Symantec by Broadcom Software

Symantec™ Messaging Gateway 10.9.0 Release Notes

Table of Contents

Symantec Messaging Gateway 10.9.0 Release Notes

About Symantec Messaging Gateway 10.9.0

Document publication date: 1/31/2024

Symantec Messaging Gateway SMG 10.9.0 is the update to previous versions of SMG. All functionality of SMG 10.7.x and 10.8.x is maintained unless otherwise noted.

NOTE: You must be at SMG 10.6.6 or later to update to SMG 10.9.0.

What's new in Symantec Messaging Gateway 10.9.0

This release (10.9.0) includes the following key features:

- **OIDC Support** - Support Single-Sign-On authentication for administrators and Quarantine users.
- **REST API Support** - Support for REST API access to query and monitor the **email processing** events reported to the Message Audit Log as well as **host** and **mail queue** status for SMG via your preferred REST tool.

This release also includes the following feature changes and updates:

- The ability to set the ciphers used for secure control center connections.
- The ability to set a policy condition to act on file encryption status.
- The ability to collect diagnostics data that includes enduser preferences.
- The ability to import DKIM certificate files that include CRLF at the end of any lines in the certificate file.
- Spam quarantine summary now includes both friendly and unfriendly addresses together.
- SMG now provides the ability to delete all stats files with the CLI command, delete statsdata.

Deprecation notice

Legacy URL Reputation Service Deprecation

By the end of calendar year 2024, the legacy URL reputation service used by SMG in releases from 10.8.0 or earlier will be retired. In SMG 10.8.1, we introduced the URL categorization service, and the two services have been offered in parallel since.

Next Steps

Depending on when you most recently freshly installed SMG on your appliances, your next steps for this change will differ. Even if you've upgraded the version of SMG running on your appliances, the focus of this begins on the version you started your configuration with.

There are two potential scenarios:

- If you last freshly installed your SMG infrastructure at version 10.8.1 or later, your system configuration is already using the URL categorization service, and no change is required.
- If your SMG infrastructure was installed using version 10.8.0 or earlier, you will need to manually disable the legacy URL reputation service on your appliance, and modify your email policy to use the URL categorization service instead to avoid an interruption in this service/functionality.

To disable legacy URL reputation, uncheck **Enable URL reputation filtering** on the **Spam** > **Scan Settings** page.

To implement URL categorization policy:

Browse to **Spam** > **Policies** > **Email** and enable and apply the following policies for all users you wish to protect from spam and malicious URLs:

- **Spam URL: Modify subject line with "[Spam URLs]" (default)**
- **Malicious URL: Delete Message (default)**

You can modify the action on these policies as your organization's spam and malicious URL policies dictate.

Documentation

You can access English documentation at the following website:

https://techdocs.broadcom.com/us/en/symantec-security-software/email-security/messaging-gateway/10-9-0.html

Check the following website for any issues that are found after these release notes were finalized:

https://knowledge.broadcom.com/external/article?articleId=251865

To access the software update description from the Control Center, click **Administration > Hosts > Version**. On the **Updates** tab, select a version and click **View Description**.

To view the Symantec support policy for SMG, see the following links:

https://knowledge.broadcom.com/external/article?legacyId=tech89724

https://knowledge.broadcom.com/external/article?legacyId=tech123135

To read the translated documentation, go to https://techdocs.broadcom.com/us/en/symantec-security-software/email-security/messaging-gateway/10-8-0.html and select the desired language from the dropdown list in the upper right corner of the screen. SMG 10.9.0 supports French, Spanish and Japanese versions of the documentation and the product's user interface locale.

> **NOTE**
> Translated documentation will be available shortly after this release is publicly available.

Support policy

Broadcom provides standard support for Symantec products, including SMG. Support is offered for only the most recent build of the licensed software.

To view the Symantec support policy for SMG, see the following links:

https://knowledge.broadcom.com/external/article?legacyId=tech89724

https://knowledge.broadcom.com/external/article?legacyId=tech123135

Supported platforms

You can update to SMG 10.9.0 on any of the following platforms:

- **HARDWARE:** All supported hardware versions: 8390/S450 purchased after 2018.
  For more information about SMG hardware testing support, go to the following URL:
  https://knowledge.broadcom.com/external/article?legacyId=TECH123135
- **Microsoft Azure**.
- **VMware:** VMware ESXi/vSphere 7.0/8.0
- **Microsoft Hyper-V:** Windows Server 2016 and later.

