Symantec Brightmail™ Gateway 9.0 Installation Guide

Symantec Brightmail™ Gateway 9.0 Installation Guide

Documentation version: 9.0

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrades protection
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level

- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Managed Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Education Services	Education Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about enterprise services, please visit our web site at the following URL:

www.symantec.com/business/services/

Select your country or language from the site index.

Contents

Chapter 1

Installing Symantec Brightmail Gateway

This chapter includes the following topics:

About installation configurations

You can install and run Symantec Brightmail Gateway in several ways:

Symantec Brightmail Gateway appliance	Install and run a physical, Symantec-supplied appliance. See "Installing the Symantec Brightmail Gateway product" on page 31.
Symantec Brightmail Gateway Virtual Edition	Install and run a virtual appliance, using your choice of hardware. See "About Symantec Brightmail Gateway Virtual Edition" on page 67.
Mixed-mode	Install and run a combination of physical and virtual components.

Before you install

Table 1-1 lists the preinstallation tasks to perform before you install Symantec Brightmail Gateway.

Table 1-1 Preinstallation tasks

Task	Description
Plan your deployment.	Review the following topics to help you plan your deployment. See "About installation configurations" on page 11. See "About the appliance's functions" on page 13. See "Where to position your Scanners" on page 13. See "About the environmental factors that affect performance" on page 14.
Meet the system requirements.	Ensure that your environment meets the minimum system requirements. See "System requirements" on page 28. See "System requirements for virtual deployment" on page 68.
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 setup the appliance. See "Installation checklist" on page 15.
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 Brightmail Gateway uses" on page 22.
Ensure that the required ports are available.	Symantec Brightmail Gateway requires that certain ports be made available. See "Required ports" on page 26.
Ensure that you have the correct DNS servers, if applicable.	If you intend to use IM filtering, ensure that you have the correct DNS servers. See "About the DNS servers required for IM filtering" on page 27.

About the appliance's functions

You can use each appliance to perform a variety of functions. During the initial setup, the installation wizard prompts you to choose the function that each appliance performs. Symantec recommends that before you install the product, you decide which function or set of functions to assign your appliance. Contact a sales representative for additional help with performance sizing.

The available functions are as follows:

Control Center	A Control Center lets you configure and manage Symantec Brightmail Gateway from a Web-based interface. The Control Center provides information on the status of all of the Symantec Brightmail Gateway hosts in your environment, including logs and reports. You must configure one Control Center for your site. One Control Center controls one or more Scanners.
Scanner	Scanners can perform all of the following tasks: ■ Filter email for viruses, spam, and noncompliant messages ■ Check email against Good Senders lists and Bad Senders list ■ Filter IM messages for Spim and scan IM file transfers for viruses You can configure one or more Scanners. **Note:** Symantec Brightmail Gateway is not intended to be used for load balancing. Administrators can associate only one host name or IP address as the MTA to which email is relayed. You must implement multiple Scanners to perform load balancing.
Control Center and Scanner	Performs both functions. This configuration is suitable for smaller installations.

See "Installing the Symantec Brightmail Gateway product" on page 31.

See "About Symantec Brightmail Gateway Virtual Edition" on page 67.

Where to position your Scanners

As a best practice, place Symantec Brightmail 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 Brightmail Gateway needs unaltered message headers and message bodies to properly filter email.
- If your Scanner is not at the messaging gateway, Symantec Brightmail Gateway Scanners might identify the IP address of your gateway MTA as a source of spam.
- Many reputation features, such as Connection Classification, Fastpass, and sender groups that match IP addresses, do not function properly when the Scanner is downstream of one or more internal MTAs. To ensure that all incoming IP addresses are correctly identified and not confused with internal IP addresses, it is best to 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 Brightmail Gateway Administration Guide*.

About the 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 email 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

Installation checklist

Table 1-2 provides a list of the items and information to have on hand when you perform the hardware and initial software setup of Symantec Brightmail Gateway.

Table 1-2 Initial configuration checklist

Completed	Item	Description	Details
_____	Console access to the appliance	You need 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. See "Setting up the appliance hardware" on page 33.	___Keyboard and VGA monitor OR ___Serial port
_____	Host domain name	You are requested to change the password during this stage. Ensure you have the new password that you want to use. To avoid problems with message routing, this host name should not be your mail domain, such as symantecexample.com. For example, the name should be similar in form to: `host6.symantecexample.com` See "Starting the appliance software set up" on page 34.	New password: _____ Host domain name: _____
_____	Ethernet interfaces	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. See "Specifying Ethernet interfaces" on page 34.	IP address of Ethernet interface 1: _____ Subnet mask for Ethernet interface 1: _____ IP address of Ethernet interface 2: _____ Subnet mask for Ethernet interface 2: _____

Table 1-2 Initial configuration checklist *(continued)*

Completed	Item	Description	Details
_____	Static IP address	The static IP address is for mail routing. You can set up multiple static IP addresses or none at all. See "Specifying a static IP address for routing" on page 35.	IP address or CIDR block of the destination host or network: 1. _____ 2. _____ 3. _____
_____	Default gateway	See "Specifying gateway and DNS IP addresses" on page 36.	Default gateway (default router) IP address: _____
_____	Domain Name Server (DNS) server	DNS is required to route email. You can use the Internet root DNS servers or specify internal DNS servers. If you plan to enable IM filtering, an external DNS server and a specially configured internal DNS server are required. See "About the DNS servers required for IM filtering" on page 27. You can have up to three DNS servers. See "Specifying gateway and DNS IP addresses" on page 36.	DNS server IP addresses: 1. _____ 2. _____ 3. _____
_____	Appliance role	Available options are as follows: ■ Scanner only ■ Control Center only ■ Scanner and Control Center See "About the appliance's functions" on page 13. See "Specifying the role for the appliance" on page 37. For Scanner only installations, you need to provide the IP address of the Control Center that will manage the Scanner.	Appliance role: _____ IP address of Control Center (for Scanner only installations): _____

Table 1-2 Initial configuration checklist *(continued)*

Completed	Item	Description	Details
_____	Valid license file	After you complete the license information on Symantec's licensing Web page, 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. See "Registering your license" on page 38.	File location of the license file: _____
_____	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. See "Registering your license" on page 38.	Proxy server host name: _____ Proxy server port: _____
_____	Administrator email address (Control Center configuration only)	Symantec Brightmail 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 ■ Inbound and outbound mail filtering with instant message filtering ■ Inbound mail filtering with instant message filtering ■ Outbound mail filtering with instant message filtering	Scanner role: _____

Table 1-2 Initial configuration checklist *(continued)*

Completed	Item	Description	Details
_____	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 in bound 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 1-3 provides the information to have on hand to configure a Scanner for inbound mail filtering.

Table 1-3 Inbound mail filtering checklist

Completed	Item	Description	Details
_____	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	You can accept mail from all sources or specify the domains from which you accept mail.	Accept mail from all sources OR IP addresses or host names of domains from which you accept mail: 1. _____ 2. _____ 3. _____

Table 1-3 Inbound mail filtering checklist *(continued)*

Completed	Item	Description	Details
_____	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 up to three mail 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): _____
_____	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 1-4 provides the information to have on hand to configure a Scanner for outbound mail filtering.

Table 1-4 Outbound mail filtering checklist

Completed	Item	Description	Details
_____	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: _____
_____	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: _____

Table 1-5 provides the information to have on hand to configure a Scanner for instant message filtering.

Table 1-5 Instant message filter configuration checklist

Completed	Item	Description	Details
_____	Outbound IM interface	The address is used for routing internal IM traffic. You can specify up to two addresses. The secondary IP address routes AOL file transfers through the Scanner and must be a different IP address from the primary IP address.	Ethernet interface for IM filtering: _____ Outbound IP addresses: 1. _____ 2. _____

Table 1-5 Instant message filter configuration checklist *(continued)*

Completed	Item	Description	Details
_____	Inbound IM interface	The inbound Ethernet network interface may be the same as the outbound interface. If you use different network interface cards for incoming traffic and outgoing traffic, assign different IP addresses to the primary outbound address and the inbound address.	Ethernet interface to communicate with public servers: _____ Inbound IP address: _____

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 1-6 provides some examples of the port configurations that you can use (it does not include all IP address and port possibilities).

Table 1-6 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 1-6 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 use two different IP addresses, one of which is virtual. (A virtual IP address is required for Scanners if you intend to filter instant messaging.) 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. (However, an additonal, virtual IP address is required for Scanners if you intend to filter instant messaging.) This configuration can result in network bottlenecks, but is suitable for sites with relatively low email traffic.

Ports that Symantec Brightmail Gateway uses

Table 1-7 lists the ports that Symantec Brightmail 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 Brightmail Gateway filtering depends on constant updates from the Symantec Global Intelligence Network. In order to maintain the usefulness of your appliance, it is crucial that you facilitate automated communications between the appliance and Symantec.

