Symantec™ Messaging Gateway 9.5.1 Release Notes

powered by Brightmail™

Symantec Messaging Gateway 9.5.1 release notes

This document includes the following topics:

About Symantec Messaging Gateway 9.5 and 9.5.1

Symantec Messaging Gateway 9.5 is the upgrade to previous versions of Symantec Brightmail Gateway and Symantec Mail Security 8300 Series Appliance Software. Symantec Messaging Gateway 9.5.1 is the localized version of 9.5. All functionality of Symantec Brightmail Gateway 9.0 is maintained unless otherwise noted.

Documentation

You can access English documentation at the following Web site:

http://www.symantec.com/business/support/overview.jsp?pid=53991

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

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

http://www.symantec.com/docs/TECH158577

To access the Software Update Description from the Control Center, click **Administration > Hosts > Version**. On the **Updates** tab, select an available update version and 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 documentation, copy and paste the URL below into a Web browser 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

Special update instructions for 9.5 users

Special update instructions for all users

When a Control Center has been configured so that HTTP port 41080 is used instead of HTTPS port 41443, the following issues may occur after an upgrade:

- After the upgrade, a browser connection to the Control Center cannot be established using the HTTP protocol.
- If an upgrade has been initiated over an HTTP connection, the Control Center never shows the login screen after the upgrade completes.

To resolve or mitigate this issue, a connection to the Control Center can be established using a browser via the default HTTPS port 41443. To connect to the Control Center using the HTTP protocol, HTTP port 41080 must be reenabled after the upgrade:

1. Login to the Control Center machine using the Command Line Interface (CLI).

2. Verify that the upgrade has completed by executing the CLI 'show' command: show --version

The correct version should be shown.

3. Enable HTTP connections to the Control Center using the CLI 'cc-config' command: cc-config http --on

This command restarts the Control Center and enables HTTP connections.

Special instructions for users upgrading from 9.5.0-19

Symantec released two builds of 9.5. If you are upgrading from build 9.5.0-23, you may disregard this section.

If you are upgrading from 9.5.0-19, Symantec strongly recommends that you upgrade your Control Center before upgrading your Scanners. If you do not upgrade the Control Center first, you must use the Command Line Interface (CLI) to upgrade remote Scanners.

Supported platforms

You can update to Symantec Messaging Gateway 9.5.1 on any of the following platforms:

- All supported hardware versions, including the Symantec Mail Security 8300 Series and Symantec Brightmail 8300 Series. You can also view the Symantec Messaging Gateway Hardware Testing Support Statement at the following URL: http://go.symantec.com/appliance_hw_support.
- VMware ESX or ESXi 3.5 - 4.1
- vSphere 4.0 or 4.1

Supported Web browsers

You can access the Control Center on any of the following Web browsers:

- Internet Explorer 7, 8
- Firefox 3.x

Supported paths to version 9.5.1

You can update to Symantec Messaging Gateway 9.5.1 using any of the following methods:

- Software update from version 8.0.3 or later
- OSrestore from ISO on hardware or in virtual environment
- VMware installation with OVF file
  See "Important information for installing on VMware" on page 6.

Unsupported paths to version 9.5.1

You cannot update to Symantec Messaging Gateway 9.5.1 using any of the following:

- Software update from versions earlier than 8.0.3
- Direct upgrade from beta versions
- Any version of VMware not listed
  See "Supported platforms" on page 5.

Important information for installing on VMware

Symantec Messaging Gateway 9.5.1 offers two methods for installing on supported VMware platforms. You can load the ISO file into a preconfigured virtual machine or you can load the OVF which includes the virtual machine configuration. Please note the following:

- The ISO file can be used on VMware ESX or ESXi 3.5 - 4.1 or vSphere 4.0 or 4.1. Refer to *Symantec Messaging Gateway 9.5 Installation Guide* for instructions.
- The OVF can be used for VMware ESX or ESXi 3.5 - 4.1 or vSphere 4.0 or 4.1. Refer to *Symantec Messaging Gateway 9.5 Installation Guide* for instructions.

Important information for updating to version 9.5.1

The following sections contain migration information to read before you update to version 9.5.1. If you are updating from version 9.0.x, only the "best practice" suggestions in the following section apply to your situation.

