Symantec™

A Division of Broadcom

Symantec ™ Messaging Gateway 10.7.4 Installation Guide

Symantec™ Messaging Gateway 10.7.4 Installation Guide

Legal Notice

Technical Support

Symantec provides standard support for only the most current build of the licensed software. To view the Symantec support policy for SMG, see the following links:

http://go.symantec.com/security_appliance_support

http://go.symantec.com/appliance_hw_support

Contents

System requirements

This chapter includes the following topics:

System configuration options

You can install and run (Symantec Messaging Gateway) in the following ways:

- You can use a Symantec-supplied appliance. Hardware options include:
  - 8380
  - 8380-S450

    Note: SMG 10.7 runs on two different hardware platforms: The Dell 83XX and the Symantec 8380-S450. The Dell 83XX platform supports iDRAC, but the Symantec 8380-S450 platform does not.
  - 8360
  - 8340
- You can install and run a virtual appliance on your choice of hardware using VMware or Microsoft Hyper-V.
- You can install and run a combination of physical and virtual components.

System requirements for deployment on VMware

Table 1-1 lists the system requirements to deploy Symantec Messaging Gateway as a guest on a VMware ESXi Server. You must install and configure a VMware server before you install Symantec Messaging Gateway Virtual Edition ().

Note: Symantec Messaging Gateway does not provide any version of BusLogic Controller.

For the requirements that are specific to the VMware ESXi Server, refer to your VMware documentation.

Table 1-1 Supported configurations for on VMware

Description	Recommended	Minimum	Notes
VMware ESXi Server	ESXi Version 6.0 or later	Version 6.0	Supported versions: ESXi/vSphere 6.0/6.5/6.7server. The processor on the host must support VT and have this setting enabled in the BIOS before you install .
Disk type	Fixed disk	----	Symantec Messaging Gateway does not support installation on a virtual machine with a flexible disk.
Disk space	For more information, see the Symantec Knowledge Base article, *Disk Space Recommendations for Symantec Messaging Gateway Virtual Edition*.	120 GB	The recommended minimum disk space is the same for scanner-only, Control Center-only, and combined scanner and Control Center VMs.
Memory	16GB to 32 GB	8 GB	A minimum of 8 GB is necessary to run Symantec Messaging Gateway and the virtual machine.

Table 1-1 Supported configurations for on VMware *(continued)*

Description	Recommended	Minimum	Notes
CPUs	8	4	Symantec recommends allocating eight or more CPUs, based on workload demands and hardware configuration. **Note:** Your environment must support 64-bit applications.
NICs	2	1	Only one network interface card is required per virtual machine. **Note:** The maximum number of NICs that are supported is 2.
Network adapter	VMXNET3		
Storage controller			The relevant controller is automatically chosen.

See "About Symantec Messaging Gateway Virtual Edition" on page 31.

System requirements for deployment on Microsoft Hyper-V

Table 1-2 lists the system requirements to deploy Symantec Messaging Gateway as a guest on Microsoft Hyper-V server. You must install and configure one of these servers before you install Symantec Messaging Gateway Virtual Edition.

For requirements specific to Microsoft Hyper-V Server, refer to your Microsoft Hyper-V documentation.

Table 1-2 Supported configurations for on Hyper-V

Description	Recommended	Minimum	Notes
Microsoft Hyper-V	Windows 2016 Datacenter Edition	Windows 2012 Standalone	Processor on host must support VT and have this setting enabled in the BIOS before installation to support the 64-bit kernel.
Disk type	Fixed disk	----	Symantec Messaging Gateway does not support installation on a virtual machine with a dynamic disk.

Table 1-2 Supported configurations for on Hyper-V *(continued)*

Description	Recommended	Minimum	Notes
Disk space	For more information, consult the Symantec Knowledge Base article, *Disk Space Recommendations for Symantec Messaging Gateway Virtual Edition*.	120 GB	The recommended minimum disk space is the same for scanner-only, Control Center-only, and combined scanner and Control Center VMs.
Memory	16 to 32	8 GB	A minimum of 8 GB is necessary to run Symantec Messaging Gateway and the virtual machine.
CPUs	8	4	Symantec recommends allocating 8 CPUs, based on workload demands and hardware configuration. **Note:** Your environment must support 64-bit applications.
NICs	2	1	Only one network interface card is required per virtual machine. Symantec Messaging Gateway supports the use of synthetic NICs only. **Note:** The maximum number of NICs that are supported is 2.

See “About Symantec Messaging Gateway Virtual Edition” on page 31.

LDAP and web browser system requirements

Table 1-3 lists the minimum web browser and LDAP system requirements.

See “System requirements for deployment on Microsoft Hyper-V” on page 10.

See “Before you install” on page 13.

Table 1-3 System requirements

Item	Requirement
Web browsers	The Control Center supports the following browsers: ■ Microsoft Internet Explorer 11 or later ■ Mozilla Firefox 63 or later ■ Chrome 70 or later
LDAP	Symantec Messaging Gateway supports the following LDAP directory types: ■ Windows® 2012 Active Directory® (both LDAP and Global Catalog) ■ Windows 2008 Active Directory (both LDAP and Global Catalog) ■ Oracle® Directory Server Enterprise Edition 11.1.1.7 ■ Sun™ Directory Server 7.0 (EOL Dec 2017) ■ IBM® Domino® (formerly Lotus Domino) LDAP Server 8.5.3 ■ IBM LDAP Server 8.5.2 ■ IBM Domino LDAP Server 8.5 ■ OpenLDAP 2.4 ■ OpenLDAP 2.3 Symantec Messaging Gateway is LDAP v.3 compliant and can be configured to work with other directory server types. For more information about how to configure Symantec Messaging Gateway for use with LDAP, see the *Symantec™ Messaging Gateway 10.7 Administration Guide.*

Planning for installation

This chapter includes the following topics:

Before you install

Table 2-1 lists the tasks to perform before you install Symantec Messaging Gateway.

Table 2-1 Preinstallation tasks

Task	Description
Plan your deployment.	Review the following topics to help you plan your deployment. See "System configuration options" on page 8. See "Where to position your scanners" on page 21. See "Environmental factors that affect performance" on page 22.

Table 2-1 Preinstallation tasks *(continued)*

Task	Description
Meet the system requirements.	Verify that your environment meets the minimum system requirements. See "LDAP and web browser system requirements" on page 11. See "System requirements for deployment on VMware" on page 9. See "System requirements for deployment on Microsoft Hyper-V" on page 10.
Gather the items and information on the preinstallation checklist.	The preinstallation checklist specifies the items and information to have readily available when you install and set up the appliance. See "Installation checklists" on page 14.
Configure your firewall, if applicable.	If there is a firewall between any of your appliances and the Internet, configure the firewall to permit network traffic through certain ports. See "Ports that Symantec Messaging Gateway uses" on page 66.
Ensure that the required ports are available.	Symantec Messaging Gateway requires that certain ports be made available. See "Required ports" on page 65.
Virtual environments only: take a snapshot.	If you plan to update your existing virtual deployment, Symantec recommends that you take a snapshot of your existing configuration before you begin the update. Consult the documentation for your virtual environment for information about how to take snapshots.

Installation checklists

The Table 2-2 lists items and information you need to have on hand when you run bootstrap and do the initial configuration of Symantec Messaging Gateway.

Table 2-2 Initial configuration checklist

Action/Item	Description
Verify system requirements	You can install (Symantec Messaging Gateway) as a physical appliance or virtual appliance. Physical and virtual appliances can co-exist within the same enterprise network. See "*System requirements*" on page 8.
Download virtual image files (virtual appliance only)	Download the virtual image files from https://fileconnect.symantec.com/ into a single directory that you can access from the console.

Table 2-2 Initial configuration checklist *(continued)*

Action/Item	Description
Console access to the appliance	A keyboard and VGA monitor or access from another computer through a serial port. The serial port must be a null modem cable with a DB9 connector and settings of 9600 bps, 8/N/1. ___Keyboard and VGA monitor OR ___Serial port OR ___DRAC See “Installing an 8300 series appliance ” on page 28.
Open required ports on the firewall and other network devices	Some ports may need to be opened on your firewall to allow Dell Remote Access Controller (DRAC) access. For more information, see Dell Support for your iDRAC version. Required ports are TCP 22, 53, 80, 443, 41000 and 41002. As well as UDP 53 and 123. See “Required ports” on page 65. for information about usage of all ports on SMG.
Have Ethernet cables (up to four normal cables and two crossover cables) available	The number and types of cables depends on your network configuration and the number of LAN and WAN ports on the appliance. You may need crossover cables for an Inline deployment. Crossover cables are not required if one or both devices (switch, firewall) connected to the WAN port and LAN port have automatic MDI/MDI-X.
New password and host domain name	You specify a new, secure password for the administrator user that you enter when you start bootstrap. This administrator user and password is for console access to use bootstrap and the command-line interface. **Note:** No recovery mechanism for this account information exists. Make certain to safeguard this information for future use. To avoid problems with message routing, do not use your mail domain alone as the host name, such as symantecexample.com. The host name should be similar in form to: `host6.symantecexample.com` New password: ______________________________ Host domain name: ______________________________ See “Running bootstrap to configure the appliance ” on page 42.