Table 1-7 Ports to open in your network for Symantec Brightmail 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	Scanners	Internal mail servers	IM user self-registration	
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	
80	TCP	IM clients	Scanners with IM filtering	Yahoo! Messenger	This port is used for instant messaging file transfers.
80	TCP	Scanners with IM filtering	Internet	Yahoo! Messenger	This port is used for instant messaging file transfers.

Table 1-7 Ports to open in your network for Symantec Brightmail Gateway *(continued)*

Port	Protocol	Origin	Destination	Description	Notes
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.
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.
443	TCP	IM clients	Internet	HTTPS connection from Google Talk, MSN Messenger, and Yahoo! Messenger clients for user authentication	
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.
1863	TCP	IM clients	Scanners with IM filtering	MSN Messenger	This port is used for instant messaging and instant messaging file transfers.
1863	TCP	Scanners with IM filtering	Internet	MSN Messenger	This port is used for instant messaging and instant messaging file transfers.

Table 1-7 Ports to open in your network for Symantec Brightmail Gateway *(continued)*

Port	Protocol	Origin	Destination	Description	Notes
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.
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		Web management port for the Control Center.
41443	TCP	Your management hosts	Control Center	Control Center Web management interface (HTTPS)	
5050	TCP	IM clients	Scanners with IM filtering	Yahoo! Messenger	This port is used for instant messaging.
5050	TCP	Scanners with IM filtering	Internet	Yahoo! Messenger	This port is used for instant messaging.

Table 1-7 Ports to open in your network for Symantec Brightmail Gateway *(continued)*

Port	Protocol	Origin	Destination	Description	Notes
5190 - 5192, 5290 - 5292	TCP	IM clients	Scanners with IM filtering	AOL Instant Messenger (AIM)	This port is used for instant messaging.
5190	TCP	Scanners with IM filtering	Internet	AOL Instant Messenger (AIM)	This port is used for instant messaging and instant messaging file transfers.
5193, 5194	TCP	IM clients	Scanners with IM filtering	AOL Instant Messenger (AIM)	This port is used for instant messaging file transfers.
5222	TCP	IM clients	Scanners with IM filtering	Google Talk	This port is used for instant messaging. (Google Talk does not support instant messaging file transfer.)
5222	TCP	Scanners with IM filtering	Internet	Google Talk	This port is used for instant messaging. (Google Talk does not support instant messaging file transfer.)

Required ports

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

Table 1-8 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.

Table 1-8 Required ports *(continued)*

Protocols needed	Name	Protocol	Default port	Notes
Access to the Control Center and outbound access to external Internet	HTTP	TCP	80	See "Ports that Symantec Brightmail Gateway uses" on page 22.
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)

About the DNS servers required for IM filtering

If you want to use Symantec Brightmail Gateway to filter IM traffic, the following types of DNS servers are required:

- DNS accessed by the internal hosts that routes internal IM traffic to a Scanner for filtering
- DNS accessed by Scanners that routes outgoing IM traffic to public IM networks on the Internet

Changes to your firewall are also required for IM filtering.

See "Ports that Symantec Brightmail Gateway uses" on page 22.

System requirements

Table 1-9 lists the minimal system requirements.

See "System requirements for virtual deployment" on page 68.

Table 1-9 System requirements

Item	Requirement
Web browsers	The Control Center supports the following browsers: ■ Microsoft Internet Explorer 6, 7, and 8 ■ Mozilla Firefox 3 and 3.5
LDAP	Symantec Brightmail Gateway supports the following LDAP directory types: ■ Windows 2008 Active Directory (both LDAP and Global Catalog) ■ Windows 2003 Active Directory (both LDAP and Global Catalog) ■ Windows 2000 Active Directory (both LDAP and Global Catalog) ■ Sun Directory Server 6.3 ■ Sun Directory Server 6.0 ■ Sun Directory Server 5.2 (formerly known as iPlanet, SunONE, and Java directory servers) ■ Lotus Domino LDAP Server 8.5 ■ Lotus Domino LDAP Server 8.0 ■ Lotus Domino LDAP Server 7.0 ■ Lotus Domino LDAP Server 6.5 ■ OpenLDAP 2.4 ■ OpenLDAP 2.3 ■ OpenLDAP 2.2 Symantec Brightmail Gateway is LDAP v.3 compliant and can be configured to work with other directory server types. Refer to the *Symantec Brightmail Gateway Administration Guide* for more information about how to configure Symantec Brightmail Gateway for use with LDAP.

Features that can affect performance

Table 1-10 describes how features might affect performance and how to off-set the performance demands.

Table 1-10 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 (split 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.
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.
Logs	The higher the log levels, the more data the Control Center must consolidate over the network. Consider keeping log levels relatively low unless you are troubleshooting. You can also set logs to be purged more frequently.
Reports	Configure scheduled reports to run at times when utilization 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.
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 1-10 Features that can affect performance *(continued)*

Feature	How performance can be affected
Spam Quarantine	The following are Spam Quarantine performance implications: ■ The more messages that Symantec Brightmail Gateway routes to Spam Quarantine, the larger the Quarantine becomes, and the more processing that is required. Reduce the maximum size of Spam Quarantine. You can delete the messages that are identified as spam or reduce spam retention time. ■ The more users that access Spam Quarantine, the more performance overhead that is required. Not allowing end user access to Spam Quarantines ca increase performance significantly. ■ LDAP lookups for message recipients against a limited capacity LDAP server can severely impair Spam Quarantine performance. Ensure that you have adequate capacity on your LDAP server. ■ 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.
DKIM signing	Enabling DKIM signing can impact outbound messaging performance. Using a shorter encryption key can reduce this impact.
SMTP authentication	SMTP authentication adds overhead that can impact outbound messaging performance.

For more information about these topics, see the *Symantec Brightmail Gateway Administration Guide*.

Chapter 2

Installing the Symantec Brightmail Gateway product

This chapter includes the following topics:

Installing the Symantec Brightmail Gateway product

Before you install Symantec Brightmail Gateway, ensure that you have reviewed and completed the preinstallation tasks.

See "Before you install" on page 12.

After you successfully complete installation, perform the post-installation tasks.

See "Post-installation tasks" on page 79.

Table 2-1 Symantec Brightmail Gateway installation process

Step	Task and description
1	Unpack the appliance, mount it, and connect the appropriate cables to the appliance box. See "Setting up the appliance hardware" on page 33.
2	Turn on the appliance. The setup wizard guides you through the setup process. See "Starting the appliance software set up" on page 34.
3	Specify the Ethernet settings. See "Specifying Ethernet interfaces" on page 34.

Table 2-1 Symantec Brightmail Gateway installation process *(continued)*

Step	Task and description
4	Specify static IP address for routing. This step is optional. See "Specifying a static IP address for routing" on page 35.
5	Specify the IP addresses for the default gateway and your DNS servers. See "Specifying gateway and DNS IP addresses" on page 36.
6	Specify the role for the appliance. See "Specifying the role for the appliance" on page 37.
7	Register your license. See "Registering your license" on page 38.
8	Update the product with the latest software. See "Updating to the latest software during initial setup" on page 40.
9	Set up and configure the Control Center. See "Configuring the Control Center" on page 41.
10	Set up the Scanner. Set up your Scanner based on one of the following scenarios: ■ The Scanner is on the same appliance as the Control Center. After the setup wizard guides you through the process to setup the Control Center, it automatically begins the process to add a Scanner. See "Configuring the Control Center" on page 41. ■ The Scanner is on different appliance than the Control Center. Install Scanners on a different appliance from the Control Center through the Control Center. See "About adding a Scanner through the Control Center" on page 43.

Table 2-1 Symantec Brightmail Gateway installation process *(continued)*

Step	Task and description
11	After you set up your Scanner, configure it based on its intended function, as follows: See "Configuring the Scanner for inbound and outbound mail filtering" on page 46. See "Configuring the Scanner for inbound mail filtering only" on page 50. See "Configuring the Scanner for outbound mail filtering only" on page 52. See "Configuring the Scanner for inbound mail filtering with instant message filtering" on page 54. See "Configuring the Scanner for outbound mail filtering with instant message filtering" on page 58. See "Configuring the Scanner for inbound and outbound mail filtering with instant message filtering" on page 61.

Setting up the appliance hardware

Before you can install and configure the appliance, you must first set up the hardware.

See "Installing the Symantec Brightmail Gateway product" on page 31.

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 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 Ethernet jack that is labeled **1** on the back panel of the appliance, which corresponds to eth0.

   To use the second Ethernet port for outbound traffic, connect a second cable to the Ethernet jack that is labeled **2** on the back of the appliance and corresponds to eth1.

   See "Starting the appliance software set up" on page 34.

Starting the appliance software set up

After you set up the appliance hardware, begin the software set up process.