NOTE
Hyper-V installation from a VHD image is not supported.

- **Linux Kernel Virtual Machine (KVM):** The kernel component of KVM is included in mainline Linux as of 2.6.20. The user space component of KVM is included in mainline QEMU as of 1.3.

Unsupported platforms

Unsupported platforms are as follows:

- Any platform that is not listed in the Supported Platforms section of this document.
- Hardware platforms 8220, 8240, 8260, 8320, 8340, 8360, and 8380.

Symantec does not test software releases on appliance models for which the hardware warranty period has expired.

To determine what hardware version you have, at the command line type the following:

```
show --info
```

Supported web browsers

Access to the SMG Control Center has been tested and verified with the following web browser versions:

- Mozilla Firefox 115 or later
- Google Chrome 119 or later

Supported paths to version 10.9.0

You can use any of the following methods to update to SMG 10.9.0:

- Software update from version 10.6.6 or later on supported hardware or in a supported virtual environment.
- OS Restore from ISO on supported hardware or in a supported virtual environment.
- VMware installation with OVA template.

NOTE
Broadcom provides an OVA template that can load an SMG virtual machine into VMware. This template is designed for demonstration or testing purposes. You should use this template for deployment in a production environment only if explicitly recommended. For any production environment, create a virtual machine in accordance with best practices as outlined in the Symantec Messaging Gateway Installation Guide, located here: https://techdocs.broadcom.com/us/en/symantec-security-software/email-security/messaging-gateway/10-9-0/related-documents.html. Then install SMG using the ISO file.

Important information about installation in virtual environments

SMG 10.9.0 supports four virtual environments: VMware, Microsoft Hyper-V, Microsoft Azure, and Linux KVM.

To install on Microsoft Azure

A single method is supported for installing SMG on Azure:

VHD file	Upload the SMG VHD file to Azure to create an image for installation, and use that image to create VM in Azure.
VHD file	

To install on VMware

Two methods for installing on supported VMware platforms are:

ISO file	You can load the ISO file into a preconfigured virtual machine. You can use the ISO file on VMware ESXi/vSphere 7.0/8.0
OVA file	You can also load the OVA, which includes the virtual machine configuration. You can use the OVA for VMware ESXi/vSphere 7.0/8.0

To install on Hyper-V

Symantec supports one method for installing on supported Hyper-V platforms:

ISO file	You can load the ISO file into a pre-configured virtual machine. You can use the ISO file on Windows Server 2016 and above.

NOTE
Hyper-V installation from a VHD image is not supported.

See the *Symantec ™ Messaging Gateway 10.9.0 Installation Guide* (located at https://techdocs.broadcom.com/us/en/symantec-security-software/email-security/messaging-gateway/10-9-0/Related-Documents.html) for instructions and system requirements.

To install on KVM

Symantec supports one method for installing on KVM platforms:

ISO file	You can deploy an instance of Symantec Messaging Gateway from an ISO image on a computer running Linux KVM. For an example installation of KVM on a system running the CentOS Linux distribution, see the Symantec Messaging Gateway 10.9 Installation Guide.

See the *Symantec ™ Messaging Gateway 10.9.0 Installation Guide* (located at https://techdocs.broadcom.com/us/en/symantec-security-software/email-security/messaging-gateway/10-9-0/Related-Documents.html) for instructions and system requirements.

Important information before you update to version 10.9.0

This section describes the migration information that you should read before you update to version SMG 10.9.0.

ATTENTION
Do not update the Control Center from the SMG UI. The Control Center must be updated from the Command Line Interface. Once the Control Center is updated, you can use the SMG UI to update other quarantines or scanners.

The best practices for all updates are listed in Best practices for all updates.

You can only update to SMG 10.9.0 from SMG 10.6.6 or later.

If you are updating from 10.6.6, you should enable the new Malware configuration options for better detection. These options use static and dynamic artificial intelligence and the relationship-based AI for file and mobile detections.

NOTE
After the upgrade completes, you might not automatically return to the login screen. Instead, the system might display a screen that offers the choices **Advanced** or **Go Back**. Reload the page in your browser to return to the login screen.

