Symantec™ Messaging Gateway 10.5.3 Release Notes

powered by Brightmail™

Symantec Messaging Gateway 10.5.3 Release Notes

This document includes the following topics:

About Symantec Messaging Gateway 10.5.3

Symantec Messaging Gateway 10.5.3 is the upgrade to previous versions of Symantec Messaging Gateway. All functionality of Symantec Messaging Gateway 10.5.2 is maintained unless otherwise noted.

Note: You must be at Symantec Messaging Gateway 10.5.1 or later in order to update to Symantec Messaging Gateway 10.5.3. You can only update to version 10.5.1 from version 10.0.3 or later.

What's new

This release of Symantec Messaging Gateway fixes known defects and addresses known vulnerabilities, and also includes the following new and enhanced features:

- This version requires your browser to use TLS 1.2 when you access the Control Center.
- You can import and export RSA tokens to enable automated tasks without storing passwords in configuration files or scripts.
- You can change the size for individual lines in a remote syslog from the default of 1K to 4k.
- The Message Audit Log now records that a message is received through TLS.
- Language Identification scanning is now skipped only if the body of the message is over 100K.
- Incoming TLS connections now support PFS (Perfect Forward Secrecy).

Documentation

You can access English documentation at the following website:

http://www.symantec.com/business/support/index?page=content&key=53991&channel=DOCUMENTATION&sort=recent

The site provides best practices, troubleshooting information, and other resources for Symantec Messaging Gateway.

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

http://www.symantec.com/docs/TECH223626

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 Symantec Messaging Gateway, see the following links:

http://go.symantec.com/security_appliance_support

http://go.symantec.com/appliance_hw_support

To read the translated 10.5 documentation, go to the following URLs, and then click the **Documentation** link:

Chinese (Simplified)

http://www.symantec.com/business/support/index?page=landing&key=53991&locale=zh_CN

Chinese (Traditional)

http://www.symantec.com/business/support/index?page=landing&key=53991&locale=zh_TW

Japanese

http://www.symantec.com/business/support/index?page=landing&key=53991&locale=ja_JP

Korean

http://www.symantec.com/business/support/index?page=landing&key=53991&locale=ko_KR

You can access English documentation at the following website:

http://www.symantec.com/business/support/index?page=content&key=53991&channel=DOCUMENTATION&sort=recent

The site provides best practices, troubleshooting information, and other resources for Symantec Messaging Gateway.

Support policy

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

For more information about Symantec's support policies, go to the following URL:

http://go.symantec.com/security_appliance_support

Supported platforms

You can update to Symantec Messaging Gateway 10.5.3 on any of the following platforms:

- All supported hardware versions: 8380 purchased after March 2009, 8360 purchased after March 2009, and 8340 purchased after September 2010
- VMware ESXi/vSphere 5.0/5.1/5.5
- Microsoft Hyper-V: Windows Server 2008 and Hyper-V Server 2008, Windows Server 2012 and Hyper-V Server 2012
- For more information about Symantec Messaging Gateway hardware testing support, go to the following URL:
  http://www.symantec.com/docs/TECH123135

Unsupported platforms

Unsupported platforms are as follows:

- Any virtual platform that is not listed in the Supported Platforms section of this document.
- Hardware platforms 8220, 8240, 8260, 8320, and 8340 (PowerEdge 860 and R200 versions) purchased on or before September 2010
- Hardware platforms 8360 (PowerEdge 1950 versions 1 and 2) and 8380 (PowerEdge 2950 versions 1 and 2) purchased on or before March 2009.

For more information about Symantec Messaging Gateway hardware testing support, 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 Symantec Messaging Gateway Control Center on any of the following supported web browsers:

- Internet Explorer 8 or later. See the associated knowledge base article for details about using IE8.
  http://www.symantec.com/docs/TECH215638
- Firefox 28 or later
- Chrome 34 or later

Supported paths to version 10.5.3

You can update to Symantec Messaging Gateway 10.5.3 by using any of the following methods:

- Software update from version 10.5.1 or later on supported hardware or in supported virtual environments
- OSRestore from ISO on supported hardware or in supported virtual environments
- VMware installation with OVF file

Unsupported paths to version 10.5.3

You cannot update to Symantec Messaging Gateway 10.5.3 by using any of the following methods:

- Versions earlier than 10.5.1
- Direct upgrade from beta versions

Important information about installation in virtual environments

Symantec Messaging Gateway 10.5 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 5.0/5.1/5.5.
OVF template	You can also load the OVF, which includes the virtual machine configuration. You can use the OVF for VMware ESXi/vSphere 5.0/5.1/5.5.