Note: You must update to Symantec Messaging Gateway 9.5.1 from Symantec Brightmail Gateway 8.0.3 or later. If your Control Center and Scanners are not running version 8.0.3 or later you must update them to 8.0.3 before you update to version 9.5.1. After you update the Control Center and Scanners to version 8.0.3, ensure that the Control Center can communicate with all Scanners. If the communication is successful, proceed to update the Control Center and Scanners to version 9.5.1.

Table 1-1 Symantec Messaging Gateway Migration Guidance

Item	Description
Best practice: Perform a backup	Symantec recommends that you take a full system backup before you run the software update.
Important: Do not reboot	The software update process may take several hours to complete. If you reboot before the process is complete, data corruption is likely. If data corruption occurs, the appliance must be reinstalled with a factory image.
Important: Reduce Spam Quarantine size	Versions prior to 9.0 used a database for Spam Quarantine messages. In 9.x, Spam Quarantine messages are stored in the file system to make the message store more robust and scalable. Migration of Spam Quarantine messages to the file system can take a significant amount of time depending on the number of messages to be migrated. Migration can take several hours if your Spam Quarantine contains a large number of messages. To minimize the migration time, reduce the number of messages in Spam Quarantine before you update the Control Center to version 9.5.1 from version 8.0.3. Use the Spam Quarantine Expunger to reduce the number of Spam Quarantine messages. This is not applicable if you are already running 9.0.x.
Important: Reduce content incident folder size	Changes have been made in how content incidents are stored. As a result, migrating content incidents can take a significant amount of time. In particular, the amount of time can be large if your Control Center has a large number of incidents in the folders. To minimize update time, delete unnecessary incidents before you update the Control Center to version 9.5.1 from version 8.0.3. This is not applicable if you are already running 9.0.x.
Best practice: Delete log messages	If your site policies let you, delete all Scanner and LDAP log messages.

Table 1-1 Symantec Messaging Gateway Migration Guidance *(continued)*

Item	Description
Best practice: Stop mail flow to Scanners and flush queues before updating	To reduce Scanner update time and complexity you should stop mail flow to Scanners and reduce the size of all queues. To halt incoming messages, click **Administration > Hosts > Configuration**, 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.
Best practice: Stop mail flow to shared Control Center/Scanner systems if using content incidents	Stop mail flow to all-in-one Control Center and Scanner systems before you update. The new incidents that are created on a combined Control Center and Scanner during the migration process are stored in the default incident folder. This behavior is limited to only the new incidents that are created during the Control Center migration. All previously created incidents are migrated to the correct folders. After you update to version 9.5.1, new incidents are sent to the correct folder.
Best practice: Update Scanners first	Each appliance must be updated individually. As a best practice, Symantec recommends that you update all Scanners before updating the Control Center. You do not have to update all of your Scanners at the same time. You can update some Scanners to version 9.5.1 and leave some with the older version. That way some Scanners continue to protect your site while you update others. However, if the Control Center and Scanner versions are different, the Control Center cannot make configuration changes to the Scanner.
Best practice: Perform software update at off-peak hours	When you update the Control Center, the Control Center appliance is offline and unusable. Scanners cannot deliver messages to quarantine on the Control Center during the software update, so messages build up in a queue. Running software update on 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.