Table 2-2 Initial configuration checklist *(continued)*

Action/Item	Description
Choose the IP address, subnet mask, default gateway address, and password for The integrated Dell Remote Access Controller (iDRAC). Physical appliance only.	Ethernet 1 is for inbound email; Ethernet 2 is for outbound. If you do not intend to use the appliance for outbound scanning, you do not need to specify an Ethernet interface 2. The integrated Dell Remote Access Controller (iDRAC) on the physical appliance provides console access to the appliance. Although integrated, iDRAC is a separate device that requires its own network address to function. The password is required to access the iDRAC's browser-based interface. On the 8380-S450, use the IP address of the host machine. There is no iDRAC on the 8380-S450 appliance. IP address of Ethernet interface 1: ______________________________ Subnet mask for Ethernet interface 1: ______________________________ IP address of Ethernet interface 2: ______________________________ Subnet mask for Ethernet interface 2: ______________________________ Default gateway (default router) IP address: ______________________________ See "Running bootstrap to configure the appliance " on page 42.
Static IP address	The static IP address is for mail routing. You can set up multiple static IP addresses or none at all. IP address or CIDR block of the destination host or network: 1. ______________________________ 2. ______________________________ 3. ______________________________ See "Running bootstrap to configure the appliance " on page 42.

Table 2-2 Initial configuration checklist *(continued)*

Action/Item	Description
Domain Name Server (DNS) server	DNS is required to route email. You can use the Internet root DNS servers or specify internal DNS servers. You can have up to three DNS servers. DNS server IP addresses: 1. ________________________________ 2. ________________________________ 3. ________________________________ See "Running bootstrap to configure the appliance " on page 42.
Appliance role	Available options are as follows: - Scanner-only - Control Center only - Scanner and Control Center For scanner-only installations, you need to provide the IP address of the Control Center that manages the scanner. Appliance role: ________________________________ IP address of Control Center (for scanner only installations): ________________________________
Valid license file	After you complete the license information on Symantec's licensing webpage, Symantec emails you a license file. The license file has a .slf suffix. The same license file can be used to license multiple appliances. You must be able to access the license file from the Control Center. File location of the license file: ________________________________ See "Register your license" on page 45.
Proxy server host name and port (optional)	You only need to provide proxy server information if you use a proxy server to communicate with Symantec. Proxy server host name: ________________________________ Proxy server port: ________________________________ See "Register your license" on page 45.

Table 2-2 Initial configuration checklist *(continued)*

Action/Item	Description
Administrator email address (Control Center configuration only)	Symantec Messaging Gateway sends alerts to this address, if alert notifications are enabled. Administrator email address: ______________________________
NTP servers (optional)	You can specify an Internet or internal NTP server to manage time. You can specify up to three servers. NTP servers: 1. ______________________________ 2. ______________________________ 3. ______________________________
Scanner role	The scanner roles are as follows: ▪ Inbound and outbound mail filtering ▪ Inbound mail filtering only ▪ Outbound mail filtering only Scanner role: ______________________________
Scanner host name or IP address (Scanner configuration only)	You must provide a host name or IP address for the scanner. Scanner host name or IP address: ______________________________
Virtual IP address (Scanner configuration only)	If the scanner performs multiple roles (such as inbound and outbound mail filtering), you must have more than one Ethernet interface. You can do create multiple Ethernet interfaces by creating a virtual IP address. Virtual IP address: ______________________________ Netmask: ______________________________ Port: ______________________________

Table 2-3 lists information you need to have on hand when you configure a scanner to filter inbound mail.

Table 2-3 Inbound mail filtering checklist

Item	Description
Inbound mail address	This address is the address and port to use for inbound mail filtering. This address is most likely the address for your Ethernet 1 port. Inbound mail filtering IP address: ______________________________ Port: ______________________________
Inbound mail acceptance	Accept mail from all sources. OR IP addresses or host names of domains from which you accept mail: 1. ______________________________ 2. ______________________________ 3. ______________________________
Inbound local mail delivery	You can specify a specific server or you can use Enable MX Lookup. This server is typically a downstream mail server, such as your corporate mail server. You can specify an unlimited number of servers to accept inbound mail relay. IP address of mail server to accept mail relay: 1. ______________________________ Port: ____________ 2.______________________________ Port: ____________ 3.______________________________ Port: ____________ OR MX Lookup host name (do not use IP address): ______________________________

Table 2-3 Inbound mail filtering checklist *(continued)*

Item	Description
Non-local mail delivery	You can use MX Lookup, add a new host, or use an existing host. If there is a separate gateway MTA between the scanner and the Internet, provide that MTA's host name or IP address and port. Host name or IP address: ______________________________ OR MX Lookup host name: ______________________________
Local domains	These addresses are added to the **Local Domains** list. Domain or IP address: 1. ______________________________ 2. ______________________________ 3. ______________________________ OR MX Lookup host name: ______________________________

Table 2-4 lists the information you need to have on hand when you configure a scanner to filter outbound mail.

Table 2-4 Outbound mail filtering checklist

Completed	Item	Description
_____	Outbound mail address	This address is the address and port to use for outbound mail filtering. This address is most likely the address for your Ethernet 2 port. Outbound mail filtering IP address: ______________________________ Port: ______________________________

Table 2-4 Outbound mail filtering checklist *(continued)*

Completed	Item	Description
_____	Outbound mail acceptance	Provide an IP address or domain. You can specify multiple addresses and domains. IP addresses or domains: 1. ______________________________ 2. ______________________________ 3. ______________________________
_____	Outbound local mail delivery	You can specify a specific server or you can use Enable MX Lookup. This server is typically a downstream mail server, such as your corporate mail server. IP address of mail server to accept mail relay: ______________________________ OR MX Lookup host name: ______________________________
_____	Non-local mail delivery	You can use MX Lookup, add a new host, or use an existing host. If there is a separate gateway MTA between the scanner and the Internet, provide that MTA's host name or IP address and port. Host name or IP address: ______________________________ OR MX Lookup host name: ______________________________

Where to position your scanners

As a best practice, place Symantec Messaging Gateway scanners in front of other filtering products and MTAs for the following reasons:

- Filtering products and MTAs can alter or remove pre-existing message headers or modify message bodies. Symantec Messaging Gateway needs unaltered message headers and message bodies to properly filter email.
- Scanners might identify the IP address of your gateway MTA as a source of spam if your scanner is not at the messaging gateway.

- Some reputation features do not function properly when the scanner is downstream of internal MTAs. These features include Connection Classification, Fastpass, and sender groups that match IP addresses. To ensure that all incoming IP addresses are correctly identified and not confused with internal IP addresses, place your scanner at the messaging gateway.

If you plan to place your scanners downstream of an MTA, specify the gateway MTA IP address when you set up the appliance. You can also specify the IP address of the gateway MTA after installation through the Control Center.

For more information about how to specify gateway MTAs through the Control Center, see the *Symantec™ Messaging Gateway 10.7 Administration Guide*.

See “System configuration options” on page 8.

Environmental factors that affect performance

Environmental factors affect performance, including historical usage patterns of your particular deployment. Collect information about your environment to understand typical usage patterns before you install the appliance.

Outgoing SMTP connections can cause additional overhead. They can swell disk queues with email destined for the remote mail servers that might not immediately accept new email. Larger queues on disk result in reduced MTA performance. For larger organizations, inbound and outbound mail streams can be configured on separate scanners.

The characteristics of messages sent and received can affect performance; key parameters to consider are as follows:

- Average message size
- Number of messages with attachments
- Average attachment size
- Types of attachments
- Percentage of virus-infected messages in the email traffic

See “Where to position your scanners” on page 21.

See “System configuration options” on page 8.

Features that can affect performance

Table 2-5 describes how features might affect performance and how to offset the performance demands.

Table 2-5 Features that can affect performance

Feature	How performance can be affected
Policy groups	You can define the policy groups, including in each policy group the users that share filtering requirements. If a message has multiple recipients with members in different policy groups, then the scanner bifurcates the message (splits it into one or more messages). Bifurcated messages for many policy groups can degrade performance. Use policy groups as necessary, but be aware that a large number of policy groups can affect performance. For more information about Policy Groups, see the *Symantec™ Messaging Gateway 10.7 Administration Guide*.
Scanners	Performance can be affected when a Control Center must collect logging and statistics from multiple scanners. As you add scanners, monitor performance to ensure that the additional scanners do not degrade performance to unacceptable levels. For more information about scanner roles, see the *Symantec™ Messaging Gateway 10.7 Administration Guide*.
Logs	The higher the log levels, the more data the Control Center must consolidate over the network. Keep log levels relatively low unless you are troubleshooting. You can also set logs to be purged more frequently. For more information about managing the log database size, see the *Symantec™ Messaging Gateway 10.7 Administration Guide*.
Reports	Configure scheduled reports to run at times when utilization of the appliance is low. This configuration helps reduce the demand on system resources during peak hours. Store report data only for the reports you need, for the length of time you need. For more information about reports and storing report data, see the *Symantec™ Messaging Gateway 10.7 Administration Guide*.
Appliance roles	When you configure the appliance to be a Control Center and a scanner, the appliance requires the resources to fulfill both roles. In mid-sized environments and large environments, this configuration can slow performance. Consider setting up the Control Center and scanner on separate appliances.

