Symantec™ Messaging Gateway 10.6.2 Release Notes

powered by Brightmail™

Symantec.cloud

Symantec™ Messaging Gateway 10.6.2 Release Notes

Documentation version: 10.6.2

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information

- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

support.symantec.com

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apj@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Symantec Messaging Gateway 10.6.2 Release Notes

This document includes the following topics:

About Symantec Messaging Gateway 10.6.2

Symantec Messaging Gateway (SMG) 10.6.2 is the upgrade to previous versions of SMG. All functionality of SMG 10.6 is maintained unless otherwise noted.

Starting with the SMG 10.5.4 release, this product supports the Symantec SHA-2 transition program. (See http://www.symantec.com/docs/ALERT1868 for more information.)

Note: You must be at SMG 10.5.4 or later to update to SMG 10.6.2. You must upgrade to version 10.5.4 or later by June, 2016. Failure to do so may result in your system's inability to retrieve software updates and filter updates.

What's new in SMG 10.6.2

Symantec recommends that all customers using version 10.6 of the SMG software update at their earliest convenience.

New features include the following:

- The ability to disable clickable URLs in messages.
- Previously, the MTA would immediately retry the first message in the queue for each domain when it was restarted. In this version, the MTA waits for the completion of the retry interval before it attempts delivery again.

This release also fixes known defects and addresses known vulnerabilities.

Documentation

You can access English documentation at the following website:

https://support.symantec.com/en_US/messaging-gateway.html

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

http://www.symantec.com/docs/INFO3863

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 10.6 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

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 SMG 10.6.2 on any of the following platforms:

- All supported hardware versions: 8380 purchased after March 2010, 8360 purchased after March 2010, and 8340 purchased after September 2010
- VMware ESXi/vSphere 5.0/5.1/5.5/6.0
- Microsoft Hyper-V: Windows Server 2008 and Hyper-V Server 2008 including sub-releases, Windows Server 2012, and Hyper-V Server 2012 including sub-releases
- For more information about SMG hardware testing support, go to the following URL:
  http://www.symantec.com/docs/TECH123135

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, and 8340 (PowerEdge 860, R200, and R210 versions) purchased on or before June 2011.
- 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 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 SMG Control Center on the following supported web browsers:

- Internet Explorer 9 or later.
- Firefox 40 or later
- Chrome 50 or later

Supported paths to version 10.6.2

You can update to SMG 10.6.2 by using any of the following methods:

- Software update from version 10.5.4 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
  Note: Symantec provides an OVF template which can load a virtual machine running SMG into VMware. This template, is designed for demonstration or testing purposes and not for deployment in a production environment unless explicitly recommended. For any production environment, Symantec recommends that you create a virtual machine in accordance with best practices as outlined in the *Symantec™ Messaging Gateway 10.6 Getting Started Guide*. Then install SMG using the ISO file.

Unsupported paths to version 10.6.2

You cannot update to SMG 10.6.2 by using any of the following methods:

- From versions earlier than 10.5.4
- Direct upgrade from beta versions

Important information about installation in virtual environments

SMG 10.6.2 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 5.0/5.1/5.5/6.0.
OVF template	You can also load the OVF, which includes the virtual machine configuration. You can use the OVF for VMware ESXi/vSphere 5.0/5.1/5.5/6.0.

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 10.6 Getting Started Guide* for instructions and system requirements.

Important information before you update to version 10.6.2

This topic contains the migration information that you should read before you update to version SMG 10.6.2. You must update to SMG 10.6.2 from SMG 10.5.4 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 Best practices for all upgrades

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. 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. The system restarts automatically when the upgrade completes.
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 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. Keep the time frame in which you update your Scanners as short as possible. The Control Center is unable to propagate configuration changes to Scanners that are not on the same version of the software. 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 SMG 10.6.2.

