Symantec Brightmail™ Gateway 9.0.2 Release Notes

Symantec Brightmail Gateway 9.0.2

This document includes the following topics:

- About Symantec Brightmail Gateway 9.0.2
- Documentation
- Supported platforms
- Supported Web browsers
- Supported paths to version 9.0.2
- Unsupported paths to version 9.0.2
- Important information for installing on VMware
- Important information for updating from version 8.0.3 to version 9.0.2
- Restoring default attachment lists
- General improvements
- Known issues
- Command line interface changes

About Symantec Brightmail Gateway 9.0.2

Symantec Brightmail Gateway 9.0.2 is the upgrade to previous versions of Symantec Brightmail Gateway and Symantec Mail Security 8300 Series Appliance

Software. All functionality of Symantec Brightmail Gateway 9.0.1 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 Brightmail Gateway.

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

http://go.symantec.com/brightmail_gateway_release_updates

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 Brightmail Gateway, see the folllowing links:

http://go.symantec.com/security_appliance_support

http://go.symantec.com/appliance_hw_support

Supported platforms

You can update to Symantec Brightmail Gateway 9.0.2 on any of the following platforms:

- All supported hardware versions
- VMware ESX or ESXi 3.5 Update 4 and later
- VMware ESX or ESXi 4.0

Supported Web browsers

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

- Internet Explorer 6, 7, 8
  See "Internet Explorer 8 crash when using scroll bars" on page 17.
- Firefox 3, 3.6

Supported paths to version 9.0.2

You can update to Symantec Brightmail Gateway 9.0.2 using any of the following methods:

- Software update from version 8.0.3, 9.0.0, or 9.0.1.
- OSrestore from ISO on hardware or in virtual environment
- VMware installation with OVF file
  See "Important information for installing on VMware" on page 5.

Unsupported paths to version 9.0.2

You cannot update to Symantec Brightmail Gateway 9.0.2 using any of the following:

- Software update from versions other than 8.0.3, 9.0.0, or 9.0.1.
- Any version of VMware not listed
  See "Supported platforms" on page 4.

Important information for installing on VMware

Symantec Brightmail Gateway 9.0.2 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 ESX/ESXi 3.5 update 4 and ESX/ESXi 4.0. Refer to *Symantec Brightmail Gateway 9.0 Installation Guide* for instructions.
- The OVF can be used for ESX/ESXi 4.0 without any conversion.
- The OVF can be used in ESX/ESXi 3.5 update 4 after you use the VMware conversion tool. Refer to *Symantec Brightmail Gateway 9.0 Installation Guide* for instructions. If conversion fails, the ISO file should be used.

Important information for updating from version 8.0.3 to version 9.0.2

The following sections contain migration information to read before you update to version 9.0.2. If you have already updated your appliance to version 9.0.0 or version 9.0.1, only the "best practice" suggestions in the following section will apply to your situation.

Note: You must update to Symantec Brightmail Gateway 9.0.2 from Symantec Brightmail Gateway 8.0.3, 9.0.0, or 9.0.1. You cannot update to version 9.0.2 from any other version of Symantec Brightmail Gateway. If your Control Center and Scanners are not running version 8.0.3 you must update them to 8.0.3 before you update to version 9.0.2. 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 9.0.2.

Table 1-1 Symantec Brightmail 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 Symantec Brightmail Gateway 9.0.0 and later versions, 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 9.0.2 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 in Symantec Brightmail Gateway 9.0. 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 9.0.2 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 Brightmail 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 9.0.2, 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 9.0.2 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.
Staggered update notifications	The Symantec Brightmail Gateway Control Center displays (and can deliver) update notifications to customers when new software is available for download. Starting as a new feature with Symantec Brightmail Gateway 9.0, Symantec has a rolling notification process. Customers are incrementally notified of a new update over several weeks between the software release date and the general availability (GA) date. If you learn of a new software update but have not received a notification, you can check for an update before receiving an update notification. In the Control Center, click **Administration > Hosts > Version > Updates > Check for Updates**. If an update is available, you can download and install the update. Not receiving a notification right away is not a problem, and there is no need to contact Technical Support.

