Alert:** and are followed by a descriptive message.

Websense support in CFS 4.0

The Websense configuration settings are shown in the **Security Services > Content Filter** page when the **Content Filter Type** selection is set to ***Websense Enterprise***. Websense only works for IPv4 requests. It does not work with IPv6.

Websense can be used even when the firewall is not licensed for CFS 4.0 (Content Filtering Premium).

Deprecated CFS 3.0 features

CFS 4.0 includes the following changes to CFS 3.0 features:

- Merge "CFS via App Rules" and "CFS via Zones" into one.
- Remove the Global/Local custom lists, replaced by URI List objects.
- Users cannot use CFS without a license, but can still use Websense.
- Remove CFS configuration from Users/Groups CFS tab.
- Remove CFS configuration from Zone page if using SonicWALL CFS. The CFS configuration in Zone is available only if CFS type is Websense.
- Remove Restrict Web Features for Java/ActiveX. They can be replaced with entries in the Forbidden URI list using **.java* and **.ocx*.
- Remove Restrict Web Features for HTTP Proxy Server.
- In CFS 4.0, to block access to HTTP Proxy Server, go to the **Firewall > App Control Advanced** page, enable **App Control**, and then edit the 3648 signature ID to block HTTP proxy access.

Comparison of CFS 3.0 to CFS 4.0

The following table compares the user experience for various aspects of the old and new CFS.

CFS 3.0	CFS 4.0
Configure CFS on CFS page, Zone page, User page and App Rules page.	Centralized CFS configuration in one place.
Two modes (via Zones and via App Rules).	Merged functions into one mode.
Admin cannot predict the filtering results accurately after configuration.	Admin can exactly predict the filtering results.
Need to define duplicated filtering options.	Define CFS Category object, URI List object, Profile object and Action object, which can be reused in multiple policies.
Does not support wildcard matching.	Supports wildcard (*) matching for URI List.
Consent feature is global.	Consent feature is per policy.
BWM is only supported in App Rules mode.	BWM is fully supported.
Does not support Override – Confirm.	Supports Override – Confirm.
Only supports GET, POST and HEAD commands for HTTP.	Supports GET, HEAD, POST, PUT, CONNECT, OPTIONS, DELETE, REPORT, COPY and MOVE commands.
Cannot enable/disable CFS globally.	Can enable/disable CFS globally.
Custom category is based on category.	Custom category is based on domain, which is more intuitive.
Websense configuration is mixed with CFS configuration.	Separate Websense configuration from CFS configuration helps prevent errors.

Open Java Development Kit and Tomcat 8 upgrade

Current Java Runtime Environment (JRE) and Tomcat versions have been phased out. Still, there are many library-related security updates that are only supported in the newer versions. The effort is bundled together to upgrade both JDK/JRE and Tomcat in the GMSVP 8.2 release.

Apache Flex BlazeDS XXE

The BlazeDS data services library has been upgraded from 4.0 versions to 4.7.2.

One of the Blaze DS library jar files was vulnerable (flex-messaging-core.jar) to the XXE injection attack. This has been addressed in the latest version 4.7.2.

Geo map support in GMS with a proxy

Geo map on the dashboard is not displayed when GMS is configured to go through proxy. The traffic to get the map was not going through the proxy, and hence failed.

Data deletion

Update to the settings of Data Deletion.

Optimized code for performance

There were many feature enhancements to the Summarizer module of the GMS, and many old codes that were no longer in use that needed cleanup. Included are the details of the changes made during the cleanup of the Summarizer code.

Email Security and GMS integration

Email Security version 7.X.X has disabled iFrame support. As a result, GMS is unable to show the Email Security user interface for Recording Policy changes.

Applications report

Categories Report shows a different category of applications, events, and a transferred bytes column.

Resolved issues

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

Vulnerability

Issue	Issue ID
A vulnerability was discovered that allows a remote, unauthenticated attacker to gain Admin access to the Universal Management Host (UMH) or the Universal Management Appliance (UMA) interface of a Dell SonicWALL GMS/Analyzer system. The product allows the hacker to reset the password of the user “Admin” to “'password.” To prevent this, the user must provide a valid password reset key (pwdResetKey). Researcher acknowledgement: Tenable Network Security.	178678

General

Resolved issue	Issue ID
GMS systems including Summarizer and Reports DB Services stall intermittently causing performance issues. Occurs when agents or virtual machines need to be restarted.	171927