See "Setting up the appliance hardware" on page 33.

See "Installing the Symantec Brightmail Gateway product" on page 31.

To start the appliance software set up

1. Turn on the power.
2. Log on with the logon name `admin` and the password `symantec`.
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, this host name should not be your mail domain, such as symantecexample.com.

   For example, the name should be similar in form to:

   ```
   host6.symantecexample.com
   ```

5. When you are prompted, type the correct time zone.

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

   Press the space bar to scroll through the list or type **Q** to exit the list.
6. To continue installation, next you specify Ethernet interfaces.

   See "Specifying Ethernet interfaces" on page 34.

Specifying Ethernet interfaces

After you perform the initial steps of starting the appliance setup, the next step is to configure the Ethernet interfaces.

See "Starting the appliance software set up" on page 34.

See "Installing the Symantec Brightmail Gateway product" on page 31.

To specify Ethernet interfaces

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

   For example:

   ```
   192.168.0.1
   ```

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

   For example:

   ```
   255.255.255.0
   ```

3. When you are prompted if you want to use the second Ethernet interface, interface 2, type one of the following responses:

YES	You want to use interface 2.
NO	You do not want to use interface 2. Skip to the next procedure. See "Specifying a static IP address for routing" on page 35.

4. When you are prompted, type the IP address for Ethernet interface 2.

   For example:

   ```
   192.168.12.3
   ```

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

   For example:

   ```
   255.255.255.0
   ```

6. To continue installation, next you specify a static IP address for routing.

   See "Specifying a static IP address for routing" on page 35.

Specifying a static IP address for routing

After you set up the Ethernet interfaces, the next step in setting up your appliance is to set up a static IP address for routing. You can set up multiple static IP addresses or none at all.

See "Specifying Ethernet interfaces" on page 34.

See "Installing the Symantec Brightmail Gateway product" on page 31.

To specify a static IP address static for routing

1 When you are prompted whether you want to add a static IP address for routing, type one of the following responses:

YES	You want to add a static IP address for routing.
NO	You do not want to add a static IP address for routing. Skip to the next procedure. See "Specifying gateway and DNS IP addresses" on page 36.

2 When you are prompted, specify the IP address or CIDR block of the destination host or network.

3 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.

4 When you are prompted whether you want to add another static IP address, type one of the following responses:

YES	You want to add another static IP address. Repeat steps 2 through 3 to add another static IP address.
NO	You do not want to add another static IP address. Skip to the next procedure. See "Specifying gateway and DNS IP addresses" on page 36.

5 To continue installation, next you specify gateway and DNS IP addresses.

See "Specifying gateway and DNS IP addresses" on page 36.

Specifying gateway and DNS IP addresses

After you configure the static IP address, specify the default gateway IP address and the IP address of your DNS server. You can add up to three DNS server IP addresses.

See "Specifying a static IP address for routing" on page 35.

See "Installing the Symantec Brightmail Gateway product" on page 31.

To specify gateway and DNS settings

1. When you are prompted, type the IP address of the default gateway (default router).
2. When you are prompted, type the IP address of the DNS server.
3. When you are prompted if you want to enter another DNS server, type one of the following responses:

YES	You want to add an additional DNS server. Type the IP address. You can add up to three addresses.
NO	You do not want to an additional DNS server. Skip to the next procedure. See "Specifying the role for the appliance" on page 37.

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

   See "Specifying the role for the appliance" on page 37.

Specifying the role for the appliance

After you have specified IP addresses for your default gateway and DNS servers, specify the role for the appliance.

See "Specifying gateway and DNS IP addresses" on page 36.

See "Installing the Symantec Brightmail Gateway product" on page 31.

The roles that you can choose are as follows:

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

See "About the appliance's functions" on page 13.

To set the role for the appliance

1. When you are prompted, choose one of the following roles for this appliance:
   - Scanner only

- Control Center only
- Scanner and Control Center

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

3 When you are prompted whether the summary information is correct, type one of the following responses:

YES	The summary information is correct. Product setup is complete and the appliance restarts. After the appliance restarts, you can register your appliance. See "Registering your license" on page 38.
NO	The summary information is not correct. You return to the beginning of the process to make your changes. See "Starting the appliance software set up" on page 34.

Registering your license

To register your license, you need the license file that Symantec provides you. 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. However, 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 Brightmail Gateway communicates with Symantec Security Response over a secure connection for product registration and ongoing operations.

If you are performing the initial setup of your appliance, these steps appear in the setup wizard after the appliance restarts.

See "Specifying the role for the appliance" on page 37.

See "Installing the Symantec Brightmail Gateway product" on page 31.

To register your license

1. From a computer that can access your appliance, locate the appliance in a browser.

   The default logon address is as follows:

   https://<hostname>

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

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

   See the *Symantec Brightmail Gateway Administration Guide* for information about the `http` command.
2. When the security alert message appears, accept the self-signed certificate to continue.
3. On the Control Center logon page, log on as user `admin` and use the password that you specified set during initial setup.
4. On the **End-User License Agreement** page, click **I accept the terms of the license agreement** and click **Next**.
5. On the **License Information Registration** page, click **Browse** to locate your license file.
6. Select your license file and click **Open** to return to the **License Registration** page.
7. If your Scanner uses a proxy server for communications with Symantec, click **Proxy Server**.
8. 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.
9. Click **Register License**.

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

   See "Troubleshooting license file registration" on page 40.

   Registration may fail because of an inaccessible proxy, closed port 443, or an expired, missing, or corrupt license file.

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.

See "Configuring the Control Center" on page 41.

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

See "Updating to the latest software during initial setup" on page 40.

Troubleshooting license file registration

If you have difficulty installing a license during installation, the installation wizard lets you troubleshoot the issue with the Traceroute utility or the Ping utility.

Troubleshooting license file registration

1 On the License Information Registration page, click **Utilities**.

2 In the **Utility** field, click the drop-down menu and select whether to use **Traceroute** or **Ping**, and then in the **Host name or IP address** field, type the host name or IP address.

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

3 Click **Run**.

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

4 Click **Register License**.

5 Complete registration.

See "Registering your license" on page 38.

Updating to the latest software during initial setup

Symantec recommends that you apply the current software update after you register the product, if one is available.

See "Registering your license" on page 38.

See "Installing the Symantec Brightmail Gateway product" on page 31.

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 "Configuring the Control Center" on page 41.
Cancel	Returns you to the **License Registration** page.
Back	See "Registering your license" on page 38.

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

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

3 To continue installation, next you configure the Control Center.

See "Configuring the Control Center" on page 41.

Configuring 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 "Registering your license" on page 38.

See "Updating to the latest software during initial setup" on page 40.

See "Installing the Symantec Brightmail Gateway product" on page 31.

Configure the Control Center before you configure any Scanners. If you specified that this appliance is a Control Center and a Scanner, the wizard continues with the Scanner set up after the Control Center set up finishes.

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 Brightmail Gateway send alerts to this address. You can add additional administrators or modify this administrator's settings in the Control Center later.

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 Brightmail Gateway uses for messages.

7 Select a **Quarantine fallback encoding** format.

Fallback encoding is the formatting that the product 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, and you must define your Scanner role.

See "Configuring the Scanner for inbound and outbound mail filtering" on page 46.

See "Configuring the Scanner for inbound mail filtering only" on page 50.

See "Configuring the Scanner for outbound mail filtering only" on page 52.

See "Configuring the Scanner for inbound mail filtering with instant message filtering" on page 54.

See "Configuring the Scanner for outbound mail filtering with instant message filtering" on page 58.

See "Configuring the Scanner for inbound and outbound mail filtering with instant message filtering" on page 61.

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. This option is the default setting.
Back	You want to modify your settings.
Cancel	You want to end the setup without saving your 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 "Adding a Scanner through the Control Center" on page 44.

About adding a Scanner through the Control Center

If you configure your appliance as a Control Center and Scanner, you set up the Scanner during the initial appliance setup. If the Scanner is separate from the Control Center or you want to add a Scanner at any time after installation, do so through the Control Center.

See "Installing the Symantec Brightmail Gateway product" on page 31.

Table 2-2 lists the steps to add a Scanner through the Control Center.

Table 2-2 How to add a Scanner

Step	Task description
1	Use the **Add Scanner** setup wizard in the Control Center to add a Scanner. See "Adding a Scanner through the Control Center" on page 44.