Table 1-1 Symantec Brightmail 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 Symantec Brightmail Gateway 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 9.0.2 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 Symantec Brightmail Gateway 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 9.0.2. If you previously modified any of the default query filters, confirm the functionality of the authentication and address resolution functions in 9.0.2. 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 Symantec Brightmail Gateway 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 Symantec Brightmail Gateway 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 Brightmail 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 Brightmail 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 Brightmail 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, Symantec Brightmail Gateway 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 Symantec Brightmail Gateway 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.

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

Item	Description
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 Symantec Brightmail Gateway 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.
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 Brightmail Gateway sends Symantec Security Response every URI in the messages that Symantec Brightmail 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**.

Restoring default attachment lists

Symantec has become aware of an issue that can cause a failure in the database migration step that occurs after performing a software update from version 8.0.3 to 9.0.0 (this does not occur for upgrades directly from 8.0.3 to 9.0.1 or directly from 8.0.3 to 9.0.2). This issue only occurs on systems where customers have either deleted or renamed one or more of the following default attachment lists:

- Archive Files
- Document Files
- Executable Files
- Image Files
- Multimedia Files
- True Type Executable Files

How to determine if this issue affects your site

1. Login to the Symantec Brightmail Gateway Control Center.
2. Click **Compliance > Attachment Lists** to open the **Attachment Lists** page.
3. Validate that each of the attachment lists (listed above) appears on the page exactly as displayed in this document. Capitalization and spelling MUST match.

   If all of the listed attachment lists appear, then you are not affected by this issue and you may proceed with the standard update process.
4. If any of the above listed items do NOT appear you MUST perform the following steps for EACH of the missing lists prior to beginning the software update process:
   - Click **Compliance > Attachment Lists** to open the **Attachment Lists** page.
   - Click the **Add** button.
   - Enter the name of the missing list in the **Attachment list name** box.
   - From the **File classes** list, select an attachment type (you may use anything; this step is only being performed to allow you to save the list).
   - Click **Add** to add the selected type to the list.
   - Click **Save**.
   - Validate that the attachment list you just re-created now appears on the **Attachment List** page with the correct capitalization, spelling, and spacing.
     For example: Assume that you have examined the list of attachment lists on your system and you notice that the entries for **Archive Files** and **Multimedia Files** are missing. You must perform the above steps twice: once to create a list named **Archive Files** and a second time to create a list named **Multimedia Files**.
     Capitalization and spacing MUST match the original name.
5. Once you have validated that all of the required attachment lists have been restored, you may safely continue with the update procedure.

General improvements

The following known issues have been resolved for this release of Symantec Brightmail Gateway (version 9.0.2).

Certificate management enhancements

A new feature allows you to export any certificate. Exporting a certificate can be useful if you need to add a certificate for which you did not generate a certificate signing request (CSR). After exporting, you can then import the certificate, without modification, even if you have not generated a CSR in Symantec Brightmail Gateway.

Warning: : Exporting a certificate can create significant security risk. The export file contains all the data necessary to authenticate as your server.

You can now import a certificate authority-signed certificate without having previously generated a CSR in Symantec Brightmail Gateway for that certificate, if any of the following is true:

- You previously exported the certificate from Symantec Brightmail Gateway.
- A previously imported certificate differs from the new certificate only in its dates of validity .
- Before importing, you modify the certificate import file as instructed in the *Symantec Brightmail Gateway Administration Guide*.

You can only import and use RSA-signed and RSA-keyed certificates with Symantec Brightmail Gateway.

New capability to configure per-Scanner DLP settings

If you have multiple outbound Scanners, you can now configure outbound mail routes to Symantec Network Prevent servers independently for each Scanner, on the **Symantec Data Loss Prevention Setup** page, or you can apply the settings to all outbound Scanners.