Appliance

Resolved issue	Issue ID
Reports fail to generate when processing syslogs with SonicOS 6.2.6. Occurs when SonicOS 6.2.6 sends syslogs with incorrect and very large values in sent and received tags to GMS. As a result, the report generation fails with an exception.	178165

CLI

Resolved issue	Issue ID
Unable to modify VPN policies through the CLI. Occurs when using a Domain Name as an IKE Identifier.	170354

Firewall configuration

Resolved issue	Issue ID
Network > Interface does not always appear for some units. Occurs when synchronizing at the Group level.	177161

Firmware upgrade

Resolved issue	Issue ID
Firmware upgrade tasks fail at the Group level. Occurs when using local upgrade files on GMS.	169664

Inheritance

Resolved issue	Issue ID
The reverse inheritance filter shows a blank screen. Occurs when inheriting any object that uses the (') character in its name.	174395

Logs

Resolved issue	Issue ID
The Web Activity and Web Filter Reporting features in CFS 4.0 are not functioning correctly with GMS. Occurs when normal (allowed) web traffic syslog filters are tagged with c=4 (instead of c=1024) which is used for blocked traffic. As a result, GMS is showing the traffic as blocked.	175417

Monitor panel

Resolved issue	Issue ID
Email destinations are removed from Live Monitor alerts. Occurs when viewing or modifying only the **Rule Manager > Rule Settings** page of Live Monitor alerts.	172637

Policies panel

Resolved issue	Issue ID
Certificates remain listed at the Group level are not deleted from the Global/Group Level although the tasks are executed and deleted from the child nodes. Occurs when deploying certificates at the Group level.	179952
The **DPI-SSL > Client SSL** screen does not display a full list of available web addresses in the DPI-SSL Client web address field. Occurs when the SGMS form field does not reflect the total number of sites listed on the firewall.	169724
Route policies configured in SonicOS to use the `Drop_TunnelIf` prefs file are using the `pbrObjIfaceName` prefs file value instead, which is not expected by GMS. Occurs when route policies are configured in SonicOS using the `Drop_TunnelIf` prefs file. The value is presenting in GMS as the `pbrObjIfaceName_7=Drop_TunnelIf` prefs file instead.	165741

Resolved issue	Issue ID
The GMS Policy panel does not support pushing Dynamic Ranges at the Group level but does at the Unit level. Occurs when attempting to push Dynamic Ranges at the group level.	145310

Unit acquisition

Resolved issue	Issue ID
The **Add Unit > Assign Privileges** feature is not functioning correctly for users logged in with admin privileges. Occurs when logged in as any other user with admin privileges except users named "Admin."	175412
5.8 firewall units configured with the initial task of minimal syslogs categories enabled stop reporting and then go down. Occurs after successfully acquiring the Sonic OS 5.8 firewall, logging in, checking the syslog categories, and doing a packet capture looking for the heartbeat.	175149

User interface

Resolved issue	Issue ID
Using one letter as the domain name (such as `mini8.i.is` or `abc.i.is`) is not allowed. Occurs because single letter domain names were blocked by validation at various layers such as javascript validation, server side validation, and service layer validation.	173584

Known issues

The following is a list of issues known to exist at the time of the GMS 8.2 release.

AppFlow Server

Known issue	Issue ID
The IP addresses and locations in the Flow Activity Reports should be hyperlinks and proper descriptions should be available. Occurs after generating Flow Reports for the firewall.	177945
The Disk Usage section in **System > Usage** shows the Total Size, Free Size, and Used Size appears to be 0. Occurs when using an appliance with Flow Server installed.	177290

Appliance

Known issue	Issue ID
The "File Not Found" `backupFileList.txt` exception appears, yet the backup continues. Occurs when running a backup of GMS.	178972

Installation/Upgrade

Known issue	Issue ID
The GMS/Analyzer upgrade fails with a "MySQL Community Server upgrade is pending" error appearing on the appliance page. Occurs when the application database SGMSDB upgrade is in progress.	178765
Tomcat fails to start after a new installation. Occurs after the virtual machine is powered ON for the first time.	177690