If you are NOT using the policy sharing feature for email content filtering introduced in Symantec Messaging Gateway 10.7.4, you may skip this section. If you ARE using policy sharing, you must ensure that all Control Center instances (both Central and Remote) are updated to the same product version.

Assume the following current deployment:

Cluster 1 = CC1, which controls Scanner01C1 and Scanner02C1.

Cluster 2 = CC2, which controls Scanner01C2 and Scanner02C2.

Cluster 3 = CC3, which controls Scanner01C3 and Scanner02C3.

Further, assume that CC1 is the central Control Center and CC2 and CC3 are the remote Control Centers.

Given the above scenario, follow these steps:

1. Update CC3.
2. Update the Scanners attached to CC3 (Scanner01C3 and Scanner02C3).
3. Update CC2.
4. Update the Scanners attached to CC2 (Scanner01C2 and Scanner02C2).
5. Update CC1 (the central Control Center for the cluster).
6. Update the Scanners attached to CC1 (Scanner01C1 and Scanner02C1).

The above steps are provided as an example of the recommended order in which to update your Scanners. You can update the Scanners in a different order (e.g. CC3 -> CC2 -> CC1, or CC2 -> CC3 -> CC1), as long as you update the Control Centers and the Scanners attached to them to the same update version.

NOTE

The software update process can take several hours. During this process, mail throughput is unaffected. However, the mail that is intended for quarantine remains in the delivery queue until migration is complete.

Table 1: Best practices for all updates

Item	Description
Perform a backup	Take a full system backup before you run the software update, and store it off-box.
Do not restart before the update process is complete.	The software update process may take several hours to complete. The system restarts automatically when the update completes. **Warning!** If you restart before the process is complete, data corruption is likely to occur. If data corruption occurs, the factory image must be reinstalled on the appliance.
Delete log messages.	If your site policies allow it, delete all scanner and DDS log messages before you update.
Stop mail flow to scanners and flush queues before you update.	To reduce scanner update time and complexity, stop mail flow to scanners and drain all queues. Then start the update. The goal is to process or deliver the messages in the queues, particularly the delivery queue, before starting the update. To halt incoming messages, click **Administration > Hosts > Configuration**, and edit a scanner. On the **Services** tab, click **Do not accept incoming messages** and click **Save**. Repeat the process individually for each scanner on the system. Allow some time for messages to drain from your queues. To check the queues, click **Status > SMTP > Message Queues**. Flush the messages that are left in the queues.

Item	Description
Update Control Center first.	Perform the update in this order: Update the Control Center, flush the queues on the scanners, and then update the scanners. • If you choose to update the scanners first, use the command line interface to update remote scanners. • After updating the Control Center, update your scanners as soon as possible. The Control Center can propagate configuration changes only to a scanner using the same version of the software. Running different versions on the Control Center and scanners for more than 24 hours is not advised. • Making configuration changes when the Control Center and scanners are running different versions is unsupported.
Perform software update at off-peak hours.	Plan to update the Control Center appliance and scanners during off-peak hours. This reduces the amount of mail that builds up in the queue. After you update the Control Center, wait a few minutes for queues to clear before updating the scanners. Software update of a scanner takes less time than the software update of the Control Center. Scanners cannot quarantine messages on the Control Center during the Control Center update process. Messages may build up in a queue. When you update a scanner, it goes offline. Scanner resources are unavailable during the update process.
Check available space on the / partition before you start the update process.	When updating, the installation process does not pre-test the available space on the / partition before starting the update. If the available space is insufficient, a partial installation of the new release can occur, leaving the system in an unsupported state. You should verify that at least 500 MB of space is available before you begin the update. To find out how much space is available, use the CLI command: `monitor other_free` (output is not labeled; 500 MB is 500000 in this context). To free up space, use the CLI command: `list --temp` or `list --top | grep -v data` and then use the CLI command: `delete file <filename>` to delete unneeded files in `/tmp` and `/var/tmp`.
Monitor the update process carefully.	If you observe unexpected behavior during the software update process, or if the process fails or appears to terminate before completion, examine the Messaging Gateway log files to verify that the update succeeded and to determine whether further action is required.

After 10.9.0 installation

To verify that your appliance is running SMG version 10.9.0, log into the command line and type the following command:
`show --version`

Perform a LiveUpdate as soon as possible after the update completes. The virus definitions in the new version may be out of date.

