==========
Symantec Messaging Gateway (formerly Symantec Brightmail Gateway) version 10.5 Software Update Notes
==========
November 2013
*
SPECIAL INSTRUCTIONS AND CAUTIONS
==========
*
Unsupported platforms

Hardware platforms 8220, 8240, 8260, 8320, and 8340 (PowerEdge 860 version) purchased on or before November 2008 are unsupported. For more information about unsupported hardware, 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:
show --info
*
*
Supported platforms

You can update to Symantec Messaging Gateway 10.5 on any of the following platforms:
--All supported hardware versions: 8380, 8360, and 8340 purchased after November 2008.
--VMware ESXi/vSphere 4.1/5.0/5.1/5.5
For more information about Symantec Messaging Gateway hardware testing support, on the Internet, go to the following URL:
http://www.symantec.com/docs/TECH123135
*
To determine what hardware version you have, at the command line type the following:
show --info
*
*
Supported Web browsers

You can access the Symantec Messaging Gateway Control Center using any of the following supported Web browsers:
--Internet Explorer 9/8
--Firefox 22 or later
--Chrome 27 or later
*
*
Please thoroughly review the following sections:
==========
*
--What's new
--Update considerations
--Running software update
--Known and Resolved Issues

--Documentation
--End User License Agreement (EULA)
*
*
What's new
==========
*
This version of Symantec Messaging Gateway introduces new features for
customers, including:
*
--Remove Zero Day Malware and Targeted Attacks from Microsoft Office
and Adobe PDF attachments with new Disarm technology.
--Block more Spam and Malware with Expanded Threat URL Reputation
--Simplify management with LDAP Authenticated Administration
--Improve management of Unscannable Messages
--Communicate securely with trusted partners using enforced inbound
TLS encryption
--Increase security with TLS-encrypted delivery to Symantec Data
Loss Prevention
--Control Spam attacks and message volume from inside your environment
with Outbound Sender Throttling Capability
--Deploy using new Hyper-V support
*
*
Update considerations
=====================
*
--Update to Symantec Messaging Gateway 10.5.0 is only supported
from version 10.0.3. No earlier or later version is supported for update.
*
--Please read the Symantec Messaging Gateway 10.5 release notes for a
complete list of update considerations.
*
As a best practice, back up your existing data before you run the software
update. The software update process may take several hours to complete. Do not
reboot while the software update is in process. If you reboot before the
process is complete, data corruption is likely. If data corruption occurs the
appliance must be re-installed with a factory image.
*
--Symantec Messaging Gateway 10.5 includes a pre-update check that verifies
that your hardware or virtual environment version can support the new release.
You can pre-check your system to ensure you are ready to upgrade either from
the command line or from the Control Center. If you are updating from the
command line interface, type "update check". If you are updating
from the Control Center, the update check is performed automatically. If a
problem exists, the status displayed is "Version not available for
download/install", along with a tooltip that provides details about the
problem and its solution, if a solution is possible. If there are no problems,
the status displayed is “Available for download”.
*
--Symantec Messaging Gateway 10.5 also includes a mandatory EULA acceptance
step. As part of the update process, the EULA is displayed in its entirety,
and you must accept it in order to continue the update.
*

--You may experience issues when updating to Symantec Messaging Gateway 10.5, especially under certain known conditions. All of the issues relate to the Control Center showing unexpected results when preparing for or performing an update. However, the update process itself is unaffected. If you encounter unexpected behavior when updating, see http://www.symantec.com/docs/TECH210607
*
Important information for installing in virtual environments