Policies Panel

Known issue	Issue ID
The firewall goes offline and loses LAN/WAN access. A hard restart in Safe Mode is required to recover the firewall. Occurs when modifying a firewall Address Object through the Policy Panel.	179952
The Access Rules forward inheritance filter causes GMS to fail. Occurs when creating new access rules within a group and then performing forward inheritance.	179100
The “Enable Gateway AV Exclusion List” option in GMS’s **Security Services > GAV/Anti Spyware** adds up only address ranges, other configurations are not updated. Occurs when configuring an exclusion list with the “Use Address Object” radio button selected.	178248
The reverse inheritance filter for dynamic ranges is not functioning correctly at the unit level. Occurs when a reverse inheritance filter for dynamic ranges is applied to the parent node and all unit nodes below it.	177727
The filter for reverse inheritance for static entries does not function correctly. Occurs when a reverse inheritance filter for static entries is applied to the parent node and all unit nodes below it.	177707
The filter for forward inheritance for dynamic ranges does not function correctly. Occurs when a forward inheritance filter for dynamic ranges is applied to the parent node and all unit nodes below it.	177177
An error message appears on the **Console > View > Logs** page. Occurs when clicking **Update** after selecting either a static or a dynamic entry on the **Policies > DHCP** page.	177108
In **WAN Acceleration > Web Cache**, the **Enable Web Cache** feature fails to create a task. An error message appears instead that reads, "Task creation failed due to the following reason: No configuration in the change is applicable to the node." Occurs when checking the **Enable Web Cache** check box and clicking **Update**.	176989
The filter for forward inheritance for static entries does not function correctly. Occurs when a forward inheritance filter for static entries is applied to the parent node and all unit nodes below it.	176691
Multiple extra params incorrectly show as being modified in the change order request screen. Occurs when updating the Settings page at the group level.	176574

Reporting

Known issue	Issue ID
The drill-down for the Target Host column under Top Targets in **Attacks > Targets** has value of N/A which shows "No Matching records found" in error. Occurs when using the unsupported N/A entry for filtering.	177618

Known issue	Issue ID
The CIDR notation filter does not function as expected for **Capture > ATP > Blocked Reports**. Occurs when filtering based on CIDR notations in reports.	177614
Using the Capture ATP > Blocked Reports to filter for the target IP “Not like” shows a false positive message while the report is being fetched. Occurs when filtering for the IP address of the target country.	177603
Filtering for target countries using the 'like' option does not function correctly for **Capture > Blocked** reports. Occurs when the target country is a private IP.	177601
The **Capture ATP > Status** page shows some filenames as blank. Occurs when using GMS where Capture ATP is licensed with a newly added firewall.	177322

Tree Control

Known issue	Issue ID
In GMS, firewalls do not always appear to be configured correctly for High Availability as the High Availability icon is sometimes missing in tree control. Occurs after adding High Availability units to GMS.	177831
In **Console > Management > Custom Group,** creating a view with a newly added custom group does not function correctly. Occurs when adding a new Group in Category (Custom Group).	177830

Unit Acquisition

Known issue	Issue ID
The GMS Flow Server agent configuration has changed. Users must now click **Apply** after making any changes or those changes do not take effect. Occurs when the `gmsServerCfgSeq` tag is not present in the prefs file which ultimately configures the firewall to internally update to the new flow server IP. SonicOS 6.2.6 is required for the fix to function correctly.	175592

Universal Scheduler

Known issue	Issue ID
The USR and Email Archive Now PDF custom reports do not show the Firewall Action column. Occurs when the **Report > Analyzer > Log Analyzer | Save a log analyzer report** is used to create the custom reports.	177515

Platform compatibility

The Dell SonicWALL GMS 8.2 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: **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 8.2, 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
- 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

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 *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:

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 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 *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 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.software.dell.com/sonicwall-gms/kb/sw14003

Mobile device browsers are not recommended for Dell 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

Dell SonicWALL appliances supported for GMS management

> **NOTE:** GMS 8.2 does not support legacy SonicWALL appliances, including:
>
> - Firewall appliances running firmware earlier than SonicOS 5.0
> - CSM Series
> - CDP Series

Dell SonicWALL GMS 8.2 supports the following Dell SonicWALL appliances and firmware versions:

Component requirements

Dell SonicWALL platforms	Dell SonicWALL firmware version
Network security appliance	
SuperMassive 10000 Series	SonicOS 6.0 or newer **NOTE:** Only partial policy management and reporting support is currently available. The following SuperMassive specific features are not supported for centralized policy management in GMS: • Multi-blade Comprehensive Anti-Spam Service (CASS) • High Availability/Clustering • Support for Management Interface • Flow Reporting Configurations • Multi-blade VPN • Advanced Switching • Restart: SonicOS versus Chassis Contact your Dell SonicWALL Sales representative through https://support.software.dell.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
Dell 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 8.2 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 8.2

This section provides procedures for upgrading an existing Dell SonicWALL GMS 8.1 or newer installation to GMS 8.2.

