Symantec™ Messaging Gateway 10.7.4 Release Notes

Table of Contents

Symantec Messaging Gateway 10.7.4 Release Notes

About Symantec Messaging Gateway 10.7.4

Document publication date: 12/9/2020

Symantec Messaging Gateway SMG 10.7.4 is the update to previous versions of SMG. All functionality of SMG 10.6.x and 10.7.x is maintained unless otherwise noted.

NOTE: You must be at SMG 10.6.6 or later to update to SMG 10.7.4.

What's new in SMG 10.7.4

This release (10.7.4) introduces support for policy sharing. Administrators can create, edit and delete global policies using a central Control Center, and then publish these changed policies to all remote Control Centers that are linked to the central one in a cluster. Policy sharing is supported for Content Filtering only at this time. Of the six categories of resources that can be used in a content filtering policy, all of them except **Records** have been updated to support the policy sharing feature.

IMPORTANT: to enable the shared policy feature across networks, ensure that you allow traffic on port 41616.

VMWare 6.0 is in EOL status, and as a result Symantec Messaging Gateway is dropping support for that platform as of this release. Existing installations on VMWare 6.0 can upgrade to 10.7.4, but new VMs should be created and run under 6.7. See this article for details: https://kb.vmware.com/s/article/66977. Customers using ESX 6.0 should note that SHA1 is no longer considered secure, and thus they must either convert the OVA or do an ISO install.

This release also includes:

- Several additions to MAL that provide more information for customers about TLS ciphers and about the timing of SMTP transactions.
- Improved ability to detect and handle encrypted attachments.
- Improvements to safeguard message handling during the action phase.
- The Content Filtering policy option **Modify Clickable URLs** now affects the message subject as well as attached and embedded messages. It also intelligently skips modifying URLs that were already modified (in the case of a back-and-forth conversation of quoted emails).
- Individual customers can no longer opt out of the collection of telemetry; all SMG users are now automatically included. See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=204204
- The support account's access to the `tcpdump` CLI command has been removed to address potential security concerns.
- The default minimum TLS level has been changed from 1.0 to 1.2 for fresh installations of SMG.
- ClickTime NOCLICK URLs are now checked in the body of the message. If they exist, SMG does not modify the URL, and continues checking the next URL in the message until all URLS are checked. SMG modifies any URLs that do not have the NOCLICK modifier.

Documentation

You can access English documentation at the following website:

https://techdocs.broadcom.com/us/en/symantec-security-software/email-security/messaging-gateway/10-7-4.html

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

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

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

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

http://go.symantec.com/security_appliance_support

http://go.symantec.com/appliance_hw_support

To read the translated documentation, go to https://techdocs.broadcom.com/us/en/symantec-security-software/email-security/messaging-gateway/10-7-4.html and select the desired language from the dropdown list in the upper right corner of the screen. SMG 10.7.4 supports French, Spanish and Japanese versions of the documentation and the product's user interface locale. PDF versions of the documentation are available in Brazilian Portuguese.

Support policy

Symantec provides standard support for only the most current build of the licensed software.

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

http://go.symantec.com/security_appliance_support

http://go.symantec.com/appliance_hw_support

Supported platforms

You can update to SMG 10.7.4 on any of the following platforms:

- **HARDWARE:** All supported hardware versions: 8380-S450, 8380 purchased after March 2010, 8360 purchased after 2010, and 8340 purchased after May 2015.
  For more information about SMG hardware testing support, go to the following URL:
  http://www.symantec.com/docs/TECH123135
- **VMWARE:** VMware ESXi/vSphere 6.5/6.7

  NOTE

  VMWare 6.0 is in EOL status, and as a result Symantec Messaging Gateway is dropping support for that platform as of this release. Existing installations on VMWare 6.0 can upgrade to 10.7.4, but new VMs should be created and run under 6.7. See this article for details: https://kb.vmware.com/s/article/66977. Customers using ESX 6.0 should note that SHA1 is no longer considered secure, and thus they must either convert the OVA or do an ISO install.

  Support for VMware ESXi/vSphere 5.5 ended with SMG 10.6.6.