Table 1-2 Resolved issues

Issue	Description and knowledge base article link (if applicable)
The sensor for the CPU temperature status erroneously returned "Not Available" for some 8340s.	CPU temperature is now accurately reported. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH233695
Disabling SSLv3 in all SMTP conversations did not prevent RC4 ciphers from being used.	Enabling FIPS mode resolved the issue. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH234747
On some 8340s a fan status error appeared.	The fan status now displays correctly. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH234974
Control Center was unable to send updated configuration files to scanners if the configuration file is over 7MB.	This issue has been resolved. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH234968
SSH weak MAC algorithms were enabled in SMG.	The administrator can now disable SSH weak MAC algorithms. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH235646
A message had both "strip all attachments" and "strip and delay in suspect virus quarantine" actions. When the message was released from quarantine, all attachments were present.	This issue has been resolved.

Table 1-2 Resolved issues *(continued)*

Issue	Description and knowledge base article link (if applicable)
Replies to messages that were sent through the Symantec Content Encryption service failed Bounce Attack Validation.	This issue has been resolved. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH174807
In some cases, the error "CReconstructor::LogStats: cannot create directory for Symantec Messaging Gateway$filenameSymantec Messaging Gateway with error:File exists." erroneously appeared in the Disarm log.	This issue has been resolved. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH211467
SMG did not support Elliptic Curve Cyphers.	This implementation now supports EECDH cyphers. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH232774
Addresses that were aliases with a subaddress failed recipient validation.	This issue has been resolved. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH228278
Symantec Messaging Gateway closed the network connection prematurely when it delivered messages.	This issue has been resolved. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH230314
Message Audit Log truncated the subject line on Russian emails, and showed different characters.	This issue has been resolved. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH232869

Table 1-2 Resolved issues *(continued)*

Issue	Description and knowledge base article link (if applicable)
Messages were rejected when LDAP server was offline.	Currently messages are deferred when LDAP is off line. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH233872
When the user added UTF-16 text to a content filtering Dictionary, content filtering rules silently failed.	Under these conditions, the following error appears in the Brightmail Engine log: Gatekeeper module: Error in rule file, line number 44: Cannot parse: "<unreadable>". See the associated knowledge base article for details: http://www.symantec.com/docs/TECH235657
Changes made to remote logging levels were not propagated until the system was restarted.	This issue has been resolved. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH233111
Messages with double-byte characters in the subject line did not create an informational incident.	This issue has been resolved.
A user was unable to copy a favorite report with a name longer than 254 characters.	A favorite report with a name longer than 254 characters can now be copied. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH234530
"DNS resolution failure: <domain> 4" appeared in MTA log at inappropriate level.	This issue has been resolved. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH233694

Table 1-2 Resolved issues *(continued)*

Issue	Description and knowledge base article link (if applicable)
In some cases, files within winmail.dat went undetected by content filtering policies.	Files within winmail.dat are now detected based on the file extension. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH235659
Conduit got stuck on an old submission ruleset.	This issue has been resolved. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH234536
The Received header inserted by SMG omitted the hostname.	The Received header inserted by SMG no longer omits the SMG hostname. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH233823
In some cases, SMG was unable to deliver mail if configured to attempt TLS delivery, and was unable to negotiate an acceptable cipher.	These issues have been resolved. See the associated knowledge base articles for details: http://www.symantec.com/docs/TECH233871 http://www.symantec.com/docs/TECH233869
Sending Brightmail admin events to remote syslog were not enabled when a Control Center-only appliance was used.	This issue has been resolved. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH233957
Control Center did not process new statistics due to a missing stats file.	The Control Center now reports an error and continues to process statistics. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH235658

Table 1-2 Resolved issues *(continued)*

Issue	Description and knowledge base article link (if applicable)
DNS latency detection/protection resulted in large numbers of ERROR level messages in the Brightmail Engine logs.	DNS latency detection/protection now stops trying for 5 minutes after 20 or fewer errors. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH234173
In some cases, a Dictionary rule does not catch a non-US ASCII word in the subject.	Dictionary rules now catch non-US ASCII words in the subject. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH234540
Some messages were garbled in the body of the message after they were processed through the SMG.	This issue has been resolved. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH234596
Attempts to modify DDS sources failed with an invalid credentials error and/or information was not saved.	Configuration updates are now successful and information is saved as expected. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH234776
Network connection errors appear in conduit_log during installation.	These errors can be safely ignored. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH234529
Recipient Validation incorrectly rejected Recipients with a BATV tag.	Recipient validation is now performed correctly for recipients with the BATV tag. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH235317