Support added for SNMP v3

You can now use SNMP version 3 queries with Symantec Brightmail Gateway. You can also continue to use SNMP version 2, with or without version 3. A new **Versions** tab on the **Adminstration > Settings > SNMP** page provides fields for both versions. See the *Symantec Brightmail Gateway Administration Guide* for more information.

Note: SNMP version 3 traps are NOT supported at this time.

SNMP query and trap now available on all 8340 models

Previously, SNMP query and trap were not available for Symantec Mail Security models 8340 sold starting in August, 2010. This issue has been fixed.

New gcore option aids in troubleshooting with diagnostics command

A new option for the `diagnostics` command, `--gcore`, allows you to generate a core of a currently running process. You can use this option to capture necessary data regarding a hung or spinning component, before restarting the component.

The following components are available:

- bmagent
- bmserver
- conduit
- imrelay
- jlu-controller
- mta

Diagnostics command no longer dumps named cache to disk

The diagnostics command, regardless of the options invoked, no longer dumps the named cache to disk. This change was made to address a known problem in the version of bind used in Symantec Brightmail Gateway Versions 9.0.x. A future version will upgrade the version of bind and revert to dumping the name cache.

New option for sshd-config command toggles block cipher support

A new option is added to the sshd-config command, --cbc. This option turns on or off support for CBC ciphers, also known as block ciphers. If set to off, the only cipher available for use is RC4, also known as arcfour.

Diagnostics now allows ftp without username and password

A new checkbox on the **Administration > Hosts > Utilities/Diagnostics** tab allows you to use ftp without entering a username or password. Uncheck the **Requires authentication** checkbox to use ftp without specifying a username or password.

You can also now use ftp without a username or password when using the `db-backup`, `db-restore`, and `diagnostics` commands from the command line.

Archive settings can now be applied to all content filtering policies

Previously, in some instances the **Apply to all current policies** checkbox on the **Content > Settings > Archive** page did not in fact apply changes to all content filtering policies. This problem has been fixed.

Problem with LDAP referrals fixed

Previously, the Symantec Brightmail Gateway LDAP Server in some cases did not handle LDAP referrals properly. LDAP referrals are a means of communicating to an LDAP client that additional results for a query may reside in one or more additional LDAP servers. This resulted in a Directory Data Service (DDS) error, and policy group resolution did not complete, causing mail to be queued. The **Administration > Users > Find User** function did not work in these cases. This problem has been fixed.

Messages from senders without fully qualified domian names no longer accepted

Previously, Symantec Brightmail Gateway in some cases accepted messages with a `MAIL FROM` value that was not a fully qualified domain name, in violation of RFC http://tools.ietf.org/html/rfc5321#section-2.3.5. This problem has been fixed.

DDS upgrade problem fixed

Previously, if you had an address resolution data source specified in your Directory Data Service but had deleted the synchronization source and upgraded Symantec Brightmail Gateway, the MTA did not function after the upgrade. This problem has been fixed.

Buffer length mismatch on EHLO fixed

Previously, an error could occur in response to a rejection at EHLO that caused a buffer length mismatch in memory. This problem has been fixed.

Quarantine Incidents folder issue with ampersands in attachment filenames resolved

Previously, if a message stored in the Quarantine Incidents folder had an ampersand character in the filename of an attachment, saving the attachment could cause the filename to be truncated and the file type to be stored as unknown. This problem has been fixed.

Issue with special characters in local domain email addresses resolved

Previously, an error in domain identification caused incorrect identification of domains. This error occured in situations where an email address containing a special character was designated as a local domain. This problem has been fixed.

Issue with preference numbers and load balancing resolved

Previously, per-domain destination routing preference numbers were in some cases ignored when using MX lookup. You specify these preference numbers on the **Delivery** tab of the **Protocols > SMTP > Domains/Edit Domain** page. This could cause load balancing to work in a sub-optimal manner. This problem has been fixed.