Symantec Messaging Gateway 10.5 supports two virtual environments: VMware and Microsoft Hyper-V.
*
To install on VMware:
There are 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 ESXi/vSphere 4.1/5.0/5.1./5.5
Refer to Symantec Messaging Gateway 10.5 Installation Guide for instructions and system requirements.
--The OVF can be used for VMware ESXi/vSphere 4.1/5.0/5.1/5.5
Refer to Symantec Messaging Gateway 10.5 Installation Guide for instructions and system requirements.
*
To install on Hyper-V:
There is one method for installing on supported Hyper-V platforms. You can load the ISO file into a preconfigured virtual machine.
*
Please note the following:
--The ISO file can be used on Hyper-V Windows Server 2008 and Windows Server 2012.
See the Symantec Messaging Gateway 10.5 Installation Guide for instructions and system requirements.
*
Note: To update to Symantec Messaging Gateway 10.5 in a virtual environment, you must verify that your virtual environment can support 64-bit virtualization. When Intel Virtualization Technology (also known as Intel-VT) is enabled in the BIOS, it allows the CPU to support multiple operating systems, including 64-bit architecture. On many Intel processors this setting may be disabled in the BIOS and must be enabled prior to installing Symantec Messaging Gateway 10.5. AMD processors that support 64-bit architecture usually have this setting enabled by default. See KB 1003945 from VMware for more information:
http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1003945
*
Supported paths to version 10.5.0

You can update to Symantec Messaging Gateway 10.5.0 by using any of the following methods:
--Software update from version 10.0.3 (only on supported hardware)
--OSrestore from ISO on supported hardware or in supported virtual environments
--VMware installation with OVF file
*
*
Software update planning

--You cannot update a Control Center and multiple Scanners
simultaneously. Each appliance must be updated individually.
--Symantec strongly recommends that you update your Control Center before
you update your Scanners. If you do not update the Control Center first,
Symantec recommends that you use the command line interface to update
remote Scanners.
--It is crucial that the time frame in which you update your Scanners and
Control Center to 10.5 in as short as practicable. This 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.
*
*
Running software update
==========
*
To prepare for the software update, minimize the number of messages in any of
the queues by setting the Scanner to reject incoming messages and then waiting
for the queues to drain completely.
1 To halt incoming messages, go to Administration - Hosts -
Configuration/Edit, click "Do not accept incoming messages", and click Save.
2 To check the queues, go to Status - SMTP - Message Queues.
*
*
Using the command line interface to update

To update using the command line interface:
1 Log into an appliance using an SSH client or log in at the console.
You must use your administrator credentials to log in.
2 To list available updates, type the following command:
update list
3 To verify that your system has the correct hardware and software for update,
type the following command:
update check
4 To download the update, type the following command:
update download
5 To install the update, type the following command:
update install
*
The update progress is displayed automatically when you update using the
command line.
*
To monitor the software update progress when you update using the Control
Center:
1 Using an SSH client or the console, log into the appliance you are updating.
You must use administrator credentials when logging in.
2 Type "tail -f update.log"
*
Information about the progress of the software update appears. Do not restart
the appliance before the update completes. When the update is complete,
the appliance restarts automatically. You will see the following message:
*

sms-appliance-release-<version> successfully installed.
Rebooting appliance...
*
The appliance reboots. If you have logged into the appliance using an SSH client, the connection will be lost.
*
You may receive warnings, which you can ignore. See the release notes for more information.
*
*
Testing update success

To ensure that your appliance is running Symantec Messaging Gateway version 10.5, log into the command line interface on an appliance and type the following command:
show --version
*
*
Known and Resolved Issues
==========
*
For a full list of known and resolved issues, please see the Symantec Messaging Gateway 10.5 Release Notes.
*
*
Documentation
*
==========
For more information, see the Symantec Messaging Gateway documentation. On the Internet, go to the following URL:
*
http://www.symantec.com/business/support/index?page=content&key=53991&channel=DOCUMENTATION&sort=recent
*
For late-breaking issues, go to the following URL:
http://www.symantec.com/docs/TECH210604
*
*
End User License Agreement (EULA)
==========
*
After you update, you can display the End User License Agreement (EULA) from the command line interface.
*
To view the EULA:
1 Log into the appliance's command line interface and type:
  show --eula
The EULA appears.
2 To page through the EULA, use the space bar.
3 To exit the display of the EULA, type:
  q
The command prompt appears.