Table 1-1 Symantec Messaging Gateway Migration Guidance *(continued)*

Item	Description
Directory integration considerations when updating from version 8.0.3	■ For some installations, you may need to add access to LDAP ports for 9.0.x. The Control Center and Scanners using any LDAP features must be able to communicate to the LDAP servers. LDAP features include authentication, routing, recipient validation, and address resolution (previously known as synchronization). Your Control Center and Scanners may already meet this requirement. This access change is a new requirement if your environment matches the following criteria: ■ You have a distributed deployment with at least one separate Scanner AND ■ The deployment uses one or more LDAP sources with the Synchronization usage enabled If your environment matches these criteria, use the `ldapsearch` command to check connectivity on each host before you update to version 9.0.x. For information about how to use `ldapsearch`, go to the following URL on the Internet: service1.symantec.com/SUPPORT/ent-gate.nsf/docid/2009082610493254 ■ The new directory data service caches the query results to reduce the load that is placed on the directory servers and to improve Scanner performance. The cache builds over time. After you update from version 8.0.3 to version 9.5.1 there may be an initial slow down of mail throughput under heavy load. The slow down can occur in the first few minutes as the cache builds. ■ The LDAP query filter formats in 9.0.x have been standardized to use the %s, %u, and %d tokens. These tokens were previously used only for the recipient validation and routing query filters. If authentication, synchronization, or both are enabled in 8.0.3, the query filters are modified to use the standard tokens after you update to version 9.5.1. If you previously modified any of the default query filters, confirm the functionality of the authentication and address resolution functions in 9.5. Use the new **Test Query** option in the Control Center. ■ In Symantec Brightmail Gateway 8.0.3 and earlier releases, only LDAP groups were displayed in the **Administration > Users > Policy Groups** page. In 9.0.x, both LDAP groups and distribution lists are displayed for a newly added LDAP source. You can view both groups and distribution lists after you update your deployment. ■ The LDAP "recipient validation" function is now used to check incoming messages for both **Reject invalid recipients** and **Drop invalid recipients**. If you have an 8.0.3 deployment using LDAP synchronization with **Protocols > SMTP > Invalid Recipients** set to **Drop invalid recipients**, the LDAP source is migrated to a source with both "recipient validation" and "address resolution" functions enabled after you update to 9.0.x. Additionally, if you have any enabled "recipient validation" sources in your 8.0.3 deployment, they are used for **Drop invalid recipients** upon update to 9.0.x. ■ In versions 9.0.x, any recipient address that includes a domain alias is considered valid if the following conditions are true: ■ You have one or more domains configured as an alias in **Protocols > SMTP > Aliases** ■ You have **Protocols > SMTP > Invalid Recipients** set to either **Drop** or **Reject** If both of the conditions are true, no call is made to the LDAP server to determine whether the recipient is valid or not.

Table 1-1 Symantec Messaging Gateway Migration Guidance *(continued)*

Item	Description
Domino-specific directory integration considerations	If you are using one or more Domino LDAP Sync sources with one or more "Alias domain" values, add those values as Symantec Messaging Gateway domain aliases before you update to version 9.0.x. Once you have updated, you can optionally modify the resulting data directory service recipient validation and address resolution query filters to include (mail=%u@<domain>) and (uid=%u@<domain>) clauses as necessary, if you do not want to use domain aliases on the Symantec Messaging Gateway host.
New content folders are created	■ After you update a Control Center to version 9.0.x from 8.0.3, the Control Center displays twice the number of content incidents than you previously had configured. To facilitate the new incident expunger, 9.0.x requires Informational Incidents and Quarantine Incidents (hold for review) to be stored in separate folders. Folders containing mixed incidents are separated in the migration process. After migration, new incident folders are created for the quarantine incidents. All policies are migrated to save quarantine incidents to the new folders. You do not have to adjust your policy configuration after migration. ■ In 9.0.x the content folders can contain either informational incidents or quarantine incidents but not both. As a result, new behavior has been introduced. If a message violates multiple Content Quarantine polices then an incident is created for the higher precedence policy in the designated folder. Subsequent Content Quarantine violations are recorded as informational incidents in the default information incidents folder. This is not applicable if you are already running 9.0.x.
User Preferences Considerations	■ Versions of Brightmail Gateway prior to 9.0 used the LDAP synchronization schedule time to replicate user preferences to the Scanners. In 9.0.x, LDAP synchronization has been deprecated and user preferences replication happens on the default schedule of once per day at midnight. You can change the schedule or replicate user preferences manually on the **Users** tab of the **Administration > Settings > Control Center** page. ■ End user preferences are no longer in effect after you update from version 8.0.3 if all of the following conditions occur: ■ You have a distributed deployment ■ End user preferences are enabled ■ You update the Scanners before you update the Control Center To reenable end user preferences, update the Control Center and ensure that user preferences are replicated. ■ User preferences are not replicated to remote Scanners during the migration process. To ensure user preferences are applied, you must replicate them manually after you update the Control Center and all Scanners. Otherwise user preferences are replicated at the default time of midnight. Navigate to the **Users** tab of the **Administration > Settings > Control Center** page and click **Replicate Now** once all systems have been upgraded. ■ The user preference replication alert is enabled by default after you update to version 9.0.x. Symantec Brightmail Gateway sends an alert to administrators configured to receive alerts when user preferences replication finds an error. You can disable this alert on the **DDS** tab on the **Administration > Settings > Alerts** page.