GMS cannot be upgraded directly from 8.1 to 8.2. The process of upgrading from GMS 8.1 to GMS 8.2 requires following a specific set of steps, as there are dependencies on each of the files installed. You CANNOT upgrade directly from GMS 8.1 to GMS 8.2. The correct upgrade path is **GMS 8.1 > 8.1 Service Pack 1 > Hotfix 173751 > Hotfix 168044 > and then finally to 8.2**.

As mentioned in Pre 8.2 Upgrade Preparation, complete the following before upgrading:

- Perform a backup to GMS between each Hotfix update.
- GMS requires a mandatory restart between each update.
- Apply each Hotfix in the upgrade path on all systems in the distributed deployment before upgrading to 8.2.

The GMS 8.0/8.1 database is reporting problems when managing SonicWALL firewalls running SonicOS 6.2.6. The problems appear as an inability to access database reports because of database corruption caused by SYSLOG anomalies in SonicOS 6.2.6. These problems are resolved in GMS 8.2 and syslog reports are generated as normal.

See the associated Knowledge Base articles #213012 and #213411 at https://support.software.dell.com/kb-product-select for more information.

GMS can be configured for a single server or in a distributed environment on multiple servers. GMS 8.2 can be installed as a fresh install or as an upgrade from GMS 8.1. If you wish to perform a fresh install of GMS 8.2, refer to the *GMS Getting Started Guide* that relates to your GMS deployment.

Consider the following before upgrading to GMS 8.2:

- 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 8.2 logs into the appliances using HTTPS only.
- The scheduled reports created in GMS 8.0 continue to work properly after upgrading to 8.2. 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 **Dell 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 8.2 and others running 8.1.

> **NOTE:** DO NOT start/stop the **Dell SonicWALL Universal Management Suite - Database** service manually, before or after upgrading to 8.2. After the upgrade, the **Dell 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 8.2, complete the following steps:

1. Navigate to **www.mysonicwall.com**.
2. Download the GMS 8.2 software along with the required previous versions and Hotfixes.
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.
7. Continue these steps in order with the upgrade path as **GMS 8.1 > 8.1 Service Pack 1 > Hotfix 173751 > Hotfix 168044 > and then finally to 8.2**.

Upgrading the GMS virtual appliance

The GMS Virtual Appliance cannot be upgraded directly from 8.1 to 8.2. See Pre 8.2 Upgrade Preparation for more information.

The process of upgrading from GMS 8.1 to GMS 8.2 on a virtual machine requires following a specific set of steps, as there are dependencies on each of the files installed. You CANNOT upgrade directly from GMS 8.1 to GMS 8.2. The correct upgrade path is **GMS 8.1 > 8.1 Service Pack 1 > Hotfix 173751 > Hotfix 168044 > and then finally to 8.2**.

As mentioned in Pre 8.2 Upgrade Preparation, complete the following before upgrading:

- Perform a backup to GMS between each Hotfix update.
- GMS requires a mandatory restart between each update.
- Apply each Hotfix in the upgrade path on all systems in the distributed deployment before upgrading to 8.2.

The GMS 8.0/8.1 database is reporting problems when managing SonicWALL firewalls running SonicOS 6.2.6. The problems appear as an inability to access database reports because of database corruption caused by SYSLOG anomalies in SonicOS 6.2.6. These problems are resolved in GMS 8.2 and syslog reports are generated as normal.

See the associated Knowledge Base articles #213012 and #213411 at https://support.software.dell.com/kb-product-select for more information.

In a distributed environment, shut down all GMS servers except the one that is running the database. GMS servers with the **Dell 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 8.2 and others running 8.1.

ⓘ **NOTE:** DO NOT start/stop the **Dell SonicWALL Universal Management Suite - Database** service manually, before or after upgrading to 8.2. After the upgrade, the **Dell 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 8.2 64-bit Virtual Appliance, refer to the *GMS Virtual Appliance Getting Started Guide*.

To upgrade, complete the following:

1. Download the GMS 8.2 file from **www.mysonicwall.com** to your workstation software along with the required previous versions and Hotfixes: **sw_gmsvp_vm_eng_8.2.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.
7. Continue these steps in order with the upgrade path as **GMS 8.1 > 8.1 Service Pack 1 > Hotfix 173751 > Hotfix 168044** > and then finally to **8.2**.

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.