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 and 8320.
- Hardware platform 8340 (PowerEdge 860, R200, R210, and 210-11 xl versions) purchased on or before May 2015.
- Hardware platforms 8360 (PowerEdge 1950) and 8380 (PowerEdge 2950) purchased on or before March 2010.

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

For more information about SMG out of support hardware, go to the following URL:

http://www.symantec.com/docs/TECH186269

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

```
show --info
```

Supported web browsers

You can access the SMG Control Center on the following supported web browsers:

- Internet Explorer 11 or later.
- Firefox 63 or later. Note that if you plan to use the Smart Card functionality introduced in version 10.7.3 with Firefox, you will need to obtain and install a plugin to support PIV. See https://piv.idmanagement.gov/engineering/firefox/.
- Chrome 70 or later.

Supported paths to version 10.7.4

You can use any of the following methods to update to SMG 10.7.4:

- 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: Symantec 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 10.7.4 Installation Guide*, located here: https://techdocs.broadcom.com/us/en/symantec-security-software/email-security/messaging-gateway/10-7-4/Related-Documents.html. Then install SMG using the ISO file.

Unsupported paths to version 10.7.4

You cannot update to SMG 10.7.4 from versions earlier than 10.6.6.

Important information about installation in virtual environments

SMG 10.7.4 supports two virtual environments: VMware and Microsoft Hyper-V.

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 6.5/6.7.*
OVA file	You can also load the OVA, which includes the virtual machine configuration. You can use the OVA for VMware ESXi/vSphere 6.5/6.7.*

* VMWare 6.0 is in EOL status, and as a result Symantec Messaging Gateway is dropping support for that platform as of 10.7.4. Existing installations on VMWare 6.0 can upgrade to 10.7.4, but new VMs should be created and run under 6.7.

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 preconfigured virtual machine. You can use the ISO file on Windows Server 2012 and Hyper-V Server 2012, and Windows Server 2016 and Hyper-V Server 2016.

See the *Symantec ™ Messaging Gateway 10.7.4 Installation Guide* (located at https://techdocs.broadcom.com/us/en/symantec-security-software/email-security/messaging-gateway/10-7-4/Related-Documents.html) for instructions and system requirements.

Important information before you update to version 10.7.4

This section describes the migration information that you should read before you update to version SMG 10.7.4.

You can only update to SMG 10.7.4 from SMG 10.6.6 or later.

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

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.	Symantec recommends that you 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.
Update Control Center first.	Symantec recommends that you perform the update in this order: Update the Control Center, flush the queues on the scanners, and then update the scanner. • If you choose to update the scanners first, Symantec recommends that you 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.

Item	Description
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`.

After 10.7.4 installation

To verify that your appliance is running SMG version 10.7.4, 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 10.7.4

This section describes the issues that are resolved in SMG 10.7.4.

Table 2: Resolved issues in SMG 10.7.4

Issue	Description and knowledge base article link (if applicable)
The value of **Email Messages > total Message Size** on a **<name of report>** over a sufficiently large time range was always 2,147,483,647 regardless of the real total size.	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH254211
A specific incoming message caused a "`421 4.4.2 service timed out`" error on the MTA.	This error is a rare occurrence with very specific dependencies such as message length and format. See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=174484
When an SMIME-encrypted email was detected as "encrypted," it was no longer TruTyped as "PGP encrypted."	This issue has been resolved. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH254214
Non-ASCII file names were occasionally misrepresented.	In cases where detected file names cannot be properly represented, SMG substitutes the file name with its representation in hexadecimal. This issue has been resolved. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH254215
Setting a LiveUpdate Administrator password that contained multiple '@' signs caused LiveUpdate to fail.	This issue has been resolved. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH256831
SMG allowed users to specify an FTP address for a local LiveUpdate administration server, which caused LiveUpdate to fail.	SMG no longer allows users to specify an FTP address for that purpose. This issue has been resolved. See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=204568