Table 2-2 How to add a Scanner *(continued)*

Step	Task description
2	When you finish adding a new Scanner, configure it based on the Scanner's intended function. See "Configuring the Scanner for inbound and outbound mail filtering" on page 46. See "Configuring the Scanner for inbound mail filtering only" on page 50. See "Configuring the Scanner for outbound mail filtering only" on page 52. See "Configuring the Scanner for inbound mail filtering with instant message filtering" on page 54. See "Configuring the Scanner for outbound mail filtering with instant message filtering" on page 58. See "Configuring the Scanner for inbound and outbound mail filtering with instant message filtering" on page 61.
3	If you enable end-user preferences, manually trigger user preferences replication after you add a new Scanner. Wait until the replication completes before you let mail be sent to the new Scanner. See the *Symantec Brightmail Gateway Administration Guide* for more information.
4	Check the status of the Scanner to ensure that it functions properly. See the *Symantec Brightmail Gateway Administration Guide* for more information.

Adding a Scanner through the Control Center

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 not final until you click **Finish** at the end of the wizard.

See "About adding a Scanner through the Control Center" on page 43.

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**.
3. On the **Add Scanner Wizard** page, click **Next**.
4. On the **Scanner Host Settings** page, do all of the following:
   - In the **Host description** box, type a description for the new Scanner.
   - In the **Host name or IP address** box, type the host name or IP address for the new Scanner.
5. Click **Next**.
6. On the **License Registration** page, click **Browse** to locate your license file.
7. Select your license file and click **Open** to return to the **License Registration** page.
8. If your Scanner uses a proxy server for communications with Symantec, click **Proxy Server**.
9. To specify a proxy server, check **Use HTTP Proxy** and type the server host name and port.
10. Click **Register License**.

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

    If the license registration fails, perform troubleshooting steps.

    See "Troubleshooting license file registration" on page 40.
11. If you have another license file for a different feature, repeat the process for registering each license.
12. When all the license files are successfully registered, click **Next**.

    If your software needs to be updated, the **Software Update** page appears. If not, proceed to step 14.

13 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 returns you to the **Time Settings** page.
Cancel	Returns you to the **License Registration** page. See "Registering your license" on page 38.

14 On the **Time Settings** page, verify whether the date 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. Click and provide the IP address for up to three NTP servers.

15 To complete the **Add Scanner** wizard, you must now configure the Scanner based on its function.

See "Configuring the Scanner for inbound and outbound mail filtering" on page 46.

See "Configuring the Scanner for inbound mail filtering only" on page 50.

See "Configuring the Scanner for outbound mail filtering only" on page 52.

See "Configuring the Scanner for inbound mail filtering with instant message filtering" on page 54.

See "Configuring the Scanner for outbound mail filtering with instant message filtering" on page 58.

See "Configuring the Scanner for inbound and outbound mail filtering with instant message filtering" on page 61.

Configuring the Scanner for inbound and outbound mail filtering

You can configure the Scanner to perform both inbound mail filtering and outbound mail filtering. You can use the same Ethernet interface for both inbound mail filtering and outbound mail filtering. Or you can create a virtual IP address to use for either inbound or outbound mail filtering.

See "Sample Scanner port configurations" on page 21.

To configure the Scanner for inbound and outbound mail filtering

1. On the **Scanner Role** page, click **Inbound and Outbound mail filtering** then click **Next**.
2. On the **Create Optional Virtual IP Address** page, select one of the following options:

Yes	You want to create a Virtual IP address.
No	You do not want to create a Virtual IP address. Proceed to step 6.

3. Click **Next**.
4. On the **Create Virtual IP Address** page, do all of the following tasks:

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

5. Click **Next**.
6. On the **Inbound Mail Filtering** page, click **Inbound mail IP address** to select the IP address to use for inbound mail filtering.
7. In the **Inbound mail SMTP port** field, type the port, and then click **Next**.

8 On the **Inbound Mail Filtering - Accepted Hosts** page, to specify the IP addresses of the mail servers from which this Scanner should accept inbound mail, select one of the following options:

All IP addresses	You want your Scanner to accept mail from all sources or the Scanner is deployed at the gateway. For a Scanner deployed at the Internet gateway, Symantec recommends that you select this option to accept mail from any MTA on the Internet.
Specific IP Addresses	You want to restrict the domains from which your Scanner accepts mail. Type IP addresses, CIDR ranges, or domains. If the Scanner is deployed behind upstream mail servers, specify the upstream mail servers.

9 Click **Next**.

10 On the **Local Domains** page, check the addresses that you want to accept inbound mail for in the **Local Domains** list.

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 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.

11 Click **Next**.

12 On the **Outbound Mail Filtering** page, click the drop-down list to select the IP address to use for outbound mail filtering.

13 In the **Outbound mail SMTP port** field, type the port, and click **Next**.

14 On the **Outbound Mail Filtering - Accepted Hosts** page, do one of the following tasks:

- Specify the internal host to which this Scanner should relay local domain mail after filtering is complete. This server is typically a downstream mail server, such as your corporate mail server.
- Check **Enable MX Lookup for this host**. If you enable MX lookup, specify a host name instead of an IP address.

15 Click **Next**.

16 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.

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

18 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.

19 Click **Next**.

20 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.

Configuring the Scanner for inbound mail filtering only

You can configure the Scanner to only filter inbound email.

See "Sample Scanner port configurations" on page 21.

To configure the Scanner for inbound mail filtering only

1. On the **Scanner Role** page, click **Inbound mail filtering** and click **Next**.
2. On the **Inbound Mail Filtering** page, click the drop-down list to select the IP address to use for inbound mail filtering.
3. In the **Inbound mail SMTP port** field, type the port, and then click **Next**.
4. On the **Inbound Mail Filtering - Accepted Hosts** page, to specify the IP addresses of the mail servers from which this Scanner should accept inbound mail, select one of the following options:

All IP addresses	You want your Scanner to accept mail from all sources or the Scanner is deployed at the Internet gateway. For a Scanner that is deployed at the Internet gateway, Symantec recommends that you select this option to let the appliance accept mail from any MTA on the Internet.
Specific IP Addresses	You want to restrict the domains from which your Scanner should accept mail. Type the IP addresses or host names. If the Scanner is deployed behind one or more upstream mail servers, specify the upstream mail servers.

5. Click **Next**.
6. On the **Inbound Mail Filtering - Mail Delivery** page, do one of the following tasks:
   - In the **Host name or IP address** field, type the host where the Scanner should relay inbound mail after filtering is complete and in the **Port** field, type the port.
     This server is typically a downstream mail server, such as your corporate mail server.
   - Check **Enable MX Lookup for this host**.
     If you enable MX lookup, specify a host name instead of an IP address.
7. Click **Next**.

8 On the **Inbound 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 in the required fields. Symantec also recommends that you check **Enable MX lookup for this host** if you position the Scanner at the Internet gateway. If you choose this option, specify a host name (not an IP address) for that server.
Use an existing host	You want to use an existing host. Select an existing 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.

9 Click **Next**.

10 On the **Local Domains** page, check the addresses that you want in the **Local Domains** list. Include all domains for which you want to accept incoming mail.

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** 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 that 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.

11 Click **Next**.

12 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.

Configuring the Scanner for outbound mail filtering only

You can configure the Scanner to only filter outbound email.

See "Sample Scanner port configurations" on page 21.

To configure the Scanner for outbound mail filtering only

1. On the **Scanner role** page, click **Outbound Mail Filtering** and click **Next**.
2. On the **Outbound Mail Filtering** page, click the drop-down list to select the IP address to use for outbound mail filtering.
3. In the **Outbound mail SMTP port** field, type the port, and then click **Next**.
4. On the **Outbound Mail Filtering - Accepted Hosts** page, in the **Available IP Addresses/Domains** list, select the IP addresses from which the Scanner should accept mail for outbound filtering.

   To add a new IP address or domain, type the new IP address in the **IP addresses/domains** field and click **Add**.
5. After you add and select all of your IP addresses and domains, click **Next**.
6. On the **Outbound Mail Filtering - Mail Delivery** page, do one of the following tasks:
   - In the **Host name or IP address** field, type the host where the Scanner should relay outbound mail after filtering is complete and in the **Port** field, type the port.
     This server is typically a downstream mail server, such as your corporate mail server.
   - Check **Enable MX Lookup for this host**.
     If you enable MX lookup, specify a host name instead of an IP address.
7. Click **Next**.

8 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 in the required fields. Symantec also recommends that you check **Enable MX lookup for this host** if you position the Scanner at the Internet gateway. If you choose this option, specify a host name (not an IP address) for that server.
Use an existing host	You want to use an existing host. Select an existing host from the drop-down list. If a separate gateway MTA is configured between the Scanner and the Internet, provide that MTA's host name or IP address and port.

9 Click **Next**.

10 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.

Configuring the Scanner for inbound mail filtering with instant message filtering

You can configure the Scanner to filter inbound email and instant message filtering. When you do, you must have more than one Ethernet interface. To meet this requirement, the setup wizard lets you create a virtual IP address.

See "Sample Scanner port configurations" on page 21.

To configure the Scanner for inbound mail filtering with instant message filtering

1. On the **Scanner Role** page, click **Inbound Mail filtering**, check **Instant message filtering**, and then click **Next**.
2. On the **Create Virtual IP Address** page, do all of the following tasks:

Ethernet	Click the drop-down list 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.