Table 1-1 Symantec Messaging Gateway Migration Guidance *(continued)*

Item	Description
Change in crash alert mail from	In previous releases, crash alert notifications were sent from process-cleanup@<appliance hostname>. In versions 9.0.x, the envelope sender of a crash alert is the same address as the envelope recipient.
URI reporting enabled after update	This release can detect and record Uniform Resource Identifiers (URI) that occur in email messages to improve URI-based filters. Symantec Messaging Gateway sends Symantec Security Response every URI in the messages that Symantec Messaging Gateway scans for spam (inbound and outbound scanning). Symantec uses this information to develop new URI-based filters. You receive these updated filters through the Conduit. This feature is enabled by default. If you want to change this setting, go to the **Email** tab of the **Spam > Settings > Scan Settings** page, check or uncheck the item "Report URIs to Symantec Security Response" then click **Save**.

Known issues

Note the following known issues in version 9.5.

Ensure that all remote scanners are accessible by the Control Center when making configuration changes

An error occurs when content filters are created or policy changes are made while a scanner is unreachable. To avoid this, make sure that all enabled scanners are reachable when making changes to or creating a policy filter.

To mitigate this issue, ensure that all scanners are accessible to the Control Center. You can test this in the UI by going to **Administration** > **Hosts** > **Configuration** and then clicking on each Scanner. If no access errors are presented, then the Scanner and the Control Center can communicate.

If configuration changes are made when one or more scanners is unreachable, you may have to reapply those configuration changes

Impaired Directory Data Service functionality when using Internet Explorer 9

It is currently not possible to create, edit, or delete a data source configuration in Symantec Messaging Gateway when using Internet Explorer 9. Symantec recommends using Internet Explorer 8 instead, or another supported browser.

Expected errors in Control Center log when changing remote scanner IP address

If the IP address of remote Scanner is changed, the Control Center may initially attempt to reach the original IP address before the system updates, generating possible timeout log messages. These errors will stop within approximately three minutes of the address change.

Larger Brightmail tracker may affect MAL performance

Brightmail tracker size has increased and messages may be up to 800 bytes larger as a result of the larger tracker. This can potentially affect MAL performance. For more information, see the article at the following URL:
http://www.symantec.com/docs/TECH154442

Gatekeeper may not load for policies with a large record resource

For policies with large record resource, the gatekeeper module may fail to load. To help mitigate this issue, Symantec recommends that you keep record sizes below 200 megabytes.

Error in Brightmail Log when using the Add Scanner wizard

If you add a 9.0.2 scanner to a 9.5.1 Control Center and upgrade the scanner to 9.5.1 during scanner addition, an error message will display in the Brightmail Log indicating that the software update has failed. This error message can be safely ignored. For an accurate upgrade status, in the Control Center, navigate to Administration > Version > Updates. You can also verify the version on the dashboard and Host Configuration page.

Download Only button not available in the user interface when updating to 9.5.1

Currently, if you select the Download Only button when updating to 9.5 or 9.5.1 from a release previous to 9.5, the following message will display: "Download Only is unsupported for the selected version." Use the Install button to download and install the update.

Time settings not automatically synchronized between multiple hosts

If you have a multiple host configuration, ensure that your time settings are synchronized. Failure to do so may result in an incomplete mail audit log result set. Symantec recommends and support the use of an NTP server in these

instances. For more information, see the related article at the following URL:
http://www.symantec.com/business/support/index?page=content&id=TECH158309

Known issues for the Symantec Protection Center

Please note that all references to Symantec Protection Center are for the pending version 2.0 release of Symantec Protection Center, which has not been made available as of the release of Symantec Messaging Gateway 9.5.1.

Differences between Symantec Messaging Gateway and Symantec Protection Center report data

Due to differences in how statistics are recorded in reports presented by Symantec Protection Center, users may observe slight differences between the reports generated by Protection Center and Messaging Gateway. For more information, refer to the Protection Center documentation.

Symantec Messaging Gateway report database rows may truncate if Protection Center communication is lost

Symantec Protection Center queries the Messaging Gateway database and extracts data every three minutes. If communication is lost, Symantec Messaging Gateway continues writing reporting data to its internal database but that data is no longer extracted as expected.

When data hits 1,000,000 (one million) rows, Symantec Messaging Gateway truncates rows, starting with the oldest rows first. When communication is re-established, truncated data is not restored.