Table 1-2 Resolved issues *(continued)*

Issue	Description and knowledge base article link (if applicable)
In some cases, setting the logging level in Disarm at INFO or DEBUG caused repeated msserver crashes.	The msserver process which handles Disarm operations exceeded the maximum allowed file size limit for the log file. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH233477

Known issues

This section describes the known issues in SMG 10.6.2.

Table 1-3 Known issues

Issue	Description
In some environments, switching between pages and/or saving a change to the **Protocols> Domains** page can take a long time.	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH229166
Fastpass can be granted to sender IPs that are on the **Bad Sender IP** list if clean messages are scanned from the **Bad Sender IP**.	WORKAROUND: To prevent the potential of scanning crafted clean messages from **Bad Sender IP**, configure actions to reject (the default setting) or defer the SMTP connection. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH208717
Simplified Chinese GB2312 characters in a disclaimer cause the original email to arrive as an attachment with the disclaimer in the body of the email.	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH235660

Table 1-3 Known issues *(continued)*

Issue	Description
SMG uses the Primary email attribute to store emails in Spam Quarantine.	WORKAROUND: Add email addresses to the admin accounts. They do not have to be valid email addresses. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH235661
The subject line is corrupted when messages are sent to Spam Quarantine.	WORKAROUND: Change the encoding to the appropriate language setting. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH235662
In some cases the administrator receives an alert saying that the bmserver crashed on signal 11 exit code: 0x008B.	A binary attachment is mistakenly interpreted as a MIME object and crashes the mime engine. WORKAROUND: Go to **Protocols >Settings >Content Scanning >Advanced**, and uncheck 'MIME fuzzy main header'. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH235663
End-user Spam Quarantine does not show full subject lines in a tool tip.	The administrator access to the Spam Quarantine displays a mouseover tool tip with the full subject. For end-users the tool tip is not displayed. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH235411
The Scanner does not reatattach saved Outlook messages as possible containers.	WORKAROUND: Go to **Protocols >Settings > Content Scanning >Advanced** and uncheck "Extract OLE 1.0 native only". See the associated knowledge base article for details: http://www.symantec.com/docs/TECH235664
Content filter rules do not recognize words containing "ó" (the Polish "u").	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH235665

Table 1-3 Known issues *(continued)*

Issue	Description
The time used for the America/Santiago time zone is off by 1 hour.	When the timezone in the Control Center **Administration->Configuration->host->DNS/Time** is configured to use the America/Santiago, TZ shows "GMT-4:00". However, the timezone offset used by the system and logging is "GMT-3:00". This results in the displayed timestamp being 1 hour off from the expected time. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH235409
Office 365 rejects DSNs generated by Content Filtering actions.	WORKAROUND: Create a notification template to mimic a delivery status notification by **Content->Notifications** and set the action to "Send Notification". See the associated knowledge base article for details: http://www.symantec.com/docs/TECH235330
The error message "Failed to load hid_base_hv kernel module" appeared during install of SMG 10.6. in a Hyper-V environment.	This error message can be ignored. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH235666
Split .zip file detection is not consistent.	When a .zip file is split into several parts and sent one part per message, SMG 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

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 MAL does not log the offending IP for IP-related verdicts.	SMG reports the IP that is available at the time of connection. SMG does not differentiate between logical and connecting IP, if it is out side of internal range. 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
Microsoft Office 2007 documents with files embedded using the Symantec Messaging GatewayLink to fileSymantec Messaging Gateway 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.	In a multilevel embedded Microsoft PowerPoint document, Disarm replaces the Flash content with the first image in the Flash content, not with a white image as expected. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH211474