Table 2-5 Features that can affect performance *(continued)*

Feature	How performance can be affected
Spam Quarantine	The more messages that Symantec Messaging Gateway routes to Spam Quarantine, the larger the Quarantine becomes, and the more processing that is required. ■ Do not quarantine more spam than you need to. ■ Reduce the maximum size of Spam Quarantine. You can delete the messages that are identified as spam or reduce spam retention time. For more information about Spam Quarantine thresholds, see the *Symantec™ Messaging Gateway 10.7 Administration Guide*. ■ Consider using the quarantine only for suspect spam. ■ Consider using policy groups to quarantine spam only for the users who need it. The more users who access Spam Quarantine, the more performance overhead that is required. End user quarantine is more expensive than administrator-only quarantine. ■ When many end users log on for quarantine management, Control Center performance is affected. Administrator-only access to Spam Quarantines can increase performance significantly. ■ The Spam Quarantine notifier also adds to Control Center overhead. Make sure that your system is set up to efficiently handle Spam Quarantine. ■ Per-user Expunger thresholds use far more resources than global thresholds. ■ Spread out your scheduled tasks (especially the expungers) so they don't overlap. ■ Ensure that you have adequate capacity on your LDAP server. LDAP lookups for message recipients against a limited capacity LDAP server can severely impair Spam Quarantine performance. ■ The Spam Quarantine's SMTP server may slow down. If it does, the scanner’s delivery MTA could back up when the destination MTA accepts messages slowly or not at all. As such, some legitimate mail messages may be delayed.
Text-based attachment scanning	Symantec Messaging Gateway can scan attachments for spam in an email message. Enabling this option may result in slower performance of Symantec Messaging Gateway. By default, the option is enabled in new installations of Symantec Messaging Gateway and disabled for upgrade. When this option is disabled, Symantec Messaging Gateway does not use all scanning technologies for evaluating the attachments for spam.

Table 2-5 Features that can affect performance *(continued)*

Feature	How performance can be affected
DKIM signing	Enabling DKIM signing can affect outbound messaging performance. Using a shorter encryption key can reduce this effect.
SMTP authentication	SMTP authentication adds overhead that can affect outbound messaging performance.

For more information about these topics, see the *Symantec™ Messaging Gateway 10.7 Administration Guide*.

Sample scanner port configurations

A scanner requires one of the following configurations when you configure the appliance to filter inbound email and outbound email:

- Two IP addresses
- One IP address and two TCP ports
- One IP address and one TCP port

Table 2-6 provides some examples of the port configurations that you can use (it does not include all IP address and port possibilities).

Table 2-6 Scanner port configurations examples

Port configuration	Example IP addresses and port	Notes
■ Two physical ports (eth0 and eth1) ■ Each port has one IP address	192.0.32.1:25 192.0.47.255:25	The appliance routes inbound email and outbound email on separate Ethernet ports. This configuration is the best option in most cases because it provides the most network bandwidth.
■ One physical port ■ One IP address ■ Two different TCP ports	192.0.32.1:25 192.0.32.1:50	The appliance routes inbound email and outbound email through the same physical Ethernet port but uses two different TCP ports. This configuration can result in network bottlenecks, but is suitable for sites with relatively low email traffic.

Table 2-6 Scanner port configurations examples *(continued)*

Port configuration	Example IP addresses and port	Notes
- One physical port - One standard IP address - One virtual IP address	192.0.32.1:25 192.0.36.128:25	The appliance routes inbound email and outbound email through the same physical Ethernet port. This configuration uses two different IP addresses, one of which is virtual. This configuration can result in network bottlenecks, but is suitable for sites with relatively low email traffic.
- One physical port - One standard IP address	192.0.32.1:25	The appliance routes inbound email and outbound email through the same physical Ethernet port, using the same IP address. This configuration can result in network bottlenecks, but is suitable for sites with relatively low email traffic.

See "Before you install" on page 13.

installation workflow

Before you install Symantec Messaging Gateway, review and complete the preinstallation tasks.

Table 2-7 Symantec Messaging Gateway installation workflow

Step	Task and description
1	For installing hardware, unpack the appliance, mount it, and connect the appropriate cables. See "Installing an 8300 series appliance " on page 28. For installing , access the Symantec Messaging Gateway virtual machine through VMware vSphere Client or Microsoft Hyper-V management console. See "Installing Symantec Messaging Gateway on VMware" on page 32. or See "Installing on Hyper-V" on page 37.

Table 2-7 Symantec Messaging Gateway installation workflow *(continued)*

Step	Task and description
2	For hardware, turn on the appliance. The setup wizard guides you through the setup process. For installing the in VMware vSphere Client, right-click Symantec Messaging Gateway virtual machine and select **Power on**. For installing the in Microsoft Hyper-V client, right-click Messaging Gateway virtual machine and select **Start**. See "Running bootstrap to configure the appliance " on page 42.
3	Specify the Ethernet settings.
4	Specify static IP address for routing. This step is optional.
5	Specify the IP addresses for the default gateway and your DNS servers.
6	Specify the role for the appliance.
7	Register your license. See "Register your license" on page 45.
8	If necessary, update Symantec Messaging Gateway with the latest software. See "Updating to the latest software during installation" on page 63.
9	Set up and configure the Control Center. See "Configure the Control Center" on page 47.
10	Set up the scanner. Set up your scanner based on one of the following scenarios: ■ When a scanner and the Control Center are on the same appliance, you add a scanner after immediately you set up the Control Center. See "Configure the Control Center" on page 47. ■ If the scanner is on different appliance than the Control Center, you install scanners through the Control Center. See "To add a scanner through the Control Center" on page 49.

Chapter 3

Installing a physical appliance

This chapter includes the following topics:

- Installing an 8300 series appliance
- Installing an 8380-S450 appliance

Installing an 8300 series appliance

This section describes how to set up the SMG 8380 appliance to get it ready for installing the software.

See “ installation workflow” on page 26.

To set up the appliance hardware

1. Unpack the appliance and either rack mount it or place it on a level surface.
2. Plug in AC power.
3. Plug in an Ethernet Cable to iDRAC port and enable iDRAC. For more information on iDRAC, see Dell Support.
4. Connect to the appliance with one of the following methods:
   - Connect a keyboard and VGA monitor to the appliance.
   - Connect another computer to the appliance with the serial port.
     Use a null modem cable with a DB9 connector and settings of 9600 bps, 8/N/1.

- Connect to the appliance through iDRAC console from a remote computer.

5 Connect an Ethernet cable to the jack on the back panel of the appliance that is labeled **1**. This jack corresponds to eth0.

For outbound traffic, connect a second cable to the jack on the back of the appliance that is labeled **2**. This jack corresponds to eth1.

See “Running bootstrap to configure the appliance ” on page 42.

Installing an 8380-S450 appliance

This section describes how to set up the SMG 8380-S450 appliance to get it ready for installing the software.

To set up the appliance hardware

1 Unpack the appliance and either rack mount it or place it on a level surface.

2 Plug in AC power.

3 Connect to the appliance with one of the following methods:

- Connect a keyboard and VGA monitor to the appliance.
- Connect another computer to the appliance with the serial port.
  Use a null modem cable with a DB9 connector and settings of 9600 bps, 8/N/1.

4 Connect an Ethernet cable to the jack on the back panel of the appliance that is labeled **0:0**. This jack corresponds to eth0.

For outbound traffic, connect a second cable to the jack on the back of the appliance that is labeled **1:0**. This jack corresponds to eth1.

See “Running bootstrap to configure the appliance ” on page 42.

5 Open a program such as Microsoft HyperTerminal®, PuTTY, Tera Term, or ProComm™, and configure it to use the following settings:

Baud rate: 9600 bps	Data bits: 8
Parity: none	Stops bits: 1
Flow control: none	

6 Turn on the appliance. If the appliance does not automatically turn on, press the rear soft power switch.

7 When the BIOS appears, press CTRL C to boot from the disk.

8 At the question “Do you want to switch modes?”, type ‘Y’. The SMG software installs. When the installation finishes, the appliance restarts and a prompt appears.

Installing a virtual appliance

This chapter includes the following topics:

About Symantec Messaging Gateway Virtual Edition

Symantec Messaging Gateway Virtual Edition () installs Symantec Messaging Gateway on VMware ESXi or a Microsoft Hyper-V Server. runs in virtual environments in a similar manner to a standalone hardware platform.

You can deploy Symantec Messaging Gateway as a virtual machine (VM) using an ISO image or an OS restore CD.

- See "Create a Virtual Machine on ESXi server " on page 32.
  See "Create a Virtual Machine on a Hyper-V server " on page 37.
- You can install Symantec Messaging Gateway as a VM using an OVF on ESXi/vSphere, for demonstration or testing purposes. Symantec does not recommend deploying an OVF on ESXi/vSphere in a production environment.
  See "Install an OVF template on ESXi/vSphere" on page 36.

Note: Symantec Messaging Gateway does not support a VHD for Microsoft Hyper-V.

This documentation assumes the following:

- Your environment has an existing VMware ESXi or Hyper-V Server deployment that is capable of deploying a 64-bit architecture.
- You are familiar with administering VMs.
- Your environment meets all prerequisite system requirements. Verify that 64-bit virtualization is enabled in the BIOS of the host server.
  See “System requirements for deployment on VMware” on page 9.
  See “System requirements for deployment on Microsoft Hyper-V” on page 10.

For more information about VMware, and to download trialware and prerequisite applications, see the VMware website at www.vmware.com.

For more information about Microsoft Hyper-V, see the Microsoft website at www.microsoft.com.

See “Virtual software terminology” on page 40.

Installing Symantec Messaging Gateway on VMware

You can use an ISO image or an OS restore CD to install on VMware. Use the VMware vSphere Client to access the VMware ESXi server. Download the client software from VMware website or directly from your appliance if your VMware ESXi server is configured for https access.

To start using VMware vSphere Client

1. In VMware vSphere Client, right-click on **Symantec Messaging Gateway virtual machine** and select **Power on** from the right-click menu.
2. In VMware vSphere Client, select the Symantec Messaging Gateway VM and then click the **Console** tab.

Create a Virtual Machine on ESXi server

You can configure a VM and deploy an instance of Symantec Messaging Gateway from an ISO image or an OS restore CD. You must create the VMware ESXi/vSphere server first.

See “System requirements for deployment on VMware” on page 9.

Use only ASCII characters in the entry fields when you create a VM with the management interface. The VM's display name and path cannot contain non-ASCII characters. Do not use spaces when you create file names and directories for VMs.

You may want to verify that your guest computer is configured to restart when the host computer restarts. Consult your VMware documentation for more information.