Resolved issues in 10.9.0

This section describes the issues that are resolved in SMG 10.9.0.

Table 2: Resolved issues in SMG 10.9.0

Issue	Resolution
Issue ID: **SMGA-2347** **Hosts** > **Software and Service** > **Status** > **Conduit** > reports **Last day zero filter update** in red text.	This issue has been resolved.
Issue ID: **SMGA-3921** In some cases, when activating a standalone quarantine, reports the error, "Cannot reroute messages in the delivery queue".	This issue has been resolved.
Issue ID: **SMGA-3927** The Spam Quarantine Summary List checkbox behavior is inconsistent.	The following option, **Spam** > **Settings** > **Email Spam** > **Display friendly sender address** has been removed. Both the friendly name and email address are now shown by default.
Issue ID: **SMGA-3932** Not all settings defined in the intial setup wizard engine and filtering configuration (log level, proxy settings) that can be modified successfully apply to the system until after the first reboot. Attempting to make a change prior to the first reboot, the following error text **Error creating runner lock file**.	This issue has been resolved.
Issue ID: **SMGA-3943** The error message, "**http 413 (Request Entity Too Large)**" occurs repeatedly in the conduit log.	The CLI command **delete statsdata** has been updated to allow users to resolve this issue. Customers MUST take this action themselves to resolve the problem.
Issue ID: **SMGA-3951** In some unsupported platforms, the CLI command **show --info** displays an error.	This issue has been resolved.
SMGA-3955 No alert is generated when the certificates for **Application** or **TLS & HTTPS** are about to expire, or have expired.	This issue has been resolved.
Issue ID: **SMGA-3962** Changes made on a standalone quarantine system cause the error **Configuration saved successfully but could not publish configuration to the following hosts...** to appear.	This issue has been resolved.
Issue ID: **SMGA-3995** SMG running on Azure reports the following error - **Can't store backup - Agent config did not permit backup**.	This issue has been resolved.
Issue ID: **SMGA-3993** The buttons **Delete all** and **Release** are grayed out together when placing the cursor over the button **Release**.	This issue has been resolved.
Issue ID: **SMGA-3997** When searching MAL for messages using the **size** attribute, an application error message is displayed.	This issue has been resolved.
Issue ID: **SMGA-4003** The policy action **Password Protected Filles** does not function with rar and 7z encrypted files when used as part of Content Policy.	A new option available during policy filter creation, **Is Encrypted** is now available, and functions as expected.
Issue ID: **SMGA-4038** Installation of DKIM keys fail if certain spacing characters are present in the file.	This issue has been resolved.

Issue	Resolution
Issue ID: **SMGA-4042, SMGA-3632** When adding annotation text using special characters, the appliance fails to display the text properly, or insert the expected text.	This issue has been resolved.
Issue ID: **SMGA-4043** When using a standalone quarantine, end-user preferences (personal blacklists, whitelists, and language restrictions) are not supported.	This issue has been resolved.
Issue ID: **SMGA-4085** Making a change on the **Edit Host** page reverts DNSSEC and host entries to their default values, even if no changes were made to those tabs.	This issue has been resolved.
Issue ID: **SMGA-4143** During an upgrade to 10.9.0 from 10.8.x where a standalone quarantine is in use, the Directory Data Service (DDS) Profile ID configuration on that standalone quarantine appliances becomes corrupt. This prevents end-users from being able to log in to the quarantine, as the system displays this error text: "**An invalid profile ID was used to access the Directory Data Service. Check the Control Center and DDS logs for details. DDS error code: 800205"**	This issue will not occur on new installs of SMG 10.9.0, but it may impact configurations following an upgrade to 10.9.0 from 10.8.x. **MITIGATION**: Following an upgrade from 10.8.x to 10.9.0, customers will need to log in to the remote quarantine system, select an existing DDS configuration and click **Save** without making any changes.
Issue ID: **SMGA-1199** CSV-exported report for Unscannable - Summary does not have the Group by Hour data.	This issue has been resolved.
Issue ID: **SMGA-4101** New lines (carriage returns) in plain text annotations are replaced with **\r\n**.	This issue has been resolved.
Issue ID: **SMGA-4020** In some cases, when installing a patch, the patch notes were not displayed.	This issue has been resolved.
Issue ID: **SMGA-3986** Previously, there was no method for the customer to remove undesirable ciphers from the list of enabled protocols.	The CLI command, `cc-config set-ciphers` , has been added to permit modifications to the list of enabled ciphers. The default list of ciphers has been updated to include the following list of ciphers: `TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA`
Issue ID: **SMGA-2898** For the first few minutes, following applying a license to the appliance, the dashboard displays **unlicensed**, in error, as the license page shows the valid license, after 5 minutes, the error clears, showing the correct license information.	This issue has been resolved.
Issue ID: **SMGA-4009** Previously, end-users were allowed to log in to an inactive quarantine, however they could not release or delete messages.	End users are no longer permitted to log in to an inactive quarantine.