Login limitations for Symantec Protection Center integration

Symantec Messaging Gateway restricts SSO (single sign-on) access to only fully-enabled administrators. When registering with Symantec Protection Center, full-access administrator credentials must be used for login. The use of partial-rights or read-only administrator credentials is not supported.

Upgrade performed in Symantec Protection Center does not display as complete

If upgrading the Control Center or adding a Scanner host using the Symantec Protection Center console integration with Symantec Messaging Gateway, update progress will not display properly. Symantec recommends that you only use the Symantec Messaging Gateway Control Center host to perform these tasks and do not use Symantec Protection Center Single Sign-on to perform these tasks.

Cannot add fresh 9.5.1 instance to Symantec Protection Center 2.0

You may experience errors or failure when attempting to add an instance of Symantec Messaging Gateway 9.5.1 to Symantec Protection Center 2.0. This can be resolved by making sure that the Symantec Protection Center and Symantec Messaging Gateway Control Center system clocks are synchronized.

Use one of the following methods to synchronize your clocks:

- Manually adjust the clock in Protection Center to match the Messaging Gateway Control Center by clicking Administration > Date/Time in the user interface.
- Manually adjust the Symantec Messaging Gateway Control Center host clock using a different browser instance and clicking the DNS/Time tab in the Edit Host Configuration tab (by navigating to **Administration > Hosts > Configuration > Edit**).

After adjusting the Messaging Gateway clock you must restart the Control Center. You can do this in the command line interface using service controlcenter restart.

Note regarding IM filtering and access control features of Symantec Messaging Gateway

Symantec is planning to remove IM filtering and network access control in a future release of Symantec Messaging Gateway. Customers who are currently using the IM filtering features should plan for an alternative solution. Symantec recommends that customers do not enable IM filtering for new installations or existing installations that are not currently using IM filtering.

Resolved issues in 9.5.1

This release contains translated documentation for 9.5 and the following specific resolutions for 9.5.1:

UI translation issues resolved

UI translation issues for the Informational Incidents and IP Reputation Lookup pages have been resolved.

Accept IP addresses list could be truncated

Previously, the list of MTA accepted IP addresses on the SMTP Settings Tab of the Edit Host Configuration page could be reduced to 10 items if certain operations are done from the Control Center. This issue has been resolved.

HTML annotations not added to certain messages

Previously, HTML annotations are not added to some types of multipart messages. This issue has been resolved.

What's new in Symantec Messaging Gateway 9.5

Table 1-2 lists the new features and enhanced features for version 9.5 of Symantec Messaging Gateway.

Table 1-2 Symantec Messaging Gateway new features and enhanced features

New feature or enhancement	Description
New product name	Version 9.5 introduces Symantec Messaging Gateway, powered by Brightmail, previously known as Symantec Brightmail Gateway.
Handling unwanted mail category	Symantec Messaging Gateway now has new configurable verdicts for unwanted mail category. You can configure policies for emails pertaining to marketing, which are newsletters, and emails with suspicious URLs. You can choose whether or not to enable this functionality. For more information see the article at the following URL: http://www.symantec.com/docs/TECH154444
Matching text in message audit log and content filtering incidents	Symantec Messaging Gateway has enhanced message audit logs that capture the following for content filtering policies: ■ Matching policy ■ Matching text ■ Message part

Table 1-2 Symantec Messaging Gateway new features and enhanced features *(continued)*

New feature or enhancement	Description
Scanning text-based attachments	Symantec Messaging Gateway offers you the option to scan an email attachment for spam, that includes the following extensions: ■ .doc ■ .htm ■ .html ■ .rtf ■ .txt ■ .wps ■ .xml
Improved message tracking ID	Symantec Messaging Gateway provides a new message tracking ID for unwanted mails. Unwanted mails include marketing emails, newsletters, and emails with suspicious URL. The new message tracking ID helps reduce false positive and false negative submissions for unwanted email verdicts.
Enhanced user interface to upgrade to Symantec Messaging Gateway	Symantec Messaging Gateway provides enhanced software update process in the Control Center with the following features: ■ A progress bar to view the download status provides improved feedback regarding the progression of software update download and installation. ■ Separate Download Only and Install buttons provide the ability to stage the software update process, allowing for download and installation at different times. **Note:** This enhancement impacts software updates subsequent to the 9.5 release.
Dell Remote Access Controller (DRAC) Support	Symantec Messaging Gateway expands support for Integrated DRAC functionality in Symantec 8360 and 8380 hardware appliances. This lets you remotely monitor and manage the hardware environment.
More Flexible Restore	Symantec Messaging Gateway can restore a backup to a separate instance while preserving the network configuration of the restored instance. This enables easier appliance migration and disaster recovery.
TLS Logging	Symantec Messaging Gateway provides enhanced message audit logs to track messages with TLS encryption delivery status. This lets you confirm TLS delivery for auditing.