3. Click **Next**.
4. On the **Inbound Mail Filtering** page, click the drop-down menu to select the IP address to use for inbound mail filtering.
5. In the **Inbound mail SMTP port** field, type the port, and then click **Next**.
6. On the **Inbound Mail Filtering - Accepted Hosts** page, to specify the IP addresses of the mail servers from which this Scanner should accept inbound mail, select one of the following options:

All IP addresses	You want your Scanner to accept mail from all sources or the Scanner is deployed at the Internet gateway. For a Scanner that is deployed at the Internet gateway, Symantec recommends that you select this option to let the appliance accept mail from any MTA on the Internet.
Specific IP Addresses	You want to restrict the domains from which your Scanner should accept mail. Type the IP addresses or host names. If the Scanner is deployed behind one or more upstream mail servers, specify the upstream mail servers.

7. Click **Next**.
8. On the **Inbound Mail Filtering - Mail Delivery** page, do one of the following tasks:

- In the **Host name or IP address** field, type the host where the Scanner should relay inbound mail after filtering is complete and in the **Port** field, type the port.
  This server is typically a downstream mail server, such as your corporate mail server.
- Check **Enable MX Lookup for this host**.
  If you enable MX lookup, specify a host name instead of an IP address.

9 Click **Next**.

10 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 in the required fields. Symantec also recommends that you check **Enable MX lookup for this host** if you position the Scanner at the Internet gateway. If you choose this option, specify a host name (not an IP address) for that server.
Use an existing host	You want to use an existing host. Select an existing 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.

11 Click **Next**.

12 On the **Local Domains** page, check the addresses that you want in the **Local Domains** list.

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** 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 that 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.

13 Click **Next**.

14 On the **Configure IM interfaces** page, under **Outbound IM Interface**, click the **Ethernet** drop-down list to select an Ethernet network interface for internal IM filtering.

15 Click the **Outbound IP address** drop-down list to select an outbound IP address.

The outbound IP address is for routing internal IM traffic.

16 Click the **Secondary IM IP address** drop-down list to select a secondary IM IP address.

The secondary IP address routes AOL file transfers through the Scanner and must be a different IP address from the primary IP address.

17 Under **Inbound IM Interface**, click the **Ethernet** drop-down list to select the Ethernet network interface that IM clients use to communicate with public servers.

The inbound Ethernet network interface may be the same as the outbound interface.

18 Click the **Inbound IP address** drop-down list to select an inbound IP address.

If you use different network interface cards for incoming traffic and outgoing traffic, assign different IP addresses to the primary outbound address and the inbound address.

19 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.

Configuring the Scanner for outbound mail filtering with instant message filtering

You can configure the Scanner to filter outbound email and instant message filtering. When you do, you must have more than one Ethernet interface. To meet this requirement, the setup wizard lets you create a virtual IP address.

See "Sample Scanner port configurations" on page 21.

To configure the Scanner for outbound mail filtering with instant message filtering

1. In the **Scanner Role** page, click **Outbound mail filtering**, check **Instant message filtering**, and then click **Next**.
2. On the **Create Virtual IP Address** page, do all of the following tasks:

Ethernet	Click the drop-down list 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.

3. Click **Next**.
4. On the **Outbound Mail Filtering** page, click the drop-down list to select the IP address to use for outbound mail filtering.
5. In the **Outbound mail SMTP port** field, type the port, and then click **Next**.
6. On the **Outbound Mail Filtering - Accepted Hosts** page, in the **Available IP addresses/domains** list, select the IP addresses from which the Scanner should accept mail for outbound filtering.

   To add a new IP address or domain, type the new IP address in the **IP addresses/domains** field and click **Add**.
7. After you add and select all of your IP addresses and domains, click **Next**.
8. On the **Outbound Mail Filtering - Mail Delivery** page, do one of the following tasks:
   - In the **Host name or IP address** field, type the host where the Scanner should relay outbound mail after filtering is complete and in the **Port** field, type the port.
     This server is typically a downstream mail server, such as your corporate mail server.
   - Check **Enable MX Lookup for this host**.
     If you enable MX lookup, specify a host name instead of an IP address.
9. Click **Next**.

10 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 in the required fields. Symantec also recommends that you check **Enable MX lookup for this host** if you position the Scanner at the Internet gateway. If you choose this option, specify a host name (not an IP address) for that server.
Use an existing host	You want to use an existing host. Select an existing 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.

11 Click **Next**.

12 On the **Configure IM interfaces** page, under **Outbound IM Interface**, click the **Ethernet** drop-down list to select an Ethernet network interface for internal IM filtering.

13 Click the **Outbound IP address** drop-down list to select an outbound IP address.

The outbound IP address is for routing internal IM traffic.

14 Click the **Secondary IM IP address** drop-down list to select a secondary IM IP address.

The secondary IP address routes AOL file transfers through the Scanner and must be a different IP address from the primary IP address.

15 Under **Inbound IM Interface**, click the **Ethernet** drop-down list to select the Ethernet network interface that IM clients use to communicate with public servers.

The inbound Ethernet network interface may be the same as the outbound interface.

16 Click the **Inbound IP address** drop-down list to select an inbound IP address.

If you use different network interface cards for incoming traffic and outgoing traffic, assign different IP addresses to the primary outbound address and the inbound address.

17 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.

Configuring the Scanner for inbound and outbound mail filtering with instant message filtering

You can configure the Scanner to filter inbound email, outbound email, and instant messages. When you do, you must have more than one Ethernet interface. To meet this requirement, the setup wizard lets you create a virtual IP address.

See "Sample Scanner port configurations" on page 21.

To configure the Scanner for inbound and outbound mail filtering with instant message filtering

1 On the **Scanner Role** page, click **Inbound and Outbound mail filtering**, check the **Instant message filtering**, and then click **Next**.

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

Ethernet	Click the drop-down list 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.

3 Click **Next**.

4. On the **Inbound Mail Filtering** page, type an IP address and port to use to filter inbound mail.
5. Click **Next**.
6. On the **Inbound Mail Filtering - Accepted Hosts** page, to specify the IP addresses of the mail servers from which this Scanner accepts inbounds mail, select one of the following options:

All IP addresses	You want your Scanner to accept mail from all sources. For a Scanner that is deployed at the Internet gateway, Symantec recommends that you select this option to let the appliance accept mail from any MTA on the Internet.
Specific IP Addresses	You want to restrict the domains from which your Scanner should accept mail. Type the IP addresses or host names. If the Scanner is deployed behind one or more upstream mail servers, specify the upstream mail servers.

7. Click **Next**.

8 On the **Local Domains** page, check the addresses that you want in the **Local Domains** list.

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 that 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.

9 Click **Next**.

10 On the **Outbound Mail Filtering** page, click the drop-down list to select the IP address to use for outbound mail filtering.

11 In the **Outbound mail SMTP port** field, type the port, and then click **Next**.

12 On the **Outbound Mail Filtering - Accepted Hosts** page, in the **Available IP addresses/domains** list, select the IP addresses from which the Scanner should accept mail for outbound filtering.

To add a new IP address or domain, type the new IP address in the **IP addresses/domains** field and click **Add**.

13 After you added and select all of your IP addresses and domains, click **Next**.

14 On the **Outbound Mail Filtering - Mail Delivery** page, do one of the following tasks:

- In the **Host name or IP address** field, type the host where the Scanner should relay outbound mail after filtering is complete and in the **Port** field, type the port.

This server is typically a downstream mail server, such as your corporate mail server.

- Check **Enable MX Lookup for this host**.
  If you enable MX lookup, specify a host name instead of an IP address.

15 Click **Next**.

16 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 in the required fields. Symantec also recommends that you check **Enable MX lookup for this host** if you position the Scanner at the Internet gateway. If you choose this option, specify a host name (not an IP address) for that server.
Use an existing host	You want to use an existing host. Select an existing host from the drop-down list. If a separate gateway MTA is configured between the Scanner and the Internet, provide that MTA's host name or IP address and port.

17 Click **Next**.

18 On the **Configure IM interfaces** page, under **Outbound IM Interface** , click the **Ethernet** drop-down list to select an Ethernet network interface for internal IM filtering.

19 Click the **Outbound IP address** drop-down list to select an outbound IP address.

The outbound IP address is for routing internal IM traffic.

20 Click the **Secondary IM IP address** drop-down list to select a secondary IM IP address.

The secondary IP address routes AOL file transfers through the Scanner and must be a different IP address from the primary IP address.

21 Under **Inbound IM Interface**, click the **Ethernet** drop-down list to select the Ethernet network interface that IM clients use to communicate with public servers.

The inbound Ethernet network interface may be the same as the outbound interface.