Note: By default, ESXi uses DHCP and does not use a root password. Symantec recommends that you modify the ESXi settings to create a root password and assign a static IP address before installation.

To a VM on your ESXi Server

1. Select the ESXi server on which you want to place your VM.
2. On the **File** menu, click **New**, then click **Virtual Machine**.
3. Select the **Typical** option and click **Next**.
4. Type a name for the VM and click **Next**.
5. Select a datastore option and then click **Next**. Make this selection based on your particular storage configuration.
6. Select the VM version. Select the default unless otherwise instructed. Refer to the VMware documentation.
7. For the OS, click **Linux** as the guest operating system and **CentOS 4/5/6/7 (64-bit)** as the version. Click **Next**.
8. Reserve the necessary disk space, and then click **Next**.

   See "System requirements for deployment on VMware" on page 9.

   More disk space may be required based on your deployment. After you reserve disk space and complete deployment, you must repeat the OS restore process to make any changes to disk space.
9. On the **Ready to Complete** page, check **Edit the virtual machine settings before submitting** and click **Continue**.
10. Click **Memory** at the left. Reserve the system memory based on your deployment needs, and then click **Next**.

    See "System requirements for deployment on VMware" on page 9.
11. Click **CPU** at the left. Select the number of virtual CPUs, and then click **Next**.
12. If you want a second network interface, click **Add** at the top, then choose **Ethernet Adapter**, click **Next**, click **Next** again, and click **Finish**.
13. Click **Finish**.
14. Continue the deployment to install your virtual appliance.

    See "Install SMG on your ESXi server from OS restore CD " on page 33.

    See "Install SMG on your ESXi server from your datastore " on page 35.

    See "Install SMG on your ESXi server from your local computer " on page 34.

Install SMG on your ESXi server from OS restore CD

After you configure a VM on an ESXi Server, you can use an OS restore CD or ISO image as your bootstrap media.

See “Create a Virtual Machine on ESXi server ” on page 32.

To use an OS restore CD on your ESXi Server to boot your virtual machine

1 Insert the OS restore disk into your ESXi Server's CD drive.

2 Click **Edit virtual machine settings**.

3 On the **Hardware** tab, select **CD/DVD Drive 1**.

4 Choose **Host Device** and choose **CD**.

5 Check **Connect at power on** and click **OK**.

6 Click the turn on VM icon.

The VM now restarts from the CD drive.

7 Click **Disconnect CD/DVD** and remove the disk from your drive to prevent the system from performing another OS restore.

Symantec recommends that you disconnect your boot media immediately after the initial boot process to avoid an accidental OS restore.

8 Once the installation process is complete, turn off the computer through the client and edit your computer settings.

9 On the **Hardware** tab, select **CD/DVD Drive 1**.

10 Uncheck **Connect at power on** and click **OK**.

11 Restart your computer to begin the Symantec Messaging Gateway boot sequence.

See “Running bootstrap to configure the appliance ” on page 42.

See “ installation workflow” on page 26.

Install SMG on your ESXi server from your local computer

After you configure a VM on an ESXi Server, use an ISO image on your local computer as your bootstrap media.

See “Create a Virtual Machine on ESXi server ” on page 32.

To use an ISO image on your local computer to boot your virtual machine

1 Copy the ISO image onto your local hard drive.

2 Click **Edit virtual machine settings**.

3 On the **Hardware** tab, select **New CD/DVD** and make sure **Client Device** is selected as the Device Type.

4 On the **Options** tab, select **Boot Options** and set the **Force BIOS Setup**.

5 Click **OK**. The new VM appears in the inventory.

6 Click on the new VM in the inventory, then click **Console**.

7 Click the turn on VM icon.

8 If you use an ISO image, click **Connect CD/DVD > Use ISO image**, and browse to your ISO image. If you use an OS restore CD, choose the letter of your CD/DVD drive.

The boot process begins.

9 Once the installation process is complete, the Symantec Messaging Gateway boot sequence begins.

If the Symantec Messaging Gateway boot sequence does not begin, turn off the computer through the client, click **Disconnect CD/DVD device** to disconnect your ISO image, and then restart your computer.

See “Running bootstrap to configure the appliance ” on page 42.

See “ installation workflow” on page 26.

Install SMG on your ESXi server from your datastore

After you configure a VM on an ESXi Server, you can use an ISO image on your datastore as your bootstrap media.

See “Create a Virtual Machine on ESXi server ” on page 32.

To use an ISO image on your datastore to boot your virtual machine

1 On the **Hardware** tab, select **New CD/DVD** and check **Datastore ISO file** as the Device Type.

2 Click **Browse** and select the ISO file on your datastore. If you have not already added the ISO image to your datastore, refer to your VMware documentation for the procedure.

3 Check **Connect at Power on**, then click **Finish**. The new VM appears in the inventory.

4 Turn on your new computer and access your console. The boot process begins.

5 If the console prompts you to partition your SDA device, click on the console window, and then press **Enter** for 'Yes'.

6 Once the installation process is complete, turn off the computer through the client and edit your computer settings.

7 On the **Hardware** tab, select **CD/DVD Drive 1**.

8 Uncheck **Connect at power on** and click **OK**.

9 Restart your computer to begin the Symantec Messaging Gateway bootstrap.

See “Running bootstrap to configure the appliance ” on page 42.

See “ installation workflow” on page 26.

Install an OVA template on ESXi/vSphere

Symantec provides an OVA template for demonstration or testing purposes. If you cannot successfully deploy the OVA template, you can use an OS restore disk for demonstration or testing purposes.

See “Create a Virtual Machine on ESXi server ” on page 32.

Caution: Use the OVA template in a production environment only if you are explicitly told to do so by a Symantec representative. For any production environment, Symantec recommends that you install from an ISO image or OS restore disk.

You can install an OVA template that contains on a supported VMware ESXi/vSphere server. To install the OVA template, use a vSphere or vCenter client on a computer separate from the computer that hosts your ESXi Server. You may want to verify that your guest computer is configured to restart when the host computer restarts. Consult your VMware documentation for more information.

To deploy the OVA template

1. Insert the DVD that contains the OVA template.

2. In the **File** menu of the vSphere or vCenter client, click **Deploy OVF template**.
3. On the **Source** page, click **Deploy from file**.
4. Browse and select the file `Symantec_Messaging_Gateway_10.6.*.ova`.
5. Click **Next**.
6. On the **OVF Template Details** page, click **Next**.
7. On the **Name and Location** page, enter the name for your deployment and click **Next**.
8. On the **Ready to Complete** page, click **Finish**.

   The deployment may take a few minutes. The new computer appears in your inventory when deployment completes.
9. Access the new VM from your client. The standard Symantec Messaging Gateway boot sequence begins.

   See “System requirements for deployment on VMware” on page 9.

Symantec Messaging Gateway support for VMware Tools

Symantec Messaging Gateway virtual appliances support a limited set of VMware Tools.

Only the following tools are supported:

Second-generation vmxnet Virtual NIC driver	This tool loads automatically at virtual appliance boot time. No action is required to activate this support. Currently supports vmxnet 1, 2 and 3.
vmtoolsd daemon	This tool starts automatically during virtual appliance boot time. No action is required to activate this support. The vmtoolsd daemon supports automatic turn off of the virtual appliance from the vSphere4 Client dashboard. The vmtoolsd daemon also supports the Guest Information Service.
vmmemctl	This tool enables transparent page sharing and reclaims unused memory from the guest OS. It also enables memory swapping of the VMs.

No other VMware Tools functionality is supported.

See "About Symantec Messaging Gateway Virtual Edition" on page 31.

Installing on Hyper-V

Use to install Symantec Messaging Gateway on a Hyper-V VM.

Create a Virtual Machine on a Hyper-V server

You can configure a VM and deploy an instance of Symantec Messaging Gateway from an ISO image or an OS restore CD on a computer running Standalone or Datacenter Hyper-V on a supported Windows Server. First, install the Hyper-V server.

Use only ASCII characters in the entry fields when you create a VM with the management interface. The VM's display name and path cannot contain non-ASCII characters. Do not use spaces when you create file names and directories for VMs.

You may want to verify that your guest computer is configured to restart when the host computer restarts. Consult your Microsoft documentation for more information.

Note: Dynamic disk in a virtual deployment is not supported on Microsoft Hyper-V. Please review settings for the Hyper-V guest and set the disk to fixed.

To create a Hyper-V VM

1. Click on the Microsoft Hyper-V Server on which you want to place your VM.
2. On the **Action** menu, click **New**, then click **Virtual Machine**.
3. Click **Next** to create a VM with a custom configuration.
4. Type a name for the VM, select a storage folder that pertains to your environment, and click **Next**.

5 Specify the amount of system memory based on your deployment needs, and then click **Next**.

See "System requirements for deployment on Microsoft Hyper-V" on page 10.

6 Select a virtual switch for your network adapter and then click **Next**. If you require additional network adapters, these may be added after the New Virtual Machine Wizard has completed by editing the VM settings.

7 To add a fixed hard disk to your VM, select **Attach a virtual hard disk later** and then click **Next**.

8 Click **Finish**.

9 Right-click on new VM and select **Settings**.

10 Highlight **IDE Controller 0** and click **Add** to add a new hard drive to your VM.

11 Click **New** to create a new hard drive and then click **Next**.

12 Select **Fixed** and click **Next**.

13 Specify **Name** and **Location** for the new hard drive and then click **Next**.

14 Reserve the necessary disk space, and then click **Next**.

See "System requirements for deployment on Microsoft Hyper-V" on page 10.

More disk space may be required based on your deployment. After you reserve disk space and complete deployment, you must repeat the OS restore process to make any changes to disk space.