Issue	Description and knowledge base article link (if applicable)
In certain cases BMServer hung, causing a mail outage on all scanners.	In some cases where the SMG had been running for several months it would go into an error state and stop processing mail, requiring a restart. This issue has been resolved.
SMG's OVF package can no longer be used for VM installations.	SMG is now shipping an OVA package instead of OVF for VM installs—please see https://kb.vmware.com/s/article/2151537" for details. This issue has been resolved. See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=204203
Registering a system for the first time using `license-control` caused errors, and registration failed.	Using the CLI command `license-control` resulted in an error of "Bad IP Address" when attempting to register an appliance without Internet connectivity. This issue has been resolved. See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=204569
In some cases inbound messages with PDF attachments triggered Disarm, the attachment was identified as `winmail.dat` and the MTA crashed on signal 6.	This issue has been resolved. See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=204570
Users were unable to upgrade from any versions 10.7.0 through 10.7.3 using the CLI command `localinstall` without network access.	This issue has been resolved when using `localinstall` beginning in 10.7.4. See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=204587
Previous versions of SMG sometimes experienced an SPF-related MTA crash: program terminated with signal 11, segmentation fault.	In some cases the MTA crashed while attempting to validate SPF when the SPF record was self-referential. This issue has been resolved. See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=204595
No option existed for using HTTPS for LiveUpdate.	Previousy there was no straightforward way for a customer to use HTTPS for LiveUpdate. This version of SMG now includes an option to allow this. This issue has been resolved. See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=204596
MTA cores on signal 11 repeatedly in smtp_parse_capabilities.	In some cases, the MTA crashed when attempting to deliver to an MTA that did not follow the RFC standard for MTA responses. This issue has been resolved. This issue has been resolved. See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=204597
Password protected PDF files were being treated as encrypted attachments.	Any file that was detected as encrypted was reported as an encrypted zip file. This issue has been resolved. See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=204598
A customer was experiencing intermittent BMServer crashes that appeared to be connected to regexes used in Content Filtering policies.	This issue has been resolved.

Issue	Description and knowledge base article link (if applicable)
Messages that caused repeated failures got stuck in the inbound or outbound message queue and were reprocessed until they timed out.	If an unrecoverable error occurs during message modification, then the message is now routed to the Bad Messages queue rather than remaining in the inbound queue and continually reprocessed. This issue has been resolved. See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=163604

Known issues in 10.7.4

This section describes the known issues in SMG 10.7.4.

Table 3: Known issues in SMG 10.7.4

Issue	Description
In a distributed setup, when scanner-only (Remote Scanner) is upgraded first, the agent fails to come up on the Remote Scanner after a Software Update from SMG 10.7.1 or previous versions.	The Control Center can no longer communicate with the remote scanner. Update the Control Center first. Mitigation: Update the Control Center and the error will resolve. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH208718
The action 'Strip all attachments' in Content Filtering Policies does not strip all attachments in version 10.7.3 and later.	In some cases attachments that are email messages, text or HTML files are not removed. See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=189268
(Policy Sharing) Global Informational and Quarantine Incidents are not listed under Edit Administrator.	Although an administrator has successfully created Global and Quarantine Incident folders, these folders are not displayed under the Incident management Folder Overview heading. Instead, the administrator must navigate to the Default Incident folder for Informational and Quarantine Incidents to view these messages. This issue is seen in both central and remote Control Centers. See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=204557
Policy names that include "--" prevent converting reports to PDF.	If a report lists a policy name that contains "--", when you attempt to create a PDF, it fails and reports an error. See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=189998
The following message is sometimes seen in the **catalina.out** log during the Control Center shutdown: `SEVERE: The web application [/brightmail] appears to have started a thread named [ActiveMQ InactivityMonitor WriteCheckTimer] but has failed to stop it. This is very likely to create a memory leak.`	This error can be safely ignored. See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=204558
Messages generate scan errors in Disarm and get stuck in the inbound queue.	Mitigation: If a Disarmed document is found in an RTF email message, SMG might fail to Disarm the document. In this case, the fallback annotation will be added to the message. See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=201439

