Symantec™ Messaging Gateway 10.0 Release Notes

powered by Brightmail™
Symantec Messaging Gateway 10.0 Release Notes

This document includes the following topics:

- About Symantec Messaging Gateway 10.0
- What's new
- Documentation
- Supported platforms
- Unsupported platforms
- Supported Web browsers
- Supported paths to version 10.0
- Unsupported paths to version 10.0
- Important information about installation on VMware
- Special instructions for users who upgrade from 9.5.0-19
- Important information before you update to version 10.0
- Known issues
- Resolved issues
About Symantec Messaging Gateway 10.0

Copyright 2012 Symantec Corporation. All rights reserved.

Symantec Messaging Gateway 10.0 is the upgrade to previous versions of Symantec Messaging Gateway, formerly Symantec Brightmail Gateway. All functionality of Symantec Messaging Gateway 10.0 is maintained unless otherwise noted.

What's new

The new features and enhanced features are as follows:

- Custom spam rules specifically for your organization based on the missed spam messages and false positive messages that administrators and end users submit.
- Integration with Data Loss Prevention Enforce Server lets you remediate quarantined messages from either Symantec Messaging Gateway Control Center or the Enforce Server administration console.
- Support for IPv6.
- Improvements to content filtering to include the following:
  - Negative policy conditions.
  - Ability to scan HTML tags in the message body.
  - Ability to specify how you want Symantec Messaging Gateway to address subsequent policy actions.
  - New variables let users view or remediate incidents from incident notification messages.
  - In addition to the ability to approve or reject items in incident folders, you can now create custom actions.
- Bypass scanning content filtering policies when Symantec Messaging Gateway detects malware.
- Send spam or suspected messages to content incident folders.
- Additional information about messages in the message queue and message audit log.
- Greater flexibility to customize your backups.
- Ability for an administrator to reset a lost password without performing an OS restore.
IM filtering and network access control functionality has been removed from this release of Symantec Messaging Gateway. Customers who currently use the IM filtering features should find an alternative solution. For more information, on the Internet, go to the following URL:
http://www.symantec.com/docs/TECH186822

All of the predefined attachment lists that Symantec provides in Symantec Messaging Gateway are now premium attachment lists. If you upgrade from a previous version, predefined, customizable attachment lists are retained, as well as any modifications that you made to those lists. New versions of the default, non-editable predefined custom attachment lists also appear in the Attachment List table.

Addressed a number of reported vulnerabilities.
For more information, see the Symantec Messaging Gateway 10.0 Administration Guide.

Documentation

You can access English documentation at the following Web site:
www.symantec.com/business/support/index?page=content&key=53991&
channel=DOCUMENTATION

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/TECH193789

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 10.0 documentation, copy and paste any of the following URLs 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)
Supported platforms

You can update to Symantec Messaging Gateway 10.0 on any of the following platforms:

- All supported hardware versions
  For more information about Symantec Messaging Gateway hardware testing support, on the Internet, go to the following URL:
  http://www.symantec.com/docs/TECH123135
- VMware ESX or ESXi 5.0/4.x
- vSphere 5.0/4.x

Unsupported platforms

Unsupported platforms are as follows:

- Any version of VMware not listed
- 8220, 8240, 8260, and 8320 purchased on or before May 2008 (based on the OptiPlex GX745 platform) hardware platforms are unsupported
  For more information about Symantec Messaging Gateway hardware testing support, on the Internet, 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:
  ```bash
  show -i
  ```

Supported Web browsers

You can access the Symantec Messaging Gateway Control Center on any of the following supported Web browsers:

- Internet Explorer 9/8
- Firefox 13 or later
Chrome 19 or later

## Supported paths to version 10.0

You can update to Symantec Messaging Gateway 10.0 by using any of the following methods:

- Software update from version 8.0.3 or later
- OS restore from ISO on supported hardware or in supported virtual environment
- VMware installation with OVF file

See “Important information about installation on VMware” on page 7.