15 Click **Finish**, and then click **OK**.

16 Continue the deployment to install your virtual appliance.

See "Install on Hyper-V VM with an OS restore CD " on page 39.

See "Install on Hyper-V from an ISO image" on page 38.

Install on Hyper-V from an ISO image

After you configure a VM on a Microsoft Hyper-V Server, you can use an ISO image on your Hyper-V server as your bootstrap media.

See "Create a Virtual Machine on a Hyper-V server " on page 37.

To install on your Hyper-V VM from an ISO image

1 Copy the Symantec Messaging Gateway install ISO to your Hyper-V server.

2 Right-click on new Microsoft Hyper-V VM and select **Connect**.

3 Select **Media** menu.

4 Select **DVD Drive > Insert Disk...**.

5. Select the Symantec Messaging Gateway install ISO and then click **Open**.
6. Start your VM to begin the Symantec Messaging Gateway boot sequence.

   See “ installation workflow” on page 26.

To start up on Microsoft Hyper-V Hypervisor

1. Access the Microsoft Hyper-V Server through the Microsoft Hyper-V Microsoft Management Console. You can download this software from the Microsoft website.
2. In Microsoft Hyper-V Microsoft Management Console, right-click on the Symantec Messaging Gateway VM and select **Start** from the right-click menu.
3. In Microsoft Hyper-V Microsoft Management Console, select the Symantec Messaging Gateway VM and then right-click and select **Connect**.

Install on Hyper-V VM with an OS restore CD

After you configure a VM on a supported Microsoft Windows Hyper-V Server, you can use an OS restore CD or ISO image as your install .

See “Create a Virtual Machine on a Hyper-V server ” on page 37.

To install on your Hyper-V VM from an OS restore CD

1. Insert the OS restore disk into your Hyper-V Server's CD/DVD drive.
2. Right-click on new Microsoft Hyper-V VM and select **Connect**.
3. Select the **Media** menu.
4. Select **DVD Drive > Insert Disk...**.
5. Select Symantec Messaging Gateway install disk in your CD/DVD drive and click **Open**.
6. Start your VM to begin the Symantec Messaging Gateway boot sequence.

   See “Running bootstrap to configure the appliance ” on page 42.

   See “ installation workflow” on page 26.

Symantec Messaging Gateway Support for Hyper-V Tools

Symantec Messaging Gateway virtual appliances provide support for a limited set of Hyper-V Tools.

Only the following tools are supported:

hv_netvsc	This tool provides support for the Hyper-V-specific (or "synthetic") network adapter.
hv_storvsc	This tool provides support for all storage devices.

hv_vmbus

This tool is the fast communication channel between the server running Hyper-V and the VM.

hv_utils

This tool provides integrated shutdown, key-value pair data exchange, and heartbeat.

See “About Symantec Messaging Gateway Virtual Edition” on page 31.

Virtual software terminology

Key terminology relating to virtual software is as follows:

Virtual machine

A virtual machine, or VM, is the software that insulates the application stack from the physical hardware.

Intel Virtualization Technology

Also known as Intel-VT. Enabled in the BIOS to support multiple operating systems, including 64-bit architecture. On many Intel processors this setting may be disabled in the BIOS. Enabled this setting before you install Symantec Messaging Gateway.

Note: AMD processors that support 64-bit architecture usually have this setting enabled by default.

Host computer OS

The host computer or operating system (OS) is the physical hardware and primary OS upon which the guest computer/OS run.

Guest computer OS

The OS installed on the VM. is the guest computer and OS.

VMware ESXi Server

VMware ESXi is an enterprise-quality VM platform.

Microsoft Hyper-V Server

A native hypervisor that Microsoft distributes. It enables platform virtualization on x86-64 systems.

Virtual computer Image

A set of files in a VMware-specific format that contains an image of a preconfigured VM and . This image can be used to install a VM on a host computer that runs the VMware ESXi Server.

ISO image or OS restore CD

An image that lets you install Symantec Messaging Gateway onto a computer that runs the VMware ESXi Server.

OVF template

A VM that includes a set of software. For example, an OVF template can include the Symantec Messaging Gateway software.

VHD template

A VM for Microsoft Hyper-V that includes a set of software.

Note: Symantec Messaging Gateway software is not available as a VHD template.

vSphere client

A desktop VM platform that connects to a VMware ESXi server.

Microsoft Management Console	An extended Windows console from which an administrator can manage a Hyper-V server.

See “About Symantec Messaging Gateway Virtual Edition” on page 31.

Chapter 5

Running bootstrap

This chapter includes the following topics:

- Running bootstrap to configure the appliance

Running bootstrap to configure the appliance

Bootstrap configures your physical Symantec Messaging Gateway appliance. You can configure the appliance as a Control Center a network scanner, or an all-in-one appliance (Control Center and scanner functionality on the same appliance). It assigns a static IP address for the management port and sets up communication between the appliance and your network. After you complete bootstrap, the system automatically restarts.

In this section you will:

- Specify Ethernet interfaces
- Specify a static IP address for routing
- Specify gateway and DNS settings, and
- Set a role for the appliance

To run bootstrap

1. Open a console window on the appliance.
2. Log on with the logon name `admin` and the password `symantec`.

   Bootstrap begins automatically when you log on for the first time before configuration.
3. When you are prompted, type your new password twice.
4. When you are prompted, type a fully qualified domain name for this host.

   To avoid problems with message routing, do not use your mail domain as the host name, such as symantecexample.com. The name should be similar in form to:

   ```
   host6.symantecexample.com
   ```

5 When you are prompted, type the number for the time zone.

Type **?** to display a list of time zones.

Press the space bar to scroll through the list, or type **Q** to exit the list.

6 When you are prompted, type the IP address for the Ethernet interface that is labeled **1** on the back of the appliance.

7 When you are prompted, type the subnet mask for Ethernet interface 1.

8 When you are prompted if you want to use the second Ethernet interface, interface 2, type **Yes** or **No**.

If yes, when you are prompted, type the IP address for Ethernet interface 2.

If **No** skip to Step 10.

9 When you are prompted, type the subnet mask for Ethernet interface 2.

10 When you are prompted whether you want to add a static IP address for routing, type **Yes** or **No**.

If yes, when you are prompted, specify the IP address or CIDR block of the destination host or network.

If **No** go to Step 13.

11 If you configure multiple Ethernet interfaces, you are prompted to specify the Ethernet Interface number (either 1 or 2, the default is 1). This setting is to force the route to be associated with the specified device.

12 When you are prompted whether you want to add another static IP address, type **Yes** or **No**.

If Yes, repeat Step 10.

13 When you are prompted, type the IP address of the default gateway (default router).

14 When you are prompted, type the IP address of the DNS server.

15 When you are prompted if you want to enter another DNS server, type **Yes** or **No**.

If Yes, type the IP address.

16 To continue installation, next you specify the role for the appliance.

17 When you are prompted, choose one of the following roles for this appliance:

- Scanner only
- Control Center only
- Scanner and Control Center

18 For **Scanner only**, when prompted, type the IP address of the Control Center that you intend to use to manage this scanner.

19 The information you have entered is displayed.

If the information is not correct, type **No**. You return to the beginning of the process to make your changes.

If the information is correct, type **Yes**. Bootstrap is complete and the appliance restarts. After the appliance restarts, you can register your appliance.

Chapter 6

Running the setup wizard

This chapter includes the following topics:

Running the setup wizard

The (Symantec Messaging Gateway) setup wizard guides you through the mandatory configuration steps of an all-in-one, scanner, or Control Center-only appliance. You run the setup wizard after you bootstrap the appliance.

In this section you will:

- Upload and register the product license
- Set administrator email address, alert notifications, location, and time settings
- Add and configure a scanner through the Control Center

This set up includes and creating the first administrator account so that you can log on to The Control Center. The console admin account in the bootstrap is independent from the administrative account in the setup wizard.

Register your license

Symantec provides you with a license file. Place this file on the computer from which you access the Control Center. Each time you add a scanner, you must confirm your licenses or register again. You can use the same license file for each scanner.

Note: For your scanners, ensure that your network is configured to permit outbound connections to Symantec on port 443. Symantec Messaging Gateway communicates with Symantec Security Response over a secure connection for product registration and ongoing operations.

The following steps appear in the setup wizard after the appliance restarts when you perform the initial setup of your appliance.

See “ installation workflow” on page 26.

To register your license

1 Open a browser on a computer that can access your appliance, and logon to SMG.

The default logon address is as follows:

https://`<hostname>`

Where `<hostname>` is the IP address, or the host name that you designate for your appliance during setup.

To use HTTP, you must enable HTTP through the command line interface and specify port 41080.

For more information about the `http` command, see the *Symantec™ Messaging Gateway 10.7 Administration Guide*.

2 On the Control Center logon page, log on as user `admin` and use the password that you specified set during initial setup.

3 On the **End-User License Agreement** page, click **I accept the terms of the license agreement** and click **Next**.

4 On the **License Information Registration** page, click **Browse** to locate your license file.

5 Select your license file and click **Open** to return to the **License Registration** page.

6 If your scanner uses a proxy server for communications with Symantec, click **Proxy Server**.

7 To specify a proxy server, check **Use HTTP Proxy** and type the server host name and port. If required, type the user name and password.

8 Click **Register License**.

If registration was successful, the **License Registration Information** page returns.

9 If registration fails you may have an inaccessible proxy, closed port 443, or an expired, missing, or corrupt license file.

To troubleshoot a license registration failure, on the License Information Registration page, click **Utilities**.

In the **Utility** field drop-down menu, select **Traceroute** or **Ping**. Then in the **Host name or IP address** field, type the host name or IP address.

Make sure you can connect to https://register.brightmail.com.