Alias conflict issue resolved

Previously, if you added a multi-recipient alias that includes an address that is also a recipient in another multi-recipient alias, an error occured and the Protocols >SMTP >Aliases page became unusable. This problem has been fixed.

Known issues

Note the following known issues in version 9.0.2.

Length validation for SNMP v3 authentication user name

The **Authentication user name** field on the **Administration > Settings > SNMP/Versions** tab, only accepts the following input:

- Between 1 and 32 characters, inclusive.
- USASCII letters and numbers, and the underscore character.

This information is not included in the *Symantec Brightmail Administration Guide*, or in the online help.

Initial delay in SNMP v3 response when enabled without SNMP v2

In some cases, after upgrading to version 9.0.2 and enabling SNMP v3 without enabling SNMP v2, delays in SNMP response occur initially. SNMP commands issued from a remote machine may time out at first. Response resumes after several minutes of delay.

Hard drive firmware update recommended for some appliances

A hard drive firmware update is recommended for 8200 series appliances purchased prior to November 15, 2006. This firmware is relevant only to appliances containing the listed hard drives below. To determine whether this firmware update applies to your specific appliance, call Symantec Technical Support and provide the appliance serial number.

- Maxtor 300 GB, model CD808
- Maxtor 146 GB, model YC952
- Maxtor 73 GB, model GD084
- Seagate 300 GB, model HC492
- Seagate 146 GB, model GC828
- Seagate 73 GB, model FC960
- Seagate 73 GB, model HC486

This firmware addresses known issues that could result in higher than normal hard drive failure rates. The normal Symantec Brightmail Gateway software updates do not automatically update your appliance to this recommended firmware.

For information about how to apply the firmware update, go to the following Web site:

http://service1.symantec.com/support/ent-gate.nsf/docid/2009021211184554

Regardless of whether the firmware update is applied or not, Symantec will replace any hard drive failures that occur if the appliance is still covered by the three-year warranty. However, Symantec recommends that the firmware update be applied to minimize any potential downtime. If you have questions about the document or would like further information about the issue, contact Symantec Technical Support.

Encoding and localization issues

This section describes known issues regarding encoding and localization.

Surrogate characters not supported

Symantec Brightmail Gateway supports Unicode version 3.0. Unicode version 3.0 does not accommodate the 16-bit surrogate pairs that are used for supplemental characters in extended character sets. Using surrogate characters can result in improperly saved data and problems logging on to the Control Center.

Saving a file as CSV or HTML can result in corrupted file or report name

When saving a report as CSV or HTML, the name of the file or the name of the report within the file may be corrupted. This affects the Japanese, Korean, Simplified Chinese, and Traditional Chinese localized versions. This occurs with Internet Explorer 6 and 7 with all versions of Windows.

Strip and Delay may not strip email attachments correctly for Asian languages

If you configure a "Strip and Delay and Suspect Virus Quarantine" virus policy for suspicious attachments, some attachments in Asian language email messages may not be stripped. This affects the Japanese, Korean, Simplified Chinese, and Traditional Chinese localized versions. Users may receive two versions of the message. One version of the message will have attachments stripped. The second version of the message will be consigned to Suspect Virus Quarantine. If released from Suspect Virus Quarantine, the message will not have any attachments stripped.

General and Control Center issues

This section describes known issues that do not fall into other categories and Control Center issues.

Internet Explorer 8 crash when using scroll bars

Due to known issues, the Internet Explorer 8 browser may crash when you use the scroll bars. These crashes are limited to Internet Explorer 8 and are not seen on any other supported browsers.

Problem applying DKIM DNS record if key length is 1536 or 2048

Many DNS servers have 256 character limitation for DNS records. Records longer than 256 characters may fail to load or the DNS server may truncate them. To avoid this issue you can use 1024 length DKIM keys. To use a 1536-bit key or 2048-bit key, split the DNS entry into multiple lines of less of than 256 characters.