Issue	Description
After configuration of a central or a remote Control Center, the Login page should 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. Mitigation: 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
Backup shouldn't be restored on a Control Center of a different type (central vs. remote).	Once you have configured policy sharing, you can only back up a central Control Center to another central Control Center or a remote Control Center to another remote Control Center. Mitigation: Reinstall and reconfigure the system. See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=204560
Remote BCC does not display correct information on 'Control Centers' about the newly added Remote BCC.	When policy sharing is being configured and a new remote Control Center is added, this remote Control Center does not display the correct information. The central Control Center always displays the correct information. This issue will resolve when the incorrectly displayed policies are either modified or re-applied from the central Control Center. See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=204329
Custom time range fields on message audit logs are misaligned on Chrome.	Some versions of Chrome incorrectly display the input form for Message Audit Log time range fields. These fields are still functional, although they are misaligned. See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=204565
MAN page for CLI command `tcpdump` is incorrect. The current system default page is displayed, which does not contain SMG-specific information.	The CLI commands `help tcpdump` and `tcpdump -help` both display incorrect information. Rather than displaying the appropriate SMG-related content, they display the system default page. Mitigation: view the `tcpdump` page in the online web help or in the Command Reference. See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=204566
Content filtering policy does not detect images within RTF attachments.	Embedded images in RTF file attachments are not extracted correctly. As a result, content filtering policies that are intended to detect images are not triggered. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH208718
The Message Audit Log does not log the offending IP for IP-related verdicts.	SMG reports the connecting IP addresses and logical IP addresses. Local Bad Senders may also reject a message based on other IP addresses that SMG finds in the message headers. If this rejection occurs, that IP address is not reported. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH232769
The Control Center allows active sessions for administrators with deleted accounts.	When administrators log on, their permissions are cached. They continue with the same rights until they log out. Also, administrators with full rights to the Control Center can delete their own accounts without receiving a warning. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH208723

Issue	Description
The **Administration > Host Version > Updates** page may display an inaccurate status for a specific host and the update process.	Several update issues involve differences between the true status of the update and the status displayed in the Control Center. Viewing the update.log from the command line always provides accurate information. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH210607
Audit log policy names do not match policy actions.	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH232772
The error "server refused the connection" appears in the `catalina.out` log file during update.	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH232860
Restoring a policy-only backup may result in an incorrect administrator policy group member count.	An incorrect member count only occurs with the policy backup and restore function. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH232870
Scheduled reports are displayed in English even when "Report in Traditional Chinese (Big 5) Language" is selected.	No method is available to select the desired language or the character set for a scheduled report. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH232877
The action 'Strip all attachments' does not remove attached email messages even if they are named.	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH232882
CSV-exported report for Unscannable - Summary does not have the Group by Hour data.	WORKAROUND: Use the HTML format, open it in Excel and use the table. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH234539
You cannot search the Message Audit Log for DKIM, DMARC, SPF, or SenderID results from the Control Center.	WORKAROUND: You can search the Message Audit Log from the command line or by Content Filter verdict. See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=171252
If message headers, or the DMARC DNS record, cannot be correctly parsed, the DMARC validation status for a message is 'none' instead of an error.	See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=172109
The **Bypass Disarm** verdict shows up in the log as 'bypasspmc'.	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH250997
During a Hyper-V install, the error "`mounting /sys filesystem`" appears.	You can ignore the error "`mounting /sys filesystem`" during Hyper-V installation. See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=172113
When a remote scanner is not connected, configuration changes to DMARC settings may not be saved to other scanners. This applies to the Control Center computer if it contains a scanner.	WORKAROUND: Make sure that remote scanners are live before you make configuration changes. See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=203887
Content filtering conditions for file names matching a Dictionary entry with left square bracket do not return a match.	See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=172158
A domain with a wildcard in the **Bad Senders** list does not block mail from matching domains.	Wildcards in the **Bad Senders** list only work in a full email address. WORKAROUND: Manually prepend '*@' to the rules in question. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH254204