To install on Hyper-V

There is 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 2008 and Hyper-V Server 2008, Windows Server 2012 and Hyper-V Server 2012.

See the *Symantec Messaging Gateway 10.5 Installation Guide* for instructions and system requirements.

Note: In a virtual environment, verify that your virtual environment can support 64-bit virtualization before you update to Symantec Messaging Gateway 10.5. When Intel Virtualization Technology (also known as Intel-VT) is enabled in the BIOS, it allows the CPU to support multiple operating systems, including 64-bit architecture. On many Intel processors this setting may be disabled in the BIOS and must be enabled prior to installing Symantec Messaging Gateway 10.5. AMD processors that support 64-bit architecture usually have this setting enabled by default. See KB 1003945 from VMware for more information:

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1003945

Important information before you update to version 10.5.3

This topic contains the migration information that you should read before you update to version 10.5.3. You must update to Symantec Messaging Gateway 10.5.3 from Symantec Messaging Gateway 10.5.1 or later.

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 1-1 describes suggested best practices that you should consider when you upgrade from any version.

Table 1-1 Best practices for all upgrades

Item	Description
Perform a backup.	Symantec strongly recommends that you take a full system backup before you run the software update and store it off-box.

Table 1-1 Best practices for all upgrades *(continued)*

Item	Description
Do not restart.	The software update process may take several hours to complete. 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.
Stop mail flow to Scanners and flush queues before you update.	To reduce Scanner update time and complexity, you should stop mail flow to Scanners and drain all queues. 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**. 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 strongly recommends that you update your Control Center before you update your Scanners to the matching version. If you do not update the Control Center first, Symantec recommends that you use the command line interface to update remote Scanners. It is crucial that the time frame in which you update your Scanners to 10.5 is kept as short as possible: the Control Center is unable to propagate configuration changes to Scanners that are on different versions. Configurations in which the Control Center and Scanners run different versions for an extended period are unsupported.
Perform software update at off-peak hours.	The Control Center appliance is offline and unusable during the update process. Scanners cannot quarantine messages on the Control Center during the software update, so messages build up in a queue. Updating a Control Center appliance can take quite some time. Plan to update the Control Center appliance during off-peak hours. When you migrate a Scanner, it goes offline. Scanner resources are unavailable during the migration process. Software update of a Scanner takes less time than the software update of the Control Center.

Resolved issues

This section describes the issues that are resolved in 10.5.3.

Table 1-2 Resolved issues

Issue	Description and knowledge base article link (if applicable)
In previous releases if you enabled **Remove subaddress in recipient validation directory query**, both "+" and "-" were used to delimit the subaddress.	Only the minus sign is used to delimit the subaddress. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH163815
Language identification scanning did not occur if a message as a whole was over 100 KB.	The language identification scanning is now skipped only if the body of the message is over 100K. http://www.symantec.com/docs/TECH167825
The Message Audit Log didn't update the status for the messages that were deleted due to a verdict of ***virus/worm/unscannable***. It showed the status as "Processing Status".	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH211478
Unchecking **Enable scanning of non-plain text attachments for words in dictionaries** also prevents scanning of plain text attachments.	The UI is now consistent with the product behavior. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH216384
In some cases, Message Audit logs did not show the authenticated user name when SMTP authentication was used.	The Message Audit logs now show authenticated user name when SMTP authentication is used. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH225281
In some cases, Microsoft Office 2007-formatted document incorrectly triggered a Content Policy based on the attachment size.	This issue is now resolved. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH216386
Selecting the timezone "(GMT-04:00) Atlantic Time (Canada)" resulted in **timezone** being set to "(GMT-05:00) Eastern Time (US & Canada)".	This fix is not an automatic change. Reset the timezone manually. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH215942
In some cases, after **submission details** was selected for a rejected submission, the browser hung.	When you view the raw message for a rejected message (e.g. invalid format), it now behaves as expected and displays the raw message data. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH225282