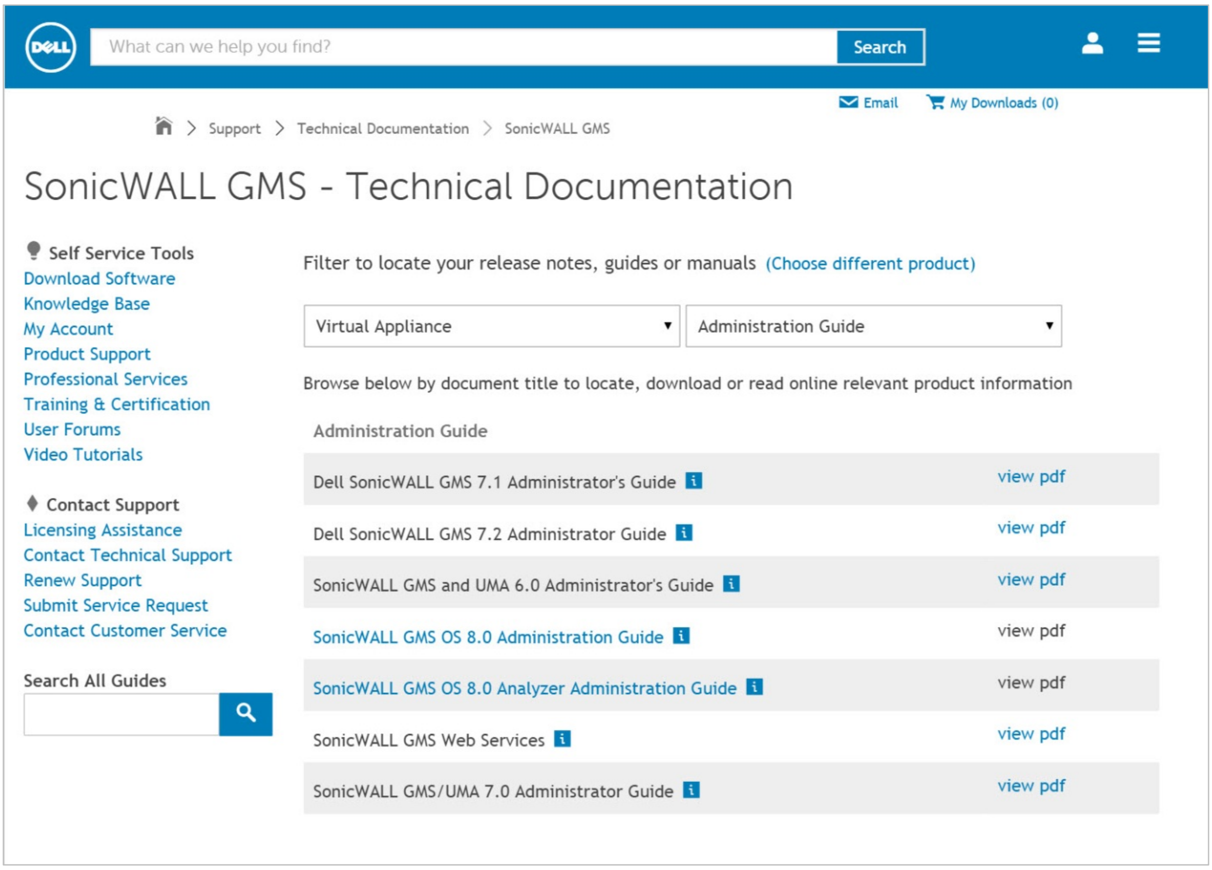
The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. In addition, the portal provides direct access to product support engineers through an online Service Request system. To access the Support Portal, go to http://software.dell.com/support/.

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

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

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



SonicWALL GMS - Technical Documentation

Filter to locate your release notes, guides or manuals (Choose different product)

Virtual Appliance ▾ | Administration Guide ▾

Browse below by document title to locate, download or read online relevant product information

Administration Guide

Dell SonicWALL GMS 7.1 Administrator's Guide	view pdf
Dell SonicWALL GMS 7.2 Administrator Guide	view pdf
SonicWALL GMS and UMA 6.0 Administrator's Guide	view pdf
SonicWALL GMS OS 8.0 Administration Guide	view pdf
SonicWALL GMS OS 8.0 Analyzer Administration Guide	view pdf
SonicWALL GMS Web Services	view pdf
SonicWALL GMS/UMA 7.0 Administrator Guide	view pdf