Table 1-3 Known issues *(continued)*

Issue	Description
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
On the **Administration > Host Version > Updates** page, the status that is displayed for a specific host may not accurately reflect the actual status of the host or of the update process.	Several update issues 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 always provides accurate information. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH210607
Documentation incorrectly states that file attachment size limits consider only the compressed size of compressed attachments.	The uncompressed size of attachments is always used to test file size. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH216385
If both inbound mail and outbound mail is received on the same IP address and port, mail from an IP address with a broken PTR record is deferred.	If inbound and outbound mail is received on different interfaces or ports, this problem does not occur. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH211480
Audit log verdict descriptions do not match policy actions.	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH232772
Content Filtering does not recognize AutoCAD 2013 files.	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH229169
MAL shows status as "Processing Status" for rejected messages.	As a workaround, leave all non-applicable fields blank. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH232858

Table 1-3 Known issues *(continued)*

Issue	Description
"server refused to connection" error appeared in the catalina.out log file during update.	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH232860
Visio Diagrams (.vsdx files) are identified as Archive/ZIP files instead of as Microsoft Office Documents.	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH232865
Restoring a policy only backup may result in an incorrect admin policy group member count.	This only occurs with the policy backup / restore. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH232870
Empty-body messages that are signed using the DKIM relaxed algorithm fail verification.	Empty-body messages that are signed using the DKIM simple algorithm are verified as expected. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH232872
On some platforms, the SNMP Disk Usage query results in an error.	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH232874
Scheduled reports display in English even when "Report in Traditional Chinese (Big 5) Language" is selected.	There is no method of selecting the desired language or charset for a scheduled report. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH232877
An error appeared in MTA log: setting dns backend to Symantec Messaging GatewayaresSymantec Messaging Gateway.	This is not an error. The system is reporting the value of the setting. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH232880
Content Filter does not strip an attached .eml file.	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH232882

Table 1-3 Known issues *(continued)*

Issue	Description
During update, "HTTP-Status 500-XML Parsing Error"is displayed on UI and errors show in catalina.out.	See the associated knowledge base article for details: http://www.symantec.com/docs/TECH233000
Online Help inaccurately mentions maximum allowed NTP servers as three.	You can specify up to 5 Network Time Protocol (NTP) time servers. Use of NTP to manage time is recommended. You also have the option to set the time manually. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH234532
The description for mta-control Symantec Messaging Gateways Symantec Messaging Gateway num-msgs-by-rcpt-all-routesSymantec Messaging Gateway argument is incorrect in all documentation.	The correct description for mta-controlSymantec Messaging Gateways Symantec Messaging Gatewaynum-msgs-by-rcpt-all-routesSymantec Messaging Gateway argument is as follows: num-msgs-by-rcpt <route> – Print the number of messages for each recipient domain on a given route num-msgs-by-rcpt-all-routes – Print the number of messages for each recipient domain on all routes See the associated knowledge base article for details: http://www.symantec.com/docs/TECH234533
In some cases, the Message Audit Log shows a malformed subject line.	Malformed subject lines occur when the subject contains encoded entity reference format. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH234535
SMG documentation for 10.6 says that we only support vmxnet1/2, but does not mention support for vmxnet3.	In 10.6, support for vmxnet3 was introduced and is the recommended adapter for VMware. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH234537

Table 1-3 Known issues *(continued)*

Issue	Description
Footer hides the attachment name when the message body is long, and scrolling is necessary to get to the bottom.	WORKAROUND: Use the zooming feature of the web browser and render the page in 85% or less. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH234538
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
Matching attachment only detects the first file in a password-protected ZIP.	Scanning the zip file contents stops when the zip file is found to be encrypted. See the associated knowledge base article for details: http://www.symantec.com/docs/TECH234541

Where to get more information

You can access English documentation at the following website:

https://support.symantec.com/en_US/messaging-gateway.html

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

http://www.symantec.com/docs/INFO3863