Table 1-2 Resolved issues *(continued)*

Issue	Description and knowledge base article link (if applicable)
"Message was sent by a suspected spammer" appeared in the Message Audit Log under untested verdicts for all messages.	The verdict "Message was sent by a suspected spammer" has been deprecated. Symantec no longer tests for this condition. All references to it have been removed. See the associated knowledge base article for details:http://www.symantec.com/docs/TECH225284
Under **Spam Quarantine Settings**, the spam notification URL automatically included **/brightmail**.	Customers can modify any part of the spam notification URL and retain the original functionality. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH225285
In some cases, the content filtering process failed to detect the Dictionary words that were enclosed in quotes.	Content filtering now detects the Dictionary words that are enclosed in quotes. See the associated knowledge base article for details:http://www.symantec.com/docs/TECH225286
The GMT timezone option was only available in the Control Center.	The **GMT:Greenwich Mean Time timezone** option can now be selected during the install process in both the CLI and the Control Center. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH225308
When SNMP was not enabled, the snmpd process used the UDP protocol to listen on port 161, and the TCP protocol to listen on port 199 on all interfaces.	The snmpd process no longer listens on either port on an externally accessible interface when SNMP is disabled. See the associated knowledge base article for details:http://www.symantec.com/docs/TECH225309
The Message Audit Log Message Detail page and the Quarantine Message Detail pages cut off the bottom portion of the screen, obscuring some display fields.	Both pages now display all details and fields as expected. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH225311
Enabling FIPS while configuring SSH to disable CBC ciphers caused the SSH daemon to stop responding.	All combinations of FIPS mode and CBC on/off will appropriately configure SSH such that it functions as expected. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH225076

Table 1-2 Resolved issues *(continued)*

Issue	Description and knowledge base article link (if applicable)
Incoming TLS connections did not support PFS (Perfect Forward Secrecy).	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH225317
In some cases, when Marketing, Newsletter, or Suspicious URL policies were enabled, they did not trigger as expected.	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH225279

Known issues

This section describes the known issues in version 10.5.3.

Table 1-3 Known issues

Issue	Description
Split .zip file detection is not consistent.	When a .zip file is split into several parts and sent one part per message, Symantec Messaging Gateway does not consistently detect all file parts. Other compressed files, such as RAR files, that are similarly divided, are scanned properly. Not all such messages are considered unscannable, as would be expected. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH176884
Replies to messages that are sent through the Symantec Content Encryption service always fail Bounce Attack Validation.	When Symantec Content Encryption and Symantec Bounce Attack Validation are used together, replies to encrypted messages that are sent from the content encryption web portal are flagged as invalid bounce messages and rejected. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH174807

Table 1-3 Known issues *(continued)*

Issue	Description
Content Filtering policy does not detect images within RTF attachments.	Embedded images in RTF file attachments are not extracted correctly, so 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 *Symantec Messaging Gateway Installation Guide* incorrectly states that inbound local delivery is limited to three servers, while the *Symantec Messaging Gateway Administration Guide* states correctly that local delivery is unlimited.	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH193367
In the Control Center online Help and in the *Symantec Messaging Gateway Administration Guide*, the list of supported MUAs is incorrect.	The topic "About using SMTP authentication" lists the MUA versions that Symantec Messaging Gateway has been tested against. This list should include Microsoft Outlook 2010, but it should not include Thunderbird 2 or Mail.app on MacOS. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH211461
Messages cannot be submitted for Customer-Specific Spam Rules through the Control Center when they have lines over 998 characters long .	Non-RFC5322-compliant messages cannot be submitted for Customer-Specific Spam Rules even though the messages are delivered to user inboxes without issue. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH205682
The Control Center allows active sessions for administrators with deleted accounts.	When administrators log in, 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