Click **Run**. The results appear in the **Results** text box.

Click **Register License**.

Complete registration.

10 If you have another license file for a different feature, repeat the process for registering each license.

11 When all of the license files are successfully registered, click **Next**.

If your software is up-to-date, the setup wizard appears. Continue with the installation process.

If a software update is available, the **Software Update** page appears.

See “Updating to the latest software during installation” on page 63.

Configure the Control Center

After you register your license or after you complete the software update, the **Administrator Settings** page appears in the setup wizard.

See “Register your license” on page 45.

See “Updating to the latest software during installation” on page 63.

See “ installation workflow” on page 26.

Configure the Control Center before you configure any scanners. If you specified this appliance as a Control Center and a scanner, the wizard continues with the scanner setup.

To configure the Control Center

1. On the **Administrator Settings** page, type an email address for the administrator.
2. Check **Receive Alert Notifications** to have Symantec Messaging Gateway send alert notifications to this address.

   You can set up alert notifications for outbreaks, spam and virus filters, message queues, disk space, SMTP authentication, directories, licenses, software updates, and events. Events include scheduled task, service, hardware, swap space, and UPS issues.

   You can add additional administrators or modify this administrator's settings in the Control Center later.

   For more information about setting up local and LDAP administrator accounts and editing an administrator, see the *Symantec™ Messaging Gateway 10.7 Administration Guide*.
3. Click **Next**.
4. On the **Time Settings** page, to verify that the date that appears in the **Current Appliance Time** area is correct, select one of the following options:

Do not change the time	The time is correct and you do not want to make changes. This option is the default setting.
Set time manually	You want to manually change the time. Type the proper values in the **Date** and **Set Time** fields.
Use NTP servers	You want to use NTP servers to manage time. Type the IP address for up to three NTP servers.

5. Click **Next**.
6. On the **System Locale** page, specify the locale that the appliance should use for formatting numbers, dates, and times. This setting is the language and regional formatting Symantec Messaging Gateway uses for messages.
7. Accept the default **Quarantine fallback encoding** format, or select one from the drop-down.

   Fallback encoding is the formatting that Symantec Messaging Gateway uses for quarantined messages if the formatting that you specified in the **System Locale** field fails.
8. Click **Next**.

   If your appliance has been set up as a Control Center and a scanner, the **Scanner Role** page appears. Select the scanner role.

   If you set up your appliance as a Control Center only, the **Setup Summary** page lists your selected configuration options.
9. On the **Setup Summary** page, select any of the following options:

- **Finish**: You are satisfied with the settings and do not want to make changes.
- **Back**: Go back to modify your settings.
- **Cancel**: End the setup process without saving changes. You cannot use the appliance until you complete the setup.

10 If your scanner is not on the Control Center, set up a scanner on a separate appliance. You can do this task through the Control Center.

See "Add and configure a scanner " on page 49.

Add and configure a scanner

You must have Full Administration rights or Manage Settings modify rights to add a scanner.

Note: None of the settings that you specify throughout the wizard are final until you click **Finish** at the end of the wizard.

To add a scanner through the Control Center

1 On the Control Center, click **Administration > Hosts > Configuration**.

2 If this scanner is the first scanner that you add, the **Add Scanner** wizard appears. Otherwise, on the **Host Configuration** page under **Reconfigure a scanner or Control Center host**, click **Add** and then click **Next**.

3 On the **Scanner Host Settings** page type a description and the host name or IP address for the new scanner and then click **Next**.

4 On the **License Registration** page, click **Browse** to locate your license file.

5 Select your license file and click **Open** to return to the **License Registration** page.

6 If your scanner uses a proxy server for communications with Symantec, click **Proxy Server**.

To specify a proxy server, check **Use HTTP Proxy** and type the server host name and port.

7 Click **Register License**.

If registration was successful, the **License Registration** page returns.

8 If registration fails on the License Information Registration page, click **Utilities** to troubleshoot.

In the **Utility** field drop-down menu, select **Traceroute** or **Ping**. Then, in the **Host name or IP address** field, type the host name or IP address.

Make sure you can connect to https://register.brightmail.com.

Click **Run**. The results appear in the **Results** text box.

Click **Register License**.

Complete registration.

9 If you have another license file for a different feature, repeat the process for registering each license.

10 When all the license files are successfully registered, click **Next**.

If your software needs to be updated, the **Software Update** page appears. See "Updating to the latest software during installation" on page 63.

11 Configure the scanner based on its function.

12 On the **Scanner Role** page, click one of the following and then click **Next**:

- **Inbound and Outbound mail filtering**
- **Outbound mail filtering**
- **Inbound mail filtering**

13 If you configured only one IP address during the initial setup, the **Create Optional Virtual IP Address** page appears.

- Select **No** if you do not want to create a Virtual IP address. Proceed to step 17.
- Select **Yes** if you want to create a Virtual IP address.

14 Click **Next**.

15 On the **Create Virtual IP Address** page, do all of the following:

Ethernet	Click to select the Ethernet interface.
IP address	Type the IP address for the virtual server.
Subnet mask	Type the subnet mask IP address.
Network	Type the network IP address.
Broadcast	Type the broadcast IP address.

16 Click **Next**.

17 As appropriate, on the following screens select or type:

- The IP address to use for inbound and outbound mail filtering.
- The port number for the SMTP port for inbound and outbound mail filtering.
- The IP addresses of the mail servers from which this scanner should accept inbound mail.
- The local domains to accept mail for.
- Specify the internal host to which this scanner should relay local domain mail after filtering is complete, or check **Enable MX Lookup for this host**. If you enable MX lookup, specify a host name instead of an IP address.

18 To modify the list, do any of the following tasks:

To add an address	Type the address into the **Domain or email address field for which to accept inbound mail** field, and click **Add**. For each domain address or email address that you add, you can also specify whether messages should be routed through a specific host and port. Add that information to the **Optionally route to the following destination host** and **Port** fields.
To delete an address	Check the address you want to remove, and click **Delete**.
To import a list of addresses	Click **Import**, and then navigate to an existing file.
To route messages according to the MX record for the specified host name	Check **Enable MX Lookup**. If you enable MX lookup, you must specify a host name, not an IP address. For example, enable MX lookup if you configure multiple downstream mail servers and use MX records for email load balancing.

19 On the **Mail Filtering - Mail Delivery** page, type a host name or IP address and port to specify how you want to relay local domain filtered mail.

20 Optionally, check **Enable MX lookup for this host**.

21 On the **Mail Filtering - Non-local Mail Delivery** page, select one of the following options to specify how you want to relay filtered mail:

Use default MX Lookup	You want to use MX Lookup to return the hosts for any domain.
Define new host	You want to specify a new host. Type a host name or IP address and port. Symantec recommends that you check **Enable MX lookup for this host** if you position the scanner at the gateway. If you choose this option, specify a host name (not an IP address).
Use an existing host	You want to use an existing host. Select a host from the drop-down list. If there is a separate gateway MTA between the scanner and the Internet, provide that MTA's host name or IP address and port.

22 Click **Next**.

23 On the **Setup Summary** page, review your settings and select one of the following options:

Finish	You are satisfied with the settings and want to save them.
Back	You want to modify your settings. Go back and revise your settings.
Cancel	You want to cancel your changes without saving them.

Chapter 7

Completing installation

This chapter includes the following topics:

Post-installation tasks

Table 7-1 lists the optional tasks that you can perform after you install Symantec Messaging Gateway.

Table 7-1 Post-installation tasks

Task	Description
Modify DNS MX records to ensure that messages are filtered.	Modify DNS mail exchange (MX) records when you implement Symantec Messaging Gateway in front of a separate MTA that receives inbound messages. See "Adjust MX records to ensure that messages are filtered" on page 54.

Table 7-1 Post-installation tasks *(continued)*

Task	Description
Modify the default filtering policies.	See "About message filtering policies " on page 55.
Test antivirus filtering.	See "Test antivirus filtering " on page 56.
Test message delivery.	See "Test the delivery of legitimate email " on page 56.
Test spam filtering.	If you filter spam, test that spam filtering works properly. See "Test spam filtering " on page 57.
Test Spam Quarantine.	If you configured Symantec Messaging Gateway to use Spam Quarantine, verify that the messages are properly quarantined. See "Test that spam messages are quarantined " on page 57.
Fine-tune features to enhance performance.	Certain features have a greater effect on performance than others. After you install the appliance, you may want to fine-tune these features to avoid performance problems. See "Features that can affect performance" on page 22.
Specify the administrator email address for email notifications.	During installation, you provide an email address for an administrator to which Symantec Messaging Gateway sends alerts. However, this address does not automatically become the email notification sender address for scheduled reports. After installation you can specify the sender address that you want to use for email report notifications. See the *Symantec™ Messaging Gateway 10.7 Administration Guide* for more details.

Adjust MX records to ensure that messages are filtered

When you implement Symantec Messaging Gateway in front of a separate MTA that receives inbound messages, you must change the DNS mail exchange (MX) records to point incoming messages to the Symantec Messaging Gateway scanner or scanners.

Spammers can look up the previous MTA's MX record if you list Symantec Messaging Gateway as a higher-weighted MX record in addition to the existing MX record. If spammers have the previous MTA's MX record, they can send spam directly to the old server and bypass spam filtering.

To prevent spammers from circumventing the new spam-filtering servers, do one of the following tasks:

- Point the MX record at your Symantec Messaging Gateway scanner or scanners. Do not point the MX record at downstream MTAs. Remove the previous MTA's MX record from DNS.
- Block off the previous MTA from the Internet through a firewall.
- Modify the firewall's network address translation (NAT) tables to route external IP addresses to internal non-routable IP addresses. You can then map from the old server to Symantec Messaging Gateway.