## Unsupported paths to version 10.0

You cannot update to Symantec Messaging Gateway 10.0 by using any of the following methods:

- Versions earlier than 8.0.3
- Direct upgrade from beta versions

## Important information about installation on VMware

You can install Symantec Messaging Gateway 10.0 on supported VMware platforms by loading either of the following:

- **ISO file**
  - You can load the ISO file into a preconfigured virtual machine.
  - You can use the ISO file on VMware ESX or ESXi 5.0/4.x or vSphere 5.0/4.x.

- **OVF template**
  - You can also load the OVF, which includes the virtual machine configuration.
  - You can use the OVF for VMware ESX or ESXi 5.0/4.x or vSphere 5.0/4.x.

See the *Symantec Messaging Gateway 10.0 Installation Guide* for instructions and system requirements.

If you use the BusLogic controller when you upgrade to 10.0 with VMware ESX or VMware ESXi 4.1/4.0, you must switch the SCSI Controller Type in your virtual machine settings to "LSI SAS".

For more information, on the Internet, go to the following URL:
Special instructions for users who upgrade from 9.5.0-19

Symantec recommends that you upgrade your Control Center before you upgrade your Scanners. If you do not upgrade the Control Center first, you must use the command line interface to upgrade remote Scanners.

For more information about how to use the command line, see the Symantec Messaging Gateway Command Line Interface Reference Guide.

Important information before you update to version 10.0

This topic contains the migration information that you should read before you update to version 10.0. You must update to Symantec Messaging Gateway 10.0 from Symantec Brightmail Gateway 8.0.3 - 9.5.3.

Note: If you run a version earlier than version 8.0.3, you must update it to 8.0.3 before you update to version 10.0. 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 10.0.

For more information, on the Internet, go to the following URL: http://www.symantec.com/docs/TECH186744

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 and important considerations you should consider when you upgrade from any version.
Table 1-1  Best practices for all upgrades

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not restart.</td>
<td>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 appliance must be reinstalled with a factory image.</td>
</tr>
<tr>
<td>Delete log messages.</td>
<td>If your site policies let you, delete all Scanner and LDAP log messages.</td>
</tr>
<tr>
<td>Perform a backup.</td>
<td>Symantec recommends that you take a full system backup before you run the software update and store it off-box.</td>
</tr>
<tr>
<td>Stop mail flow to Scanners and flush queues before you update.</td>
<td>To reduce Scanner update time and complexity, you should stop mail flow to Scanners and drain all queues. To halt incoming messages, click Administration &gt; Hosts &gt; 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 &gt; SMTP &gt; Message Queues. Flush the messages that are left in the queues.</td>
</tr>
</tbody>
</table>
| Update Control Center first. | Symantec recommends that you upgrade your Control Center before you upgrade your Scanners. If you do not upgrade the Control Center first, you must use the command line interface to upgrade remote Scanners. It is crucial that the window in which you update your Scanners to 10.0 is as short as practicable. This best practice is critical because if the Control Center and Scanner versions differ, the Control Center is unable to make configuration changes to the Scanner. Configurations in which the Control Center and Scanners run different versions for an extended period are unsupported.  
   **Note:** If you upgrade from version 9.5.0-19, you must upgrade the Control Center first. |
| 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 1-2 describes suggested best practices and important considerations you should consider before you update from version 8.0.3.
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade to version 9.0 then version 10.0.</td>
<td>Symantec recommends that you upgrade to version 9.0 before you upgrade to version 10.0 to mitigate any upgrade issues due to the volume of change.</td>
</tr>
<tr>
<td>Stop mail flow to shared Control Center/Scanner systems if you use content incidents.</td>
<td>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 10.0, new incidents are sent to the correct folder.</td>
</tr>
<tr>
<td>Reduce content incident folder size.</td>
<td>Changes have been made in how content incidents are stored. As a result, the migration of 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 10.0 from version 8.0.3. This situation is not applicable if you already run 9.0.x. For more information about how to delete items in content incident folders, on the Internet, go to the following URL: <a href="http://www.symantec.com/docs/HOWTO53781">http://www.symantec.com/docs/HOWTO53781</a></td>
</tr>
</tbody>
</table>
| New content folders are created when you update from version 8.0.3. | The following are considerations you should know before you update:  
- After you update a Control Center to version 9.0.x from 8.0.3, it displays twice the number of content incident folders 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 that contain 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 filtering polices, then an incident is created for the higher precedence policy in the designated folder. Subsequent content filtering policy violations are recorded as informational incidents in the default information incidents folder. This situation is not applicable if you already run 9.0.x. |
| Change in crash alert mail notifications. | 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. |
Table 1-2  