Error seen when you run `update check` from command line

If you run `update check` from the command line you may see the following error: `E: Conf Broken sbg-dds`. This error can be ignored and does not indicate a functional problem.

Configuring bounce attack prevention actions for email to masqueraded or aliased addresses

If you enable bounce attack prevention, by default, messages sent to masqueraded or aliased addresses that fail bounce attack validation are rejected at connect time. Additional configuration is required to configure an alternate action for messages to masqueraded or aliased addresses failing bounce attack validation. First, configure a group for the masqueraded or aliased addresses on the Groups page. Then set an alternate action for the "If a message fails bounce attack validation" condition for that group on the Email Spam Policies page.

Bounce messages from null senders fail bounce attack validation

When bounce attack prevention is enabled for a recipient, Symantec Brightmail Gateway rejects NDR messages sent to that recipient that have a MAILFROM value of NULL.

You can create content filtering policies to eliminate or reduce these rejections by creating a policy to search for something that is known to be part of your internal helpdesk messages, such as the IP in received headers, the From address, or the Subject, and exclude those messages from spam scanning.

For example, you might create a compliance policy to bypass spam scanning for any message that has text that matches 1 or more occurrences in the message header, the header name is Received, and where the text to match is the IP address of known good senders that send mail with a MAILFROM value of NULL.

If you see 4xx SMTP errors or NullPointerException, a Symantec Network Prevent patch may be required

This issue may apply to you if you integrate Symantec Brightmail Gateway with Symantec DLP Connect. If you have configured Symantec Brightmail Gateway to route email to Symantec Network Prevent, a patch for Network Prevent may be required in the following case. This issue has been fixed in Symantec Network Prevent 9.0.1.

If consecutive messages on the same SMTP connection trigger policies on Symantec Network Prevent that modify the message, the second and later messages may be deferred with a 4xx SMTP error. A NullPointerException occurs on Symantec Network Prevent. Examples of policies that modify the message include header addition or modification and rewriting recipients. Deferred messages will eventually be processed. If many messages are deferred due to this situation, contact Symantec Technical Support to obtain a patch for Symantec Network Prevent. The patch is not publically available for direct download.

Missing report graphs with certain browsing history setting on Internet Explorer

Internet Explorer 7 has settings to determine when to check for updated web pages. If you set "Every time I visit the webpage" for the "Settings for Browsing History," bar graphs for reports will be missing. This scenario will also result in "javachart.servlet.ChartStream: no chart bean found" errors in Brightmaillog.log. Report graphs display properly with the default browsing history setting of "Automatically" or "Every time I start Internet Explorer." A similar situation occurs for Internet Explorer 6.

Services stopped using the command line cannot be started in the Control Center

If you stop a service using the command `service` *servicename* `stop`, you cannot start the service in the Control Center on the Host Configuration page. If you attempt to start the service in the Control Center, the Control Center appears to show the service as being started, but it actually is not. Ensure that you start a service using the `service` command if you stop it with that command.

Issues with reports if using Internet Explorer 6.0.3790.1830 in Windows Server 2003 SP1

If you are using Microsoft Internet Explorer 6.0.3790.1830 in Windows Server 2003 SP1, you may experience problems with reports being cached. This can result in the same report being displayed no matter which report you choose. To prevent this issue from occurring, use a different browser. The following browsers do not exhibit this behavior: Microsoft Internet Explorer 6.0.3790.3959 and later and Mozilla Firefox.

Viewing correct help page may require clearing browser cache

A problem with upgrade can result in the wrong help page appearing when you use the context-sensitive online help. In some cases you may need to clear your browser cache after upgrade, even if you cleared your browser cache immediately before upgrade.