When you name Symantec Messaging Gateway, ensure that the name you choose does not imply its function. For example, antispam.yourdomain.com, symantec.yourdomain.com, or antivirus.yourdomain.com are not good choices.

If you want to send mail to a downstream MTA, you can specify a downstream load balancer.

About message filtering policies

Symantec Messaging Gateway installs with default message filtering policies. You can use these policies or customize them.

The initial default policies are as follows:

- The default policy group includes all users and specifies default filtering policies for spam, suspected spam, unwanted emails, and malware.
- The default spam policy modifies the subject line by prepending [Spam] and delivers the message to the inbox.
- The default suspected spam policy modifies the subject line by prepending [Suspected Spam] and delivers the message to the inbox.
- The following default policies for unwanted email apply to inbound messages only and are not assigned to the default policy group:

Marketing Mail	The default marketing email policy prepends the subject line with [Marketing Mail] and delivers the message to the inbox.
Newsletter	The default newsletter policy prepends the subject line with [Newsletter] and delivers the message to the inbox.
Suspicious URL Content	The default policy for email with Suspicious URLs prepends the subject line with [Caution: Message contains Suspicious URL Content]” and delivers the message to the inbox.

- The suspected spam threshold is set to 72.
- The default malware policy cleans the message.

- The default worm policy deletes the message.
- No default content filtering policies are in place.
- No user configuration capabilities are in place.

For more information about configuring policies and settings, see the *Symantec™ Messaging Gateway 10.7 Administration Guide*.

Test antivirus filtering

You can verify that antivirus filtering works properly by sending a test message that contains a pseudo virus. A pseudo virus is not a real virus.

To test antivirus filtering

1. In an email client (such as Microsoft Outlook), create a new email.
2. Address the email to a test account for which the policy is to clean virus-infected messages.
3. Attach a virus test file such as `eicar.com` to the email.

   Virus test files are located at

   http://www.eicar.org/
4. Send the message.
5. Send a message to the same email address that does not contain a virus.
6. After several minutes have passed, in the Control Center, click **Status > Dashboard**.

   Typically, several minutes are sufficient time for statistics to update on the Control Center.

   The **Viruses** counter on the **Dashboard** page increases by one if antivirus filtering works.
7. Check the mailbox for the test account to verify receipt of the cleaned message with the text that indicates cleaning has occurred.

Test the delivery of legitimate email

You can verify whether your preferred email program works properly with the scanner to deliver legitimate email by sending an email to a user.

To test the delivery of legitimate email

1. In an email client (such as Microsoft Outlook), create a new email.
2. Address the email to a valid user.
3. Give the message a subject that is easy to find, such as **Normal Delivery Test**.

4 Send the message.

5 Verify that the test message arrives correctly in the normal delivery location on your local host.

Test spam filtering

This test assumes that you use the default installation settings for spam message handling.

To test spam filtering

1 Create a POP3 account on your Mail Delivery Agent (MDA).

For the SMTP server setting on this account, specify the IP address of an enabled scanner.

2 Compose an email message that is addressed to an account on the computer on which the scanner runs.

3 Give the message a subject that is easy to find, such as **Test Spam Message**.

4 To classify the message as spam, include the following URL on a line by itself in the message body:

http://www.example.com/url-1.blocked/

5 Send the message.

6 Check the email account to which you sent the message.

You should find a message with the same subject prefixed by the word `[Spam]`.

7 Send a message that is not spam to the same address.

8 After several minutes have passed, in the Control Center, click **Status > Dashboard**.

The **Spam** counter on the **Dashboard** page increases by one if spam filtering works.

Test that spam messages are quarantined

You can configure Symantec Messaging Gateway to forward spam messages and suspected spam messages to Spam Quarantine. When you do, users see spam and suspected spam messages in their Spam Quarantine.

Note: The first spam message may be delayed depending on the amount of spam that your organization receives.

The default configuration inserts `[Spam]` in the subject line of spam messages and delivers them to users' inboxes, rather than to Spam Quarantine.

To test that spam messages are quarantined

1 In an email client (such as Microsoft Outlook), create a new email.

2 Address the email to an account that belongs to a group that is configured to filter spam to Spam Quarantine.

3 Give the message a subject that is easy to find, such as **Test Spam Message**.

4 To classify the message as spam, include the following URL on a line by itself:

  http://www.example.com/url-1.blocked/

5 Send the message.

6 Send a message to the same account that is not spam and that does not contain any viruses.

7 In the Control Center, click **Spam > Quarantine > Email Spam**.

8 Click **Show Filters** and in the **Subject:** box, type **Test Spam Message**.

9 Click **Display Filtered**. If Spam Quarantine is configured properly, the test spam message that you sent should appear in the result list.

  To release a quarantined message, select the message and click Release.

  Verify that the message was delivered.

Logging on and logging off

End users manage their Spam Quarantine, personal Good Senders list, Bad Senders list, and email language settings through the Control Center. Use the Control Center to configure an LDAP source, enable LDAP authentication, and enable those features.

Note: Do not create an account for an administrator that is identical to a user account name. Conversely, do not create an account for a user that is identical to an administrator account name. If a naming conflict occurs, the administrator logon takes precedence, and the user is denied access to their account. If an administrator and user have the same password and user name, the user will have access to the administrator account.

To log on as a user with an Active Directory, Oracle, Domino, or other LDAP directory server account, your administrator must enable LDAP authentication for the Control Center.

For more information about managing administrators, see the *Symantec™ Messaging Gateway 10.7 Administration Guide*.

To log on as an administrator

1. Access the Control Center from a browser.

   The default logon address is as follows:

   https://`<hostname>`

   where `<hostname>` is the host name designated for the appliance. Or you can use the IP address in place of `<hostname>`.

2. If you see a security alert message, accept the self-signed certificate to continue.

   The Control Center **Login** page appears.

3. Choose the language that you want to use to operate the Quarantine views and user views of the Control Center.

4. In the **User name** box, type the user name that your system administrator assigns to you.

   If you are the first administrator to access the Control Center, type **admin**.

5. In the **Password** box, type your administrative password.

   Contact your system administrator if you do not know the password.

6. Click **Login**.

To log on as an end user

1. Verify that you have an LDAP authentication source.

2. Access your Control Center from a browser.

   The default logon address is as follows:

   https://`<hostname>`

   where `<hostname>` is the host name designated for the appliance. Or you can use the IP address in place of `<hostname>`.

3. If you see a security alert message, accept the self-signed certificate to continue.

   The Control Center Login page appears.

4. Choose the language that you want to use to operate the Quarantine views and user views of the Control Center.

5. In the **User name** box, type your full email address (for example, kris@symantecexample.com).

6. In the **Password** box, type the password that you normally use to log on to the network.

7. Click **Login**.

8. To log off, in the upper right corner of any page, click the **Log Out** icon.

9. For security purposes, close your browser window to clear your browser’s memory.

Initial configuration tasks

During installation you set the initial configuration parameters that Symantec Messaging Gateway uses to operate. However, most customers benefit from reviewing the initial configuration settings, enabling additional features, and modifying settings that were not a part of the installation process.

Use the following four-step process to verify that you are ready to take full advantage of the extensive capabilities of Symantec Messaging Gateway to meet the specific needs of your installation.

Table 7-2 Initial configuration tasks

Step	Action	Description
Step 1	After you install Symantec Messaging Gateway, test message flow.	Verify that your appliance filters and delivers mail.
Step 2	Configure optional communications and monitoring features.	Symantec Messaging Gateway provides a variety of powerful communications and monitoring features. You can control SMTP communications parameters and security. You can control end user access and communications between your Control Center and your scanners. You can set up alerts, logs, and reports, as well as SNMP monitoring and UPS backup. For more information about optional communications and monitoring features, see the *Symantec™ Messaging Gateway 10.7 Administration Guide*.
Step 3	Configure optional directory integration features.	You can use LDAP directory data sources to integrate Symantec Messaging Gateway with your existing directory data infrastructure. For more information about configuring directory data integration, see the *Symantec™ Messaging Gateway 10.7 Administration Guide*.
Step 4	Configure optional email management and filtering features.	You can manage many aspects of email flow and filtering. These features can vastly increase antispam effectiveness, reduce infrastructure needs, and significantly enhance protection of your users and assets. For more information about email management, see the *Symantec™ Messaging Gateway 10.7 Administration Guide*.

Optional configuration tasks

Depending on your network environment, your users, and your processing needs, you may need to change some configuration settings to optimize Symantec Messaging Gateway in your environment.

Symantec recommends enabling reputation filtering for better antispam effectiveness and processing. Some optional features require the configuration of an LDAP directory data source, or have other requirements.

For more information about any of the tasks in this section, see the *Symantec™ Messaging Gateway 10.7 Administration Guide*.

Table 7-3 Communications and monitoring

Action	Description
Configure additional scanner settings.	In addition to the MTA and SMTP choices that you made during installation, you can configure and enable scanner email settings, and SMTP filtering. See "Add and configure a scanner " on page 49.
Configure Control Center settings.	Configure certificates, system locale, fallback encoding, listening ports, and SMTP settings for the Control Center. Set up end user logons for access to Spam Quarantine, and manage end user preferences data. See "Configure the Control Center" on page 47.

Table 7-4 Directory integration

Action	Description
Configure directory integration.	Create and configure LDAP directory data sources. Some Symantec Messaging Gateway features require you to configure a directory data source. For more information about configuring directory data integration, see the *Symantec™ Messaging Gateway 10.7 Administration Guide*.