Version 8.0.3 Specific Migration Guidance (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory data integration considerations.</td>
<td>If you upgrade from version 8.0.3 and currently use LDAP integration, see the following knowledge base article for data directory integration and user preference considerations. If you use version 9.0.x, these considerations do not apply. On the Internet, go to the following URL: <a href="http://www.symantec.com/docs/TECH187652">http://www.symantec.com/docs/TECH187652</a></td>
</tr>
<tr>
<td>Reduce Spam Quarantine size.</td>
<td>Versions before 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 10.0 from version 8.0.3. Use the Spam Quarantine Expunger to reduce the number of Spam Quarantine messages. This situation is not applicable if you already run 9.0.x. For more information about how to configure the Spam Quarantine Expunger, on the Internet, go to the following URL: <a href="http://www.symantec.com/docs/HOWTO53927">http://www.symantec.com/docs/HOWTO53927</a></td>
</tr>
<tr>
<td>URI reporting is enabled after update.</td>
<td>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 &gt; Settings &gt; Scan Settings page. Check or uncheck Report URIs to Symantec Security Response, and then click Save.</td>
</tr>
</tbody>
</table>

**Known issues**

Table 1-3 describes the known issues in version 10.0.
Table 1-3 Known issues

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIPS mode not automatically enabled when you restore a Symantec Messaging Gateway Scanner from a backup.</td>
<td>Your FIPS state is not saved as part of a backup. If you perform the restore from a backup on a Symantec Messaging Gateway 9.5.2 or later host with FIPS mode on, manually re-enable the FIPS mode after the restore completes. <a href="http://www.symantec.com/docs/TECH186248">http://www.symantec.com/docs/TECH186248</a></td>
</tr>
<tr>
<td>Unable to load cache data from /data/dds/dds-cache.ser in dds.log during upgrade from 9.x to 10.0.</td>
<td>During an upgrade of Symantec Messaging Gateway, there is an error recorded in the DDS log similar to the following: can't load data from /data/dds/dds-cache.ser This issue is benign and will be resolved during the next DDS cache update. <a href="http://www.symantec.com/docs/TECH186186">http://www.symantec.com/docs/TECH186186</a></td>
</tr>
</tbody>
</table>

Resolved issues

Table 1-4 describes the issues that are resolved in 10.0.

Table 1-4 Resolved issues

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft PowerPoint files are identified as unscannable.</td>
<td>Previous versions of Symantec Messaging Gateway would, under some circumstances, render an &quot;unscannable&quot; verdict against legacy versions of Microsoft PowerPoint files. The software has been updated to correctly recognize and identify these files.</td>
</tr>
<tr>
<td>Signed and encrypted messages that Symantec Messaging Gateway annotates may not be validated fully by an email client that is different from the one that creates the original message.</td>
<td>Customers have reported validation failures in their email clients for signed and encrypted messages. Typically, these failures occurred when the sender and recipient used different clients and a disclaimer was inserted in the message. Symantec Messaging Gateway version 10.0 ensures that the recipient’s MUA now correctly validates these types of messages.</td>
</tr>
</tbody>
</table>
### Table 1-4  Resolved issues (continued)