Issue	Resolution
Issue ID: **SMGA-2224** In some cases a database restore would produce an erroneous error, shortly before reporting that the restoration was successful.	This issue has been resolved.
Issue ID: **SMGA-3954** In prior releases the **Update Version** screen on a standalone quarantine appeared to allow the user to perform an upgrade, but if attempted, the upgrade did not take place. Upgrades of this type are unsupported, so the action this action was intended.	The **Update Version** screen is now read-only. Upgrading should be done only from the CLI or from the Control Center.
Issue ID: **SMGA-3938** The status of an inactive or quiescing quarantine was not visible on the page where the contents of the quarantine are administered.	The status is now visible.
Issue ID: **SMGA-3947** Under some conditions, a stand alone quarantine that has been upgraded from 10.8.0 to 10.9.0 may experience errors when modifying it's own configuration.	This problem has been resolved, but if this is not yet addressed by the customer, the customer needs to add the IP address of the quarantine to its agent, using the `agentconfig --add` CLI command

Known issues in 10.9.0

This section describes the known issues in SMG 10.9.0.

Table 3: Known issues in SMG 10.9.0

Issue	Description
Issue ID: **SMGA-105** Content filter policy fails to catch images within .rtf attachments.	Policy defined to trigger based on *If the attachment or body part is in the attachment list "Image Files"* fails to detect images embedded in RTF document attachments.
Issue ID: **SMGA-169** BCC allows active session for deleted accounts.	From a BCC, administrators can delete their own account, and remain active while logged in to a session. If they are signed in to the appliance at the time another admin disables their account, they can continue to perform administrative actions, including re-enabling their own account. Access is checked during login, not during operation. This is planned to be fixed in a subsequent release.
Issue ID: **SMGA-641** The error "server refused the connection" appeared in the `catalina.out` log file during update.	See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?legacyId=TECH232860
Issue ID: **SMGA-1060** When a Content Filtering policy to detect executable files was in place and an `.exe` file was compressed within an ISO file, Content Filtering could not detect the `.exe`.	**This issue has been partially resolved.** Content Filtering can now detect `.exe` files compressed within most ISO files. Detection issues persist when the ISO file was compressed using some less commonly used compression tools. See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=226215

Issue	Description
Issue ID: **SMGA-3144** (Policy Sharing) After configuration of a Central or a Remote Control Center, the **Login** page does not always appear.	After enabling policy sharing on a Central or Remote Control Center, a browser error can appear that prevents the display of the **Login** page. **b**: Wait for the Control Center service to finish restarting and refresh your display. See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=204559
Issue ID: **SMGA-2986** Smart Card authentication fails following software update.	Smart card authentication is currently set to "off" by default following a software update. **WORKAROUND**: At the command line, enter `cc-config client-cert --on` to re-enable Smart Card authentication. See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=225873
Issue ID: **4228058** A spreadsheet that is embedded in a Word document is not detected as a spreadsheet document.	**MITIGATION**: Add Word document types in any policies you use to track or control Sxcel file spreadsheet attachments.
Issue ID: **SMGA-3461** On the **Edit customer-specific URL category settings** page, the list of customer-specific categories that no longer exist is not cumulative. The list shows only the category that has most recently become unavailable.	This behavior occurs only when WebPulse permanently removes a URL category from its detection engine, which happens very infrequently. See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=225884
Issue ID: **SMGA-3758** The Spam Expunger link on a BCC for a standalone quarantine points to Quarantine Settings page for the BCC, rather than the Quarantine Settings page on the active remote Quarantine server.	Expunger management must be done on active quarantine server - in this case, the link to the local quarantine instance is incorrect and should be ignored. **WORKAROUND**: Browse to the standalone quarantine to view this data.
Issue ID: **SMGA-3867** *Application Error* appears on the software upgrade page while upgrading.	When pushing an upgrade from a Control Center to a BCC, the brightmaillog.log reports an application error. **WORKAROUND**: Ignore the error, as it occurs as a result of certain subsystems going offline during the upgrade. Once the upgrade of the BCC is complete, the issue no longer occurs.
Issue ID: **SMGA-3968** Older SMG instances (primarily on virtual appliances) that were initially installed at version 10.6.6 (2018) or earlier may experience memory problems due to the fact that the swap file on these older systems is much smaller than modern appliances.	If this applies to you, contact Broadcom support for assistance.
Issue ID: **SMGA-4022** Following upgrade via the UI, the login page may appear blank.	Steps to mitigate this issue: 1. Do not upgrade to 10.9.0 via the BCC, only via the CLI (at least for the BCC itself). 2. If you do upgrade via the BCC, you will need to manually reboot the system once the upgrade completes. 3. If you do upgrade via the BCC, you will need to monitor the upgrade status via the CLI as monitoring via the BCC will not work.