22 Click the **Inbound IP address**drop-down list to select an inbound IP address.

If you use different network interface cards for incoming traffic and outgoing traffic, assign different IP addresses to the primary outbound address and the inbound address.

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 3

Installing Symantec Brightmail Gateway Virtual Edition

This chapter includes the following topics:

About Symantec Brightmail Gateway Virtual Edition

Use Symantec Brightmail Gateway Virtual Edition with VMware to create a simulated computer environment (a virtual computer) on which to run Symantec Brightmail Gateway. The guest software is a complete operating system that

contains the Symantec Brightmail Gateway Virtual Edition software. It runs in a similar manner to the application as installed on a standalone hardware platform.

You can deploy the Symantec Brightmail Gateway as a virtual appliance on your existing VMware infrastructure in one of the following ways:

- See "Deploying an OVF template on an ESX 3.5 or ESXi 3.5 Server" on page 69.
- See "Deploying an OVF template on an ESX 4.0 or ESXi 4.0 Server" on page 71.
- See "Installing from an ISO image or OS restore CD onto a virtual machine on your ESX or ESXi Server" on page 72.

The resources that are allocated to Symantec Brightmail Gateway Virtual Edition must meet the minimum requirements.

See "System requirements for virtual deployment" on page 68.

This documentation assumes the following:

- Your environment has an existing VMware ESX or ESXi Server deployment.
- You are familiar with administering virtual computers.
- Your environment meets all pre-requisite system requirements.

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

See "Virtual software terminology" on page 77.

Note: After you complete installing your virtual appliance, you must complete additional tasks to install and register Symantec Brightmail Gateway software on your virtual appliance. During registration you will be asked agree to the End User License Agreement. You will not be able to proceed with registration without agreeing.

System requirements for virtual deployment

Table 3-1 lists the system requirements to deploy Symantec Brightmail Gateway as a guest on VMware ESX Server and VMware ESXi Server. You must have already installed and configured one of these servers before you install Symantec Brightmail Gateway Virtual Edition.

For requirements specific to VMware ESX Server and VMware ESXi Server, refer to your VMware documentation.

Table 3-1 Supported Configurations for Symantec Brightmail Gateway Virtual Edition

Description	Recommended	Minimum	Notes
VMware ESX Server	Version 4.0	Version 3.5, update 4	—
VMware ESXi Server version	Version 4.0	Version 3.5, update 4	—
Disk space	For more information, consult the Symantec Knowledge Base article, *Disk Space Recommendations for Symantec Brightmail Gateway Virtual Edition*	90 GB 90 GB 90 GB	For Scanner-only virtual machines. For Control Center–only virtual machines. For combined Scanner and Control Center virtual machines.
Memory	4 GB	2 GB	A minimum of 2 GB is necessary to run Symantec Brightmail Gateway and the virtual machine.
CPUs	4	2	ESX Server 3.5 and ESXi Server 3.5 are limited to two virtual CPUs per virtual machine. Symantec recommends allocating up to four, based on workload demands and hardware configuration.
NICs	1	1	Only one network interface card is required per virtual machine.

Deploying an OVF template on an ESX 3.5 or ESXi 3.5 Server

You can deploy an OVF template that contains Symantec Brightmail Gateway Virtual Edition on a VMware ESX Server 3.5 or VMWare ESXi Server 3.5. An OVF

template is a virtual machine that includes the software you plan to run on the machine.

To use an OVF template to install Symantec Brightmail Gateway on an ESX 3.5 or ESXi 3.5 Server, use the VMware vCenter Converter to import the OVF template.

The VMware vCenter Converter is available on the VMware Web site. The steps described here are based on using Version 4.0.1, build 161434 of the VMware vCenter Converter on an ESX 3.5, update 4 Server. Note that these instructions may vary based on the version and build of the converter that you use. Version 3.x converters do not support OVF templates. Refer to your VMware documentation for more information about the VMware vCenter Converter. You can download the converter here:

http://downloads.vmware.com/d/info/datacenter_downloads/vmware_vcenter_converter

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

Note: If you cannot successfully complete this procedure, you can instead use an OS restore disk.

See "Installing from an ISO image or OS restore CD onto a virtual machine on your ESX or ESXi Server" on page 72.

To deploy an OVF template on an ESX 3.5 or ESXi 3.5 Server

1. Insert the CD that contains the OVF template zip file or locate the OVF template online and unpack it to your hard drive. The OVF template file name is as follows:

   Symantec_Brightmail_Gateway_VMimage_9.*_Linux_Int.zip

   The unpacked folder appears as Symantec_Brightmail_Gateway_9.*.
2. Start the VMware vCenter Converter.
3. In the **VMware Conversion** menu, click **Convert Machine**.
4. On the **Select source type** page, choose **Virtual appliance**.
5. For **Location**, choose **File system**.
6. Select the OVF template file. If necessary, click **Browse** to find the file.
7. Click **Next**.
8. On the **Virtual Appliance Details** page, verify that this is the file you want to deploy.

9 On the **Specify Destination Type** page, click **VMware Infrastructure Virtual Machine**.

10 Click **Next**.

11 Specify your host server name, user name, and password, then click **Next**.

12 On the **Host/Resource** page, optionally change the name for your virtual appliance, and click **Next**.

13 On the **Summary** page, review your deployment details and click **Finish**.

Deploying the OVF may take a few minutes. When complete, the new computer appears in your inventory.

14 After deployment is complete, access the new virtual computer from your client.

15 Click the Power on icon to start your virtual machine. The standard Symantec Brightmail Gateway boot sequence begins.

See "Installing the Symantec Brightmail Gateway product" on page 31.

Deploying an OVF template on an ESX 4.0 or ESXi 4.0 Server

You can deploy an OVF template that contains Symantec Brightmail Gateway Virtual Edition on a VMware ESX Server 4.0 or VMWare ESXi Server 4.0. An OVF template is a virtual machine that includes the software you plan to run on the machine. To deploy the OVF template, you can use a VSphere or VCenter client on a different computer than the computer hosting your ESX or ESXi Server.

Note: If you intend to deploy on an ESX 3.5 or ESXi 3.5 Server, you must use the VMware vCenter Converter.

See "Deploying an OVF template on an ESX 3.5 or ESXi 3.5 Server" on page 69.

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

Note: If you cannot successfully complete this procedure, you can instead use an OS restore disk

See "Installing from an ISO image or OS restore CD onto a virtual machine on your ESX or ESXi Server" on page 72.

To deploy an OVF template on an ESX 4.0 or ESXi 4.0 Server

1. Insert the CD that contains the OVF template zip file or locate the OVF template online and unpack it to your hard drive. The OVF template file name is as follows:

   Symantec_Brightmail_Gateway_VMimage_9.*_Linux_Int.zip

   The unpacked folder appears as Symantec_Brightmail_Gateway_9.*.
2. In the **File** menu, click **Deploy OVF template**.
3. On the **Source** page, click **Deploy from file**.
4. Select the file. If necessary, click **Browse** to find the file.
5. Click **Next**.
6. On the **OVF Template Details** page, verify that this is the file you want to deploy.
7. Click **Next**.
8. On the **Name and Location** page, optionally change the name for your virtual appliance, and click **Next**.
9. If you are using vCenter, you can choose the physical machine that you want to host your virtual machine.
10. On the **Ready to Complete** page, review your deployment details and click **Finish**. Deploying the OVF may take a few minutes. When complete, the new computer appears in your inventory.
11. After deployment is complete, access the new virtual computer from your client. The standard Symantec Brightmail Gateway boot sequence begins.

    See "Installing the Symantec Brightmail Gateway product" on page 31.

Installing from an ISO image or OS restore CD onto a virtual machine on your ESX or ESXi Server

Installing from an SBG ISO image or the OS restore CD onto a custom Virtual Machine on your ESX or ESXi Server

You can configure a virtual machine and deploy an instance of Symantec Brightmail Gateway that uses an OS restore CD or an ISO image on a computer that runs one of the following platforms:

- ESX or ESXi Server Version 3.5, update 4 or later
- ESX or ESXi Server Version 4.0

You must install either server before you perform this procedure.

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

You may want to ensure 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. If you work with ESXi, Symantec recommends that you modify the ESXi settings to create a root password and assign a static IP address. You should make this modification before you create a virtual appliance and install the Symantec Brightmail Gateway software onto it. This modification is important because Symantec Brightmail Gateway requires at least one static IP address. See "Specifying a static IP address for routing" on page 35.

To instal from an ISO image or OS restore CD onto a virtual machine on your ESX or ESXi Server

1. Click on the ESX or ESXi Server on which you want to place your virtual machine.
2. In the **File** menu, click **New**, then click **Virtual Machine**.
3. Select the **Typical** option and click **Next**.
4. Type a descriptive name for the virtual computer and click **Next**.
5. Select a data store option. This setting is where your virtual computer is located on the physical disk. Make this selection based on your particular storage configuration. Options can vary.
6. For the OS, click **Linux** as the Guest Operating System and **Other Linux (32-bit)** as the Version, and then click **Next**.
7. Reserve the necessary quantity of disk space, and then click **Next**.