Erroneous CPU usage report after updating virtual appliance

After upgrading Symantec Brightmail Gateway Virtual Edition, the ESX Management Console in some cases erroneously reports increased CPU usage. In cases where other monitoring methods report no increase, Symantec Brightmail Gateway Virtual Edition is behaving normally. The issue is purely cosmetic on the ESX management side, and results from the manner in which ESX assesses the CPU usage of idle processes designed to conserve power. The issue might be corrected if you use less vCPUs in your deployment. However, before changing the number of vCPUs make sure you have the minimum number required to handle the load.

Command line interface changes

In Symantec Brightmail Gateway version 9.0, some commands that existed in version 8.0 and previous versions were renamed, incorporated into other commands, or removed. The functionality of some commands was changed in Symantec Brightmail Gateway version 9.0. Refer to the following tables for more information.

Table 1-3 describes the commands that were removed in Symantec Brightmail Gateway version 9.0. In most cases, new commands replace the functionality of the removed commands.

Table 1-2 Removed commands

Old command	New command for version 9.0
`agentconfig`	Replaced with `agent-config`.
`clear`	Replaced with `delete`. In version 9.0.0, the `clear` command clears the screen. The `delete all` command returns your appliance to the original factory configuration. Unlike the old `clear all` command, the `delete all` command deletes backup files. The Control Center **Factory Reset** option now also deletes backup files.
`crawler`	Part of `diagnostics`.

Table 1-2 Removed commands *(continued)*

Old command	New command for version 9.0
`date`	Replaced with `show --date`.
`deleter`	Replaced with `delete cores`.
`dn-normalize`	The functionality of the `dn-normalize` command is not available in version 9.0.0.
`eula`	Replaced with `show --eula`.
`http`	Replaced with `cc-config http`.
`install`	Replaced with `update install`.
`ls`	Replaced with `list`.
`mta-stats`	Replaced with `monitor mta`.
`passwd`	Replaced with `password`.
`pause-mode`	Replaced with `mta-control pause-mode`.
`rebuildrpmdb`	Replaced with `rpmdb --repair`.
`rm`	Replaced with `delete files`.
`set-control-center-port-443`	Replaced with `cc-config port-443`.
`sshdctl`	Replaced with `sshd-config`.
`sshdver`	Replaced with `sshd-config --version`.
`sys-info`	Replaced with `show --info`.
`system-stats`	Replaced with `monitor system`.
`tls-ca-cert-control`	The functionality of the `tls-ca-cert-control` command is not available in version 9.0.0.

Table 1-3 describes new commands in Symantec Brightmail Gateway version 9.0.

Table 1-3 New commands

New command	Description
`clear`	In previous releases, the `clear` command deleted files. Now `clear` clears the screen.

Table 1-3 New commands *(continued)*

New command	Description
`delete`	Delete logs, configuration information, and data. The `delete` command replaces the `clear` command.
`list`	Display the file names of all files that certain commands can act on.
`monitor`	View and record information about Brightmail processes.
`password`	Change your administrative password. The `password` command replaces the `passwd` command.
`rpmdb`	Manage and repair the RPM database.
`show`	Display system information.
`sshd-config`	Configure which addresses can SSH to the appliance.

Table 1-4 lists changed commands in Symantec Brightmail Gateway version 9.0. The behavior, options, or arguments of these commands have changed. For more information about these commands, see the *Symantec Brightmail Gateway Administration Guide*, the online help, or type `help` *`command`* on the command line.

Table 1-4 Changed commands

`agent-config`

`cc-config`

`db-backup`

`db-restore`

`diagnostics`

`help`

`mta-control`

`reboot`

`service`

`shutdown`

`tail`

`update`

Table 1-5 lists the commands that have not changed in Symantec Brightmail Gateway version 9.0.

Table 1-5 Unchanged commands

`cat`

`dns-control`

`ldapsearch`

`mallog`

`nslookup`

`ping`

Table 1-5 Unchanged commands *(continued)*

`grep`

`ifconfig`

`iostat`

`malquery`

`more`

`netstat`

`route`

`telnet`

`traceroute`