Issue	Description
Issue ID: **SMGA-4097** If the customer enables any Sender Authentication features (DKIM, DMARC, etc.) and removes all domains from the **Domain Authentication** list on the **Sender Authentication** page, then regardless of which radio button they have selected, the MTA will not start up.	**WORKAROUND**: Ensure that there is at least one domain in the domain authentication list. This behaviour will be fixed in a future release.
Issue ID: **SMGA-4125** Uploading an invalid file to **Administration** > **Domain keys** results in an application error, rather than a more user-friendly error.	**MITIGATION**: Ensure that all domain key files are valid. A future release will include a more decriptive error message.
Issue ID: **SMGA-3461** On the customer specific URL categories page, when a WebPulse category is removed, the URLs categorized with it are reported as non-exist list. URLs shows only the latest URL, overwriting existing entries.	**MITIGATION**: This is caused when WebPulse removes or renames a URLcategory. To prepare for such changes, regularly monitor the WebPulse Site Review page for warnings of planned changes:https://sitereview.bluecoat.com/.
Issue ID: **SMGA-4188** Content policies for **Messages that contain attachments** in the attachment list that use two conditions and an action of **delete matching attachment** will only delete the first matching attachment in messages that contain multiple attachments that match the condition.	**MITIGATION**: Change the policy action to **delete attachments in the list** or specify only a single condition. This issue will be addressed in a future release.
Issue ID: **SMGA-4193** Application error appears on the Administrator page after performing a quarantine-only backup restore.	**MITIGATION**: Customers are advised to use the **Full backup** option for backup and restore instead of the quarantine-only backup or custom backup.
Issue ID: **SMGA-4194** Administration policy with API view access is not restored from backup correctly.	**MITIGATION**: Customers are advised to use the **Full Backup** option for backup and restore instead of the quarantine-only backup or custom backup.
Issue ID: **SMGA-4195** A Control Center configured to use OIDC is not restored from backup correctly.	**MITIGATION**: Customers are advised to use the **Full Backup** option for backup and restore instead of the quarantine-only backup or custom backup.
Issue ID: **SMGA-4196** In some circumstances, upgrading an S450 hardware appliance from a release earlier than 10.8.1 to 10.9.0 prevents system networking from functioning as expected.	**MITIGATION**: Customers are advised to install 10.8.1 first, then 10.9.0. In the event this has happened to you, you may require serial console or front panel access to the appliance to revert the configuration.

Where to get more information

You can access English documentation at the following website:

https://techdocs.broadcom.com/us/en/symantec-security-software/email-security/messaging-gateway/10-9-0.html

You can access translated versions of the documentation at https://techdocs.broadcom.com/us/en/symantec-security-software/email-security/messaging-gateway/10-9-0.html. Select the desired language from the dropdown list in the upper right corner of the screen. SMG 10.9.0 supports French, Spanish and Japanese versions of the documentation and the product's user interface locale.

Check the following website for any issues that are found after these release notes were finalized:

https://knowledge.broadcom.com/external/article/151063


Symantec
by Broadcom Software