Table 7-5 Email management and filtering

Action	Description
Configure email settings.	Configure additional local and non-local domains, address masquerading, aliasing, invalid recipient handling, bad message handling, SMTP greetings, postmaster address, and container limits. For more information about configuring email settings, see the *Symantec™ Messaging Gateway 10.7 Administration Guide*.
Enable reputation filtering.	Enable preliminary filtering at connection time through Brightmail Adaptive Reputation Management. By enabling this feature you can dramatically reduce message processing volumes and enhance protection. For more information about configuring reputation filtering, see the *Symantec™ Messaging Gateway 10.7 Administration Guide*.
Set up email authentication.	You can set up five different types of email authentication: SPF, Sender ID, DKIM, DMARC, and SMTP. For more information about setting up email authentication, see the *Symantec™ Messaging Gateway 10.7 Administration Guide*.
Create policy groups.	You can set up groups of users, so that you can process email messages differently based on group membership. Assign policies to groups. Or, you can skip this step if you want to apply the same actions to email messages for all users. For more information about policy groups, see the *Symantec™ Messaging Gateway 10.7 Administration Guide*.

Updating software during installation

This appendix includes the following topics:

- Updating to the latest software during installation

Updating to the latest software during installation

Symantec recommends that you update to the latest version of the software after you register your license.

Updating to the latest software during initial setup

1 On the **Software Update** page, select any of the following options:

Skip	Lets you update your software later.
Update	Updates your software now. After the update, the setup wizard appears to help you configure your appliance. See "Configure the Control Center" on page 47.
Cancel	Returns you to the **License Registration** page.
Back	See "Register your license" on page 45.

2 When the software update finishes, do one of the following:

- Refresh your browser.

- Close and re-open your browser to ensure that the cached versions of graphics display correctly.

3 To continue installation, next you configure the host.

See “Configure the Control Center” on page 47.

For details on configuring scanners, see the *Symantec™ Messaging Gateway 10.7 Administration Guide*.

Ports and web addresses

This appendix includes the following topics:

- Required ports
- Ports that Symantec Messaging Gateway uses
- Reserved ports
- Web addresses Symantec Messaging Gateway uses

Required ports

Required ports lists the ports that you must have available before you install Symantec Messaging Gateway.

Table B-1 Required ports

Protocols needed	Name	Protocol	Default port	Notes
Remote access to the appliance	SSH	TCP	22	This port provides access to the command line interface.
Access to name service	DNS	UDP (TCP)	53	The destination servers can be either internal DNS servers or the Internet root DNS servers. If you use the Internet root DNS servers, ensure that you have a rule allowing external access.
Access to the Control Center and outbound access to external Internet	HTTP	TCP	80	See "Ports that Symantec Messaging Gateway uses" on page 66.

Table B-1 Required ports *(continued)*

Protocols needed	Name	Protocol	Default port	Notes
Access to time service	NTP	UDP	123	
Access to Control Center (secured)	HTTPS	TCP	443	
Outbound access to external Internet (secured)	HTTPS	TCP	443	
MTA to scanner (bi-directional)	---	TCP	41000	
Control Center to scanner (bi-directional)	---	TCP	41002	Traffic on 41002 (the agent port), flows as follows: ■ BCC to scanner (session request) ■ Scanner to BCC (session accept) ■ BCC to scanner (agent request) ■ Scanner to BCC (agent response) ■ BCC to scanner (terminate session)

Ports that Symantec Messaging Gateway uses

Table B-2 lists the ports that Symantec Messaging Gateway components and functions use. Ensure that your firewalls permit access to these ports. These assignments may differ slightly depending on your environment and filtering types (inbound, outbound, or both).

Note: The effectiveness and accuracy of Symantec Messaging Gateway filtering depends on constant updates from the Symantec Global Intelligence Network. To maintain the usefulness of your appliance, it is crucial that you facilitate automated communications between the appliance and Symantec.

Table B-2 Ports to open in your network for Symantec Messaging Gateway

Port	Protocol	Origin	Destination	Description	Notes
22	TCP	Your management hosts	Control Center/ Scanners	SSH connectivity to the appliance	This port provides access to the command line interface.
25	TCP	Control Center/ Scanners	Internal mail servers	Inbound internal email traffic	The Control Center uses internal mail hosts to send alerts and reports.
25	TCP	Internal mail servers	Scanners	Outbound internal mail traffic	
25	TCP	Internet	Scanners	Inbound Internet mail traffic	
25	TCP	Scanners	Internet	Outbound Internet mail traffic	
25	TCP	Scanners	Internal SMTP server	SMTP authentication forwarding	
53	UDP	Scanners	Internet	DNS lookups	The destination servers can be either internal DNS servers or the Internet root DNS servers. If you use the Internet root DNS servers, ensure that you have a rule allowing external access.
80	TCP	Control Center	Internet	ThreatCon updates	The ThreatCon level appears on the **Dashboard** page.
80	TCP	Scanners	Internet	Default automatic antivirus updates and rapid response antivirus updates	
123	UDP	Control Center/ Scanners	Internet/ internal NTP Servers	Time sync servers for the appliance	
161	UDP	SNMP servers	Control Center/ Scanners	SNMP management	The default port for SNMP communications. This port can be changed to match your SNMP configuration. This port is disabled by default.

Table B-2 Ports to open in your network for Symantec Messaging Gateway *(continued)*

Port	Protocol	Origin	Destination	Description	Notes
389	TCP	Control Center/ Scanners	LDAP servers	LDAP server access to lookup users, groups, and distribution lists if the directory data service is enabled.	Both Control Center and scanners use this port if directory data service is enabled.
443	TCP	Control Center/ Scanners	Internet	Rule updates, software updates, and license registration	Symantec sends rule updates to your appliances.
587	TCP	Internet	Scanners	SMTP authentication traffic	
636	TCP	Control Center/ Scanners	LDAP servers	SSL encrypted LDAP server access to lookup users, groups, and distribution lists if the directory data service is enabled.	Both Control Center and scanners use this port if directory data service is enabled.
3268	TCP	Control Center/ Scanners	LDAP servers	Active Directory Global Catalog server (LDAP)	
3269	TCP	Control Center/ Scanners	LDAP servers	SSL encrypted Active Directory Global Catalog server (LDAP)	
41000	TCP	MTA/ Scanners	MTA/ Scanners	Bidirectional	
41002	TCP	Control Center/ Scanners	Control Center/ Scanners	Bidirectional communication between the Control Center and Scanners	Traffic on 41002 (the agent port), flows as follows: ■ BCC to scanner (session request) ■ Scanner to BCC (session accept) ■ BCC to scanner (agent request) ■ Scanner to BCC (agent response) ■ BCC to scanner (terminate session)
41015 - 41017	TCP	Control Center	Scanners	Quarantine communication	
41025	TCP	Scanners	Control Center	Quarantine communication	Scanners send quarantined messages to the Control Center on this port.

Table B-2 Ports to open in your network for Symantec Messaging Gateway *(continued)*

Port	Protocol	Origin	Destination	Description	Notes
41080	TCP	Your management hosts	Control Center	Control Center web management interface (HTTP)	This port is disabled by default.
41443	TCP	Management Hosts	Control Center	Control Center web management interface (HTTPS)	Web management port for the Control Center.
8443	TCP	SPC host	Control Center	SPC management interface (HTTPS)	To integrate Symantec Messaging Gateway with Symantec Protection Center, ensure that the Protection Center server(s) can communicate with all Symantec Messaging Gateway appliances over port 8443. Depending on your environment, this may require firewall changes.

See "Before you install" on page 13.

Reserved ports

Table B-3 lists ports that you might encounter during a security audit or in log files while you troubleshoot an issue.

Table B-3 Symantec Messaging Gateway reserved ports

Port	Protocol	Listens on	Description
199	TCP	All enabled interfaces	SNMP multiplexing protocol
953	TCP	Loopback interface	DNS
3306	TCP	Loopback interface	MySQL database
41015	TCP	All enabled interfaces	Transformation Engine
41016	TCP	All enabled interfaces	Inbound internal Suspect Virus Quarantine communication
41017	TCP	All enabled interfaces	Outbound internal Suspect Virus Quarantine communication
41018	TCP	Loopback interface	Directory data service

Table B-3 Symantec Messaging Gateway reserved ports *(continued)*

Port	Protocol	Listens on	Description
41019	TCP	Loopback interface	Directory data service shutdown

See "Before you install" on page 13.

Web addresses Symantec Messaging Gateway uses

Table B-4 lists the web addresses that Symantec Messaging Gateway uses.

Table B-4 Symantec Messaging Gateway web addresses

URL	Protocol	Port	Description
swupdate.brightmail.com	TCP	443	Used to retrieve new software.
register.brightmail.com	TCP	443	Used to register the appliance.
aztec.brightmail.com	TCP	443	Used for the following customer-specific spam submission service items: ■ Administrator spam submissions ■ Provisioning the submission service ■ Service status ■ Reading reports ■ Service configuration ■ Ruleset retrieval
rules.ara.brightmail.com	TCP	443	Used to retrieve customer-specific rulesets.
submit.ara.brightmail.com	TCP	443	Used for end user missed spam and false positive spam submissions..
probes.brightmail.com	TCP	443	Used for Probe accounts
tmsg.symantec.com	TCP	443	Used for the weekly communication of telemetry data. This report allows Symantec to gather statistical data on system utilization as well as software installation and licensing status. No personal identifying information is included in the telemetry package.
liveupdate.symantecliveupdate.com	TCP	80	Default automatic antivirus updates

Table B-4 Symantec Messaging Gateway web addresses *(continued)*

URL	Protocol	Port	Description
liveupdate.symantec.com	TCP	80	Default automatic antivirus updates
definitions.symantec.com	TCP	80	Rapid response antivirus updates

See “Ports that Symantec Messaging Gateway uses” on page 66.

Index