Table 1-2 Symantec Messaging Gateway new features and enhanced features *(continued)*

New feature or enhancement	Description
Integration with Symantec Protection Center	Symantec Protection Center 2.0 will provide unified management across Symantec security products, including single sign-on, composition of product management within the Protection Center console, and unified reporting across multiple products. Protection Center 2.0 will be available at no extra charge for all customers who own Symantec Messaging Gateway. Please note that all references to Symantec Protection Center in Symantec Messaging Gateway 9.5 are for the pending version 2.0 release of Symantec Protection Center, which has not been made available as of the release of Symantec Messaging Gateway 9.5. Symantec Messaging Gateway retains the username provided by Protection Center during the initial single sign-on registration. To avoid the security risks of exposing an existing administrator login, Symantec recommends creating a dedicated administrator account solely to be used for registering (and subsequently administering) Symantec Messaging Gateway withing Protection Center. These dedicated accounts must not be the default 'admin/symantec' account that ships with Symantec Messaging Gateway out of the box.
Expanded localization in Spanish and French	The Control Center user interface is fully localized into Spanish and French, in addition to the existing translations into Japanese, Simplified and Traditional Chinese, and Korean.
DNS validation	You can now reject messages based on DNS validation. Symantec Messaging Gateway can perform a reverse DNS lookup to confirm the validity of the DNS record.
Sender authentication enhancements	The implementation of SPF and Sender ID in Symantec Messaging Gateway has been re-engineered, correcting numerous known issues from previous versions. The user interface has some minor improvements. New default policies for SPF and Sender ID are available for your use or customization and use.
Subaddressing support for recipient validation	You can now enable support for subaddressing in the recipient validation feature. Subaddressing is the practice of adding text in the local portion of an email address following a plus or minus sign. For example: user+role@samplecompany.com.

Resolved login errors after software update

Previously, after completing a software update with no errors in update.log, customers would occasionally receive an application error when attempting to login to the Control Center. This issue has been resolved.

Improved delivery timeout functionality

Previously, a message held after failed delivery attempts remained in the queue longer than the configured "Sent message time-out" period. This has been resolved.

Improved DNS lookup timeout

Symantec Messaging Gateway has improved DNS timeout functionality to provide more efficient queue removal and improved error messages and notifications.

Battery Failure logged messages no longer incorrectly reported

Previously, Battery Failure messages were sometimes incorrectly returned by the Control Center. This has been resolved.

Messages signed by Outlook 2007 no longer treated as "unscannable"

Previously, digitally-signed forwarded messages were treated as unscannable by Symantec Messaging Gateway. This issue has been resolved.

Improved ENHANCEDSTATUSCODES

Previously, Symantec Messaging Gateway did not provide all expected SMTP enhanced status codes. This has been resolved and all expected status codes are now returned by Symantec Messaging Gateway.

Full display name is now provided by address masquerading

Previously, a display name in a header without quotes was truncated by Address Masquerading. This issue has been resolved so that these display names are not truncated.

Enhanced support for aliases in upgrade to 9.x

Previously, Symantec Messaging Gateway provided limited upgrade support for aliases that used case-sensitivity. Symantec Messaging Gateway now supports the ability to migrate case-sensitive aliases when upgrading to 9.x.

Load balancing for MX records when MX Lookup is enabled

Previously, load balancing was not being performed properly based on DNS results where MX resolution was specified for a downstream route. Symantec Brightmail Gateway now provides load balancing for an enabled MX Lookup Host.

Symantec Messaging Gateway now identifies RFC 2311 encrypted attachments as encrypted content

Previously, Symantec Messaging Gateway would fail to identify RFC 2311 encrypted attachments as encrypted content, creating a heightened risk leakage of viral content in encrypted messages without warning the end user. This issue has been resolved.