   See "System requirements for virtual deployment" on page 68.

   More disk space may be required based on your deployment.

   Note: After you reserve disk space and complete deployment, any changes to disk space require that you repeat the OS restore process.

   ---

8 On the **Ready to Complete** page, check **Edit the virtual machine settings before submitting** and click **Continue**.

9 Click **Memory** at the left. Reserve the system memory based on your deployment needs, and then click **Next**.

A minimum of 2 GB is necessary to run Symantec Brightmail Gateway Virtual Edition and the virtual computer. Symantec recommends that you use at least 4 GB.

10 Click **CPU** at the left. Select the number of virtual CPUs, and then click **Next**.

ESX 3.5 and ESXi 3.5 are limited to two virtual CPUs per virtual computer. Symantec recommends allocating a minimum of two virtual processors.

11 If you want a second network interface, click the Add button at the top, choose the **Device type**, click **Next**, click **Next** again, and click **Finish**.

12 Click **Finish**.

13 Continue the deployment to bootstrap your virtual appliance.

See "Using an OS restore CD on your ESX or ESXi Server to boot your virtual computer" on page 74.

See "Using an ISO image on your datastore to boot your virtual computer" on page 75.

See "Using an OS restore CD or ISO image on your local computer to boot your virtual computer" on page 76.

Using an OS restore CD on your ESX or ESXi Server to boot your virtual computer

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

See "Installing from an ISO image or OS restore CD onto a virtual machine on your ESX or ESXi Server" on page 72.

To use an OS restore CD on your ESX or ESXi Server to boot your virtual computer

1 Insert the OS restore disk into your ESX or 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 power on virtual machine icon.

The virtual machine now reboots from the CD drive.

7 Click the **Disconnect CD/DVD** button 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 a future 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 Brightmail Gateway boot sequence.

See "Installing the Symantec Brightmail Gateway product" on page 31.

Using an ISO image on your datastore to boot your virtual computer

After you configure a virtual computer on ESX Server or ESXi Server, you can use an ISO image on your datastore as your bootstrap media.

See "Installing from an ISO image or OS restore CD onto a virtual machine on your ESX or ESXi Server" on page 72.

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

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 virtual computer 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 your mouse on the console window, and then press the **Enter** key 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 Brightmail Gateway boot sequence.

See "Installing the Symantec Brightmail Gateway product" on page 31.

Using an OS restore CD or ISO image on your local computer to boot your virtual computer

After you configure a virtual computer on an ESX Server or ESXi Server, use an OS restore Cd or ISO image on your local computer as your bootstrap media.

See "Installing from an ISO image or OS restore CD onto a virtual machine on your ESX or ESXi Server" on page 72.

To use an OS restore CD or ISO image on your local computer to boot your virtual computer

1 Insert the OS restore CD into the drive on your local computer, or 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 virtual computer appears in the inventory.

6 Click on the new virtual computer in the inventory, then click the console icon.

7 Click the power on virtual machine icon.

8 If you are using in ISO image. click **Connect CD/DVD > Use ISO image**, and browse to your ISO image. If you are using an OS restore CD, choose the letter of your computer's CD/DVD drive.

The boot process begins.

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

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

See "Installing the Symantec Brightmail Gateway product" on page 31.

Virtual software terminology

Key terminology relating to virtual software is as follows:

Virtual computer	A virtual computer is the software that insulates the application stack from the physical hardware.
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 virtual computer. Symantec Brightmail Gateway Virtual Edition is the guest computer and OS.
VMware ESX Server	VMware ESX Server is an enterprise-quality virtual machine platform that is recommended for best performance results.
VMware ESXi Server	VMware ESXi is a free download that offers similar functionality to ESX but with a smaller disk footprint. VMware ESXi is also sometimes referred to in VMware documentation as ESX Server 3i.
Virtual computer Image	A set of files in a VMware-specific format that contain an image of a preconfigured virtual computer and Symantec Brightmail Gateway Virtual Edition. This image can be used to install a virtual computer on a host computer that runs the VMware ESX Server.

ISO image or OS restore CD	An image that lets you install Symantec Brightmail Gateway onto a computer that that runs VMware ESX Server or ESXi Server.
OVF template	A virtual machine that includes a set of software. For example, an OVF template can include the Symantec Brightmail Gateway software.
vSphere client	A desktop virtual machine platform the connects to a VMWare ESX Server or VMWare ESXi server. The free version of vSphere allows you to run one virtual machine. The purchased version allows you to manage multiple virtual machines.

Chapter 4

Completing your Symantec Brightmail Gateway installation

This chapter includes the following topics:

Post-installation tasks

Table 4-1 lists the optional tasks that you can perform after you install Symantec Brightmail Gateway.

See "Post-installation tasks for instant messaging" on page 95.

Table 4-1 Post-installation tasks

Task	Description
Modify DNS MX records to block spam.	Modify DNS mail exchange (MX) records when you implement Symantec Brightmail Gateway in front of a separate MTA that receives inbound messages. See "About adjusting MX records to prevent spam" on page 81.

Table 4-1 Post-installation tasks *(continued)*

Task	Description
Modify the default filtering policies.	Symantec Brightmail Gateway installs with default policies. Review these policies to ensure that they meet your needs. If not, modify the policies as needed. See "About message filtering policies" on page 81.
Test antivirus filtering.	To ensure that your environment is protected against viruses, test to ensure that antivirus filtering works properly. See "Testing antivirus filtering" on page 82.
Test message delivery.	Test to ensure that users receive legitimate email messages. See "Testing the delivery of legitimate email" on page 82.
Test spam filtering.	If you filter spam, test to ensure that spam filtering works properly. See "Testing spam filtering" on page 83.
Test Spam Quarantine.	If you configured Symantec Brightmail Gateway to use Spam Quarantine, you can test to ensure that the messages are properly quarantined. See "Testing that spam messages are quarantined" on page 84.
Fine-tune features to enhance performance.	Certain features have a greater affect 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 28.
Specify the administrator email address for email notifications.	When you install the product, the installation wizard prompts you for an administrator email address. Symantec Brightmail Gateway sends alerts to this address. 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 Brightmail Gateway Administration Guide* for more details.

About adjusting MX records to prevent spam

You must change the DNS mail exchange (MX) records when you implement Symantec Brightmail Gateway in front of a separate MTA that receives inbound messages. The records must point incoming messages to the Symantec Brightmail Gateway Scanner or Scanners.

Spammers can look up the previous MTA's MX record if you list Symantec Brightmail 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 Brightmail 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 Brightmail Gateway.

When you name Symantec Brightmail 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 Brightmail Gateway installs with ready-made, 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, and viruses.
- The default spam policy is to modify the subject line by prepending [Spam] and deliver the message to the inbox.
- The default suspected spam policy is to modify the subject line by prepending [Suspected Spam] and deliver the message to the inbox.
- The suspected spam threshold is set to 72.
- The default virus policy is to clean the message.

- The default worm policy is to delete the message.
- No default content filtering policies are in place.
- No user configuration capabilities are in place.
- No IM filtering capabilities are in place.

For more information on configuring policies and settings, see the *Symantec Brightmail Gateway Administration Guide*.

Testing 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 indicating cleaning has occurred.

Testing 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.

Testing 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 **Dasboard** page increases by one if spam filtering works.

Testing that spam messages are quarantined

You must configure Symantec Brightmail 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: There can be a slight delay until the first spam message arrives, 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' inbox, 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.

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 as 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 user name and password and a user name and password are identical, the user is granted access to the administrator account.

To log on as a user with an iPlanet, SunONE, or Domino directory server account, your Administrator must enable LDAP authentication for the Control Center.

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. If the system administrator has enabled the **Remember me** feature, the **Remember me on this computer** option appears. Check this option to bypass your logon credentials when you subsequently access the Control Center.

   Symantec Brightmail Gateway requires you to re-enter your logon credentials after you loglogging out, or based on the duration that the administrator specifies.

   Note that if you use this feature, anyone that has access to your computer has access to the Control Center.

7. Click **Login**.

To log on as a user with an iPlanet or SunONE Directory Server account

1. 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>.

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 your full email address (for example, kris@symantecexample.com).

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

6. If the system administrator has enabled the **Remember me** feature, the **Remember me on this computer** option appears. Check this option to bypass your logon credentials when you subsequently access the Control Center.

   Symantec Brightmail Gateway requires you to re-enter your logon credentials based on the duration that the administrator specifies.

   Note that if you use this feature, anyone that has access to your computer has access to the Control Center.

7. Click **Login**.

To log on as a user with a Domino account

1. 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>.