Issue	Description
Unable to edit assigned policy groups for the **Failed Bounce Attack Validation** policy on the **Edit Email Spam Policy** page.	WORKAROUND: Assign policies on the **Edit Policy Group** page under the Administration tab. See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=204194
The dashboard displays "All scanners accessible" when some scanners are not accessible.	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH254209
A spreadsheet that is embedded in a Word document is not detected as a spreadsheet document.	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH254213
Warnings and Errors appear in the update.log during an update from SMG 10.6.6 to 10.7.x.	You can safely ignore a number of Warnings and Errors in the update.log. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH254217
Configuration file system unmounting failures appear during system restart.	You can safely ignore the following "FAILED" messages during SMG system restart: • `[FAILED] Failed unmounting Configuration File System.` • `[FAILED] Failed unmounting /data.` See the associated knowledge base article for details: http://www.symantec.com/docs/TECH254244
The following error may appear during upgrade from 10.6.6: `[ERROR] mysqld: Table './brightmail/xxxxxxxx' is marked as crashed and should be repaired"`	You can safely ignore the error message. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH254245
Although **Unscannable/Malformed MIME** and **Unscannable/Mismatched filetype** are no longer supported verdicts, the Control Center's Message Audit Log continues to show them as optional filter values for **Verdict**.	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH256796
During the update from 10.6.6 to 10.7, the **Software Update Status** page displays some actions twice.	Some update actions occur twice during update because SMG 10.7 includes a full operating system update. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH254246
If the user enables TLS using a certificate request without importing the certificate, the MTA does not start.	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH256797
New "fatal" log event seen in update.log and warning in messages during software update from 10.6.6.	These messages can safely be ignored. See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=203871
If the username or password for the LiveUpdate server or proxy contains the '/' character, LiveUpdate will not work.	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH256799
SMG 10.7 detects Microsoft document file internals as various True Type executables, differing in behavior from default 10.6 and previous releases.	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH256800
On all hardware platforms other than 8380-S450, the Control Center shows a RAID error when the RAID controller is actually having no issues when (SNMPV3-only + MD5) is configured.	See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=175448

Issue	Description

Errors in /data/logs/messages are displayed during install of 10.7.2 on the S450 hardware.	Errors displayed:
	`2019 Jul 10 15:53:14 (err) systemd-udevd: [-]could not find module by name='ipmi_si'`
	`2019 Jul 10 15:53:14 (err) systemd-udevd: [-]could not find module by name='ipmi_devintf'`
	`2019 Jul 10 15:53:14 (err) systemd-udevd: [-]could not find module by name='ipmi_msghandler'`
	`2019 Jul 10 15:53:56 (err) systemd: [-]Failed to start SYSV: Symantec Messaging Gateway Control Center.`
	`2019 Jul 10 15:53:21 (err) kernel: [-]megaraid_sas 0000:5e:00.0: Init cmd return status SUCCESS for SCSI host 0`
	These messages can safely be ignored.
	See the associated knowledge base article for details:
	https://knowledge.broadcom.com/external/article?articleId=176327

Password-protected PDF files are now being treated as encrypted attachments.	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH256802
Scheduled reports are generated and delivered in English rather than in the language specified for **Favorite** reports.	PARTIAL WORKAROUND: ad hoc reports forwarded to an email address are in the expected language. Re-run **Favorites** as ad hoc reports and forward them to generate reports in the expected language. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH256803
After a fresh install of 10.7.3, the dashboard displays the word "unlicensed," which is not correct. The **License** page shows the valid license after approximately five minutes.	WORKAROUND: wait approximately five minutes after completing the installation before attempting to log in. The **License** page displays correctly after that time interval. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH256804
The download of diagnostics to the desktop fails with no error if the diagnostics download exceeds 2 GB.	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH256805
After adding a virtual IP address, the following error message appears in /data/logs/messages: `2019 Sep 30 11:42:41 (err) snmpd: [15623] Duplicate IPv4 address detected, some interfaces may not be visible in IP-MIB" if a second ip is added either virtual or eth1.`	This issue first appeared in the version of `snmpd` that was introduced in SMG 10.7. If the system does not actually have a duplicate IP address, you can safely ignore this message. See the associated knowledge base article for details: https://knowledge.broadcom.com/external/article?articleId=176332

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/10-7-4.html

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

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


Symantec
A Division of Broadcom