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/

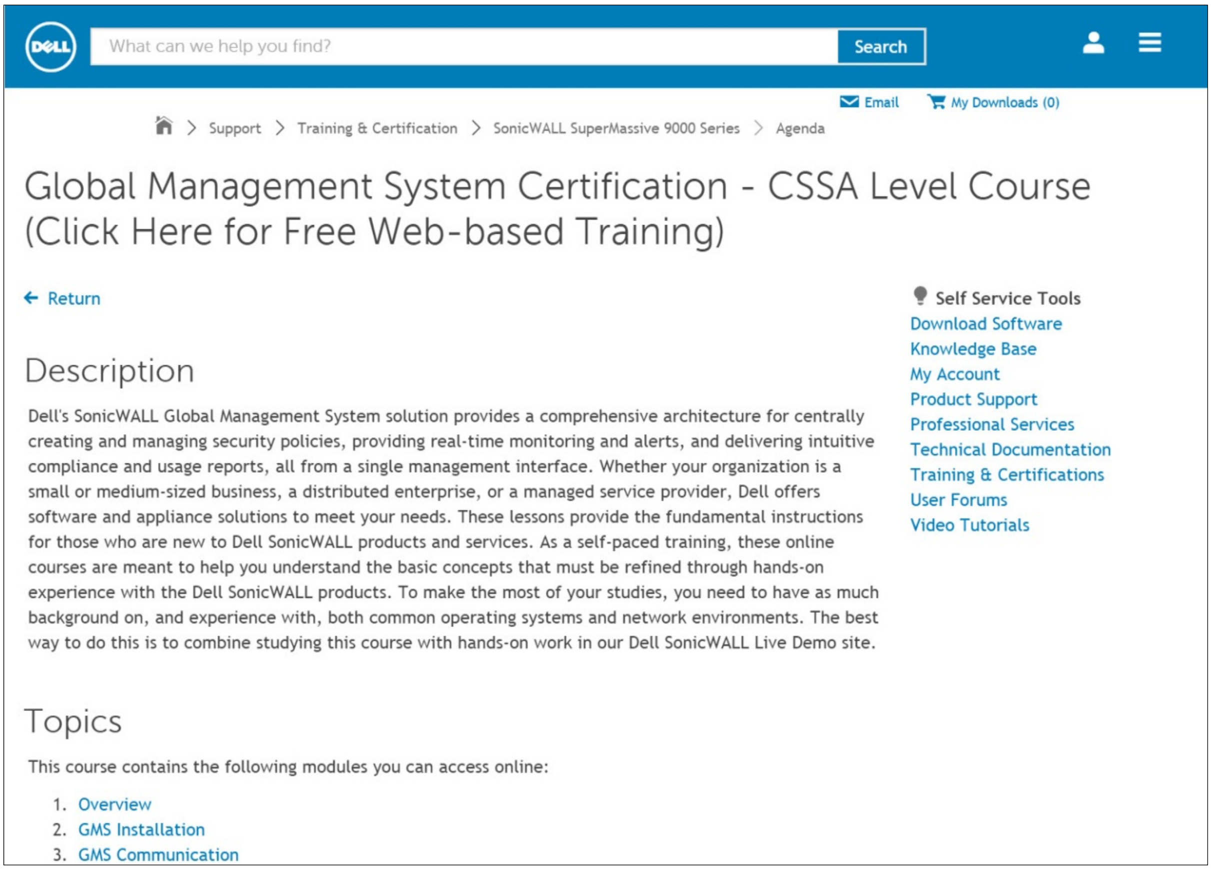
Online training materials

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**.



Global Management System Certification - CSSA Level Course (Click Here for Free Web-based Training)

Description

Dell's SonicWALL Global Management System solution provides a comprehensive architecture for centrally creating and managing security policies, providing real-time monitoring and alerts, and delivering intuitive compliance and usage reports, all from a single management interface. Whether your organization is a small or medium-sized business, a distributed enterprise, or a managed service provider, Dell offers software and appliance solutions to meet your needs. These lessons provide the fundamental instructions for those who are new to Dell SonicWALL products and services. As a self-paced training, these online courses are meant to help you understand the basic concepts that must be refined through hands-on experience with the Dell SonicWALL products. To make the most of your studies, you need to have as much background on, and experience with, both common operating systems and network environments. The best way to do this is to combine studying this course with hands-on work in our Dell SonicWALL Live Demo site.

Topics

This course contains the following modules you can access online:

1. Overview
2. GMS Installation
3. GMS Communication

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.

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: 12/9/2016

232-003379-00 Rev B