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 your full email address (for example, kris@symantecexample.com).

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

6 If the system administrator has enabled the **Remember me** feature, the **Remember me on this computer** option appears. Check this option to bypass your logon credentials when you subsequently access the Control Center.

Symantec Brightmail Gateway requires you to re-enter your logon credentials after logging out, or based on the duration that the administrator specifies.

Note that if you use this feature, anyone that has access to your computer has access to the Control Center.

7 Click **Login**.

To log on as a user with an Active Directory account

1 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>.

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 your user name (for example, kris).

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

6 Select the LDAP server that you use to verify your credentials.

7 If the system administrator has enabled the **Remember me** feature, the **Remember me on this computer** option appears. Check this option to bypass your logon credentials when you subsequently access the Control Center.

Symantec Brightmail Gateway requires you to re-enter your logon credentials after logging out, or based on the duration that the administrator specifies.

Note that if you use this feature, anyone that has access to your computer has access to the Control Center.

8 Click **Login**.

To log off

1 In the upper right corner of any page, click the **Log Out** icon.

2 For security purposes, close your browser window to clear your browser's memory.

Troubleshooting problems logging on and logging off

If you have trouble logging on or logging off, consider the following:

- When logging on, make sure that you type your user name and password in the correct case.
  Note the difference between kris, Kris, and KRIS.
- You are automatically logged off if you do not use the Control Center for 30 minutes. If it happens, log on again.

Performing initial configuration tasks

During installation you set the initial configuration parameters that Symantec Brightmail Gateway uses to operate. Symantec Brightmail Gateway will continue to operate using the initial defaults as well as the specific choices you made during installation. 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.

Follow the four-step process below to ensure that you are ready to take full advantage of the extensive capabilities of Symantec Brightmail Gateway to meet the specific needs of your installation.

Table 4-2 Initial configuration tasks

Step	Action	Description
Step 1	After installing Symantec Brightmail Gateway, test message flow.	Ensure that your appliance is filtering and delivering mail.
Step 2	Configure optional communications and monitoring features.	Symantec Brightmail Gateway provides a variety of powerful communications and monitoring features. You can control SMTP and IM communications parameters and security. You ca n 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. See Table 4-3 on page 90.
Step 3	Configure optional directory integration features.	You can use LDAP directory data sources to integrate Symantec Brightmail Gateway with your existing directory data infrastructure. See Table 4-4 on page 91.
Step 4	Configure optional email management and filtering features.	Symantec Brightmail Gateway enables you to 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. See Table 4-5 on page 91.

Performing optional configuration tasks

Depending on your network environment, your users, and your processing needs, you may need to change some configuration settings in order to make the Symantec Brightmail Gateway product work optimally in your environment.

Symantec recommends enabling reputation filtering for increased antispam effectiveness and processing efficiency. You may want to enable other optional features. Some optional features require the configuration of an LDAP directory data source, or have other requirements.

For more information on any of the tasks in this section, see the *Symantec Brightmail Gateway Administration Guide*.

Table 4-3 Communications and monitoring

Action	Description
Configure additional Scanner settings	In addition to the MTA and SMTP choices made during installation, you can configure additional settings as needed. You can enable Scanner email settings, SMTP, and IM filtering.
Set up alerts, log settings, and report settings	Ensure that the appropriate system administrators are alerted of situations requiring their attention. Set log levels and locations. Ensure that the data required for the types of reports you want to run is collected.
Set up certificates and domain keys	Enable certificates to provide secure communications via HTTPS and TLS. Set up domain keys to use for DKIM authentication.
Configure Control Center settings	Configure certificates, system locale, fallback encoding, listening ports, and SMTP settings for the Control Center. Set up end user logins for access to Spam Quarantine, and manage end user preferences data.
Set up SNMP and UPS	Set up System Network Management Protocol (SNMP) monitoring of your appliances, and set up a Universal Power Supply (UPS) automated backup power facility.

Table 4-4 Directory integration

Action	Description
Configure directory integration	Create and configure LDAP directory data sources. Some Symantec Brightmail Gateway features require you to configure a directory data source.

Table 4-5 Email managment 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.
Enable reputation filtering	Enable preliminary filtering at connection time via Brightmail Adaptive Reputation Management. By enabling this feature you can dramatically reduce message processing volumes and enhance protection.
Configure spam, virus, and IM settings and policies	You can set up custom policies that determine what actions Symantec Brightmail Gateway takes on spam, suspected spam, viruses, and IM messages. Or, you can skip this step and use default policies.
Set up email authentication	You can set up four different types of email authentication: SPF, Sender ID, DKIM, and SMTP.
Create policy groups	You can set up groups of users, so that you can process email and IM 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 and IM messages for all users.
Set up content filtering	Set up policies that process email messages based on their content. Set up policies that enforce regulatory requirements in your email message flow, including review prior to the final action on a message.

Appendix A

Web addresses and ports used by Symantec Brightmail Gateway

This appendix includes the following topics:

Reserved ports

Table A-1 lists ports that you might encounter during a security audit or in log files while you troubleshoot an issue.

Table A-1 Symantec Brightmail 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
7007	TCP	Loopback interface	IM relay
8005	TCP	Loopback interface	Internal Control Center communication
8080	TCP	Loopback interface	Software update
41015	TCP	All enabled interfaces	Transformation Engine

Table A-1 Symantec Brightmail Gateway reserved ports *(continued)*

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

If you enable IM filtering, the following ports are reserved for IM use and should not be specified as the inbound email filtering port or outbound email filtering port:

- 80
- 1860 – 1869
- 5050 – 5059
- 5190 – 5199

Web addresses Symantec Brightmail Gateway uses

Table A-2 lists the Web addresses that Symantec Brightmail Gateway uses.

Table A-2 Symantec Brightmail 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 to retrieve filters
liveupdate.symantecliveupdate.com	TCP	80	Default automatic antivirus updates
liveupdate.symantec.com	TCP	80	Default automatic antivirus updates
relay.msg.yahoo.com	TCP	80	Yahoo file transfer
definitions.symantec.com	TCP	80	Rapid response antivirus updates

Appendix B

Post-Installation tasks for instant messaging

This appendix includes the following topics:

Post-installation tasks for instant messaging

lists the optional tasks related to instant messaging that you can perform after you install Symantec Brightmail Gateway.

See "Post-installation tasks" on page 79.

Table B-1 Post-installation tasks for instant messaging

Task	Description
Configure your DNS servers for IM filtering.	Modify your DNS servers if you intend to use IM filtering. See "About configuring DNS to route outgoing IM traffic to public IM networks" on page 96. See "Configuring DNS to route internal IM traffic to a Scanner" on page 97.
Block access to IM ports and proxies.	If you use IM filtering, you can block access to certain IM ports and proxies. See "Blocking access to Yahoo! Messenger webcam features" on page 97. See "Blocking access to Web-based IM clients" on page 98. See "Blocking access to HTTP and SOCKS proxies" on page 99.
Test IM filtering.	If you use IM filtering, you can test to ensure that it works properly. See "Testing an IM client" on page 100. See "About message filtering policies" on page 81.

About configuring DNS to route outgoing IM traffic to public IM networks

The Scanner directs your IM clients to their public IM network servers through an additional DNS after it filters IM messages. You specify this DNS when you install Symantec Brightmail Gateway.

The DNS can be one or both of the following:

Internet Root DNS — This DNS resides on the Internet. If you use this DNS, you must permit a connection from your firewall to the Internet over port 53.

An internal corporate DNS	This DNS resides within your corporate network. This DNS can resolve the server names of the public IM networks that you use. **Note:** This DNS cannot be the same internal DNS that you use to direct your IM clients to the Scanner. If it is, a loopback condition occurs where IM messages are directed back to the Scanner instead of to the Internet. You may want to consult the list of public IM network server names that this DNS must be able to resolve. See "Public IM network servers" on page 99.

Configuring DNS to route internal IM traffic to a Scanner

Your organization most likely has an internal DNS configured to direct your IM client traffic directly to the Internet. To use Symantec Brightmail Gateway to filter IM traffic, reconfigure your DNS to direct your IM client traffic to your IM-filtering Scanner instead.

You may want to consult the list of host names for each public IM network for which you must create a forward lookup zone.

See "Public IM network servers" on page 99.

Configuring DNS to route internal IM traffic to a Scanner

1. Create forward lookup zones in your DNS records for each public IM network that your organization uses.
2. Assign the IM-filtering Scanner's IP address as its host.

Blocking access to Yahoo! Messenger webcam features

Yahoo! Messenger has several webcam features that let IM users communicate through video by making a direct connection to a Yahoo! network server. You can block access to this server.

To block access to Yahoo! Messenger webcam features

- Do either of the following tasks:
  - Configure your Web proxy to block access to webcam.yahoo.com on port 5100