Table 1-3 Known issues *(continued)*

Issue	Description
TLS to FIPS-enabled DLP Prevent Server Version 12 fails negotiation.	With any TLS setting enabled for a FIPS-enabled DLP appliance, messages that are sent to DLP in Reflect mode get stuck in the Delivery queue due to a failed TLS negotiation. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH212117
Microsoft Office 2007 documents with files embedded using the 'Link to file' option trigger the "unscannable due to limits exceeded" policy.	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH216390
When Disarm removes Flash from PowerPoint, Flash is not replaced with a white image in a multilevel embedded attachment.	When Disarm removes Flash content from Microsoft PowerPoint documents, Flash content that is contained in a multilevel embedded attachment is not replaced with a white image as expected. Instead, the first image in the Flash content is displayed. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH211474
Selecting "Enable HTML text scanning" in a Content Filter rule only applies to the message body, not to the message's attachments.	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH211464
When you enable **Sender ID/SPF**, the checking of SPF TXT records returned by DNS is case-sensitive for keywords such as "a", "mx", and "ip".	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH208735
Errors are displayed in the MTA Log (maillog).	The errors `heartbeat_init -> gimli_heartbeat_attach` and `heartbeat_init ->Default` appear at startup, and can be safely ignored. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH216379

Table 1-3 Known issues *(continued)*

Issue	Description
Stopping and starting the Brightmail Engine (or MTA) from the Control Center does not restart Disarm.	The Disarm service cannot be started or stopped from the Control Center. Starting or stopping Disarm can only be done from the Command Line Interface, using the `service mta` commands. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH216412
Unsaved changes to quarantine settings are lost when you edit the notification template.	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH211466
Misleading error messages may appear in the Disarm logs.	Disarm logs can display the error `CReconstructor::LogStats: cannot create directory for '$filename' with error:File exists`. This error can be safely ignored. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH211467
In the Control Center, on the **Administration > Host Version > Updates** page, the status displayed for a specific host may not accurately reflect the actual status of the host or of the update process.	There are several update issues that all involve differences between the true status of the update and its status as displayed in the Control Center. Viewing the update.log from the Command Line Interface will always provide accurate information. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH210607
Release and view links are not visible when spam summary messages are viewed as text-only.	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH211468
The `cc-config` entry in the *Command Line Reference* and man page does not include information about the `limit-tlsv1.1` option.	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH211470
Documentation incorrectly states that file attachment size limits considers only the compressed size of compressed attachments.	The uncompressed size of attachments is always used when testing file size. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH216385

Table 1-3 Known issues *(continued)*

Issue	Description
The *Symantec Messaging Gateway Installation Guide* omits AD 2012 from list of supported directory servers.	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH225349
In the 10.5.1 *Symantec Messaging Gateway Administration Guide*, on page 774, the command used to clear a hostname entered in error is misidentifies. It says to use `clear bcchostacl` instead of `delete bcchostacl`.	In the 10.5.1 *Symantec Messaging Gateway Administration Guide*, the note section on page 774 should read: Note: If you make an error when you type the host name, you block all access to the Control Center. If this situation occurs, use the command `delete bcchostacl` from the command line to clear the list of computers that are permitted to access the Control Center. See delete on page 855.
Symantec Messaging Gateway may be unable to deliver mail if TLS delivery is being attempted and the the receiving MTA strictly implements TLSv1.	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH215003
Symantec Messaging Gateway may fail to process certain messages with badly formatted MIME attachment headers.	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH216389
If both inbound and outbound mail is received on the same IP address and port, mail from an IP address with a broken PTR record will be deferred.	If inbound and outbound mail is received on different interfaces or ports, this problem will not occur. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH211480
The Symantec Messaging Gateway reaches out to https://tmsg.symantec.com/ to report telemetry. This site is not documented in our list of accessed web sites.	This is expected behavior in versions 10.5 and later. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH216382

Table 1-3 Known issues *(continued)*

Issue	Description
Multiple certificates using the same private key are not allowed on the Symantec Messaging Gateway.	When you import two certificates that have the same private key into the Symantec Messaging Gateway, the second certificate overwrites the first certificate. There is no warning when you are about to overwrite a certificate, just a confirmation message that the certificate was updated. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH218025
When you create a custom date and timestamp format, you may encounter unexpected results.	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH208718
Some messages held in the Quarantine folder may not display correctly when selected.	Some very short messsages in non-US ASCII char sets may not display correctly when using Auto-Detect or Auto Chinese. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH225315
Symantec Messaging Gateway may be unable to deliver mail if TLS delivery is being attempted,when domains are unable to negotiate an acceptable cipher.	When domains are unable to negotiate an acceptable cipher, they bounce a message instead of delivering it without TLS. To deliver messages in this circumstance, disable opportunistic TLS. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH225316