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insufficient log information in the message audit log for the messages that failed with the following: 421 4.4.0 [internal] no mxs for this domain ...</td>
<td>Previous versions of Symantec Messaging Gateway did not provide sufficient log information when mail delivery was deferred or failed due to connection failure. Symantec Messaging Gateway 10.0 has been updated to provide granular messages for the following scenarios:  ■ Attempts to connect to destination hosts failed due to timeout or no response: 421 4.4.0 [internal] Failed to connect: no mail servers for this domain could be reached at this time  ■ No attempt to connect to destination hosts due to domain marked down: 451 4.4.1 [internal] Connection was not attempted: domain is marked down (too many connection failures)</td>
</tr>
<tr>
<td>After upgrade from 9.0.2-9 to 9.5.x, the content filtering policy to route PGP encrypted messages to the PGP Server stops triggering.</td>
<td>After an upgrade to version 9.5.0 or later, you may have encountered unexpected behavior when you implemented the content filter rules described in the Integration Guide PGP Universal™ Gateway Email Symantec Brightmail™ Gateway October 2010 Manual. This issue has been addressed. The recommended content filtering rules now work as expected.</td>
</tr>
<tr>
<td>Virus outbreak alerts are sent even if no virus is detected.</td>
<td>Previous versions of Symantec Messaging Gateway included counts of ‘unscannable’ and ‘encrypted’ messages. These counts were used to compute the threshold value to generate a ‘virus outbreak’ alert, which resulted in the generation of false alerts. Symantec Messaging Gateway has been updated to only count actual virus instances, which enhances the integrity and usefulness of the ‘virus outbreak’ alert feature.</td>
</tr>
</tbody>
</table>
### Table 1-4 Resolved issues (continued)

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ssd-config -v2 command is not persistent after restart it changes itself back to version 1.</td>
<td>Setting the ssh protocol to version 2 persists following system restart and no longer needs to be reset.</td>
</tr>
<tr>
<td>Messages that have been received but not scanned have no clickable link on MAL display screen.</td>
<td>The ability to see the status of messages just received in the audit log was added.</td>
</tr>
<tr>
<td><a href="http://www.symantec.com/docs/TECH186181">http://www.symantec.com/docs/TECH186181</a></td>
<td></td>
</tr>
<tr>
<td>UPS alert that power has been restored is not always sent.</td>
<td>UPS alerts are now consistently sent.</td>
</tr>
<tr>
<td><a href="http://www.symantec.com/docs/TECH186180">http://www.symantec.com/docs/TECH186180</a></td>
<td></td>
</tr>
<tr>
<td>SMTP authentication (AUTH LOGIN) using SMTP forwarding does not work if there are imbedded nulls.</td>
<td>Symantec Messaging Gateway properly handles SMTP authentication using SMTP forwarding when there are imbedded nulls.</td>
</tr>
<tr>
<td><a href="http://www.symantec.com/docs/TECH172373">http://www.symantec.com/docs/TECH172373</a></td>
<td></td>
</tr>
<tr>
<td>Host names with IP-like strings generating false positives.</td>
<td>Host names with IP-like strings are now properly processed by the Scanners.</td>
</tr>
<tr>
<td><a href="http://www.symantec.com/docs/TECH162696">http://www.symantec.com/docs/TECH162696</a></td>
<td></td>
</tr>
<tr>
<td>Leading hash tag or pound symbol (#) in TLS certificate-signing request generates an application error.</td>
<td>A leading hash tag or pound symbol (#) in TLS certificate parameters no longer results in an error.</td>
</tr>
<tr>
<td><a href="http://www.symantec.com/docs/TECH167286">http://www.symantec.com/docs/TECH167286</a></td>
<td></td>
</tr>
<tr>
<td>File names are not recorded in log statements when decomposition is aborted due to exceeding maximum values.</td>
<td>When an attachment cannot be scanned, Symantec Messaging Gateway now logs the file name in the Brightmail Engine log.</td>
</tr>
<tr>
<td><a href="http://www.symantec.com/docs/TECH186178">http://www.symantec.com/docs/TECH186178</a></td>
<td></td>
</tr>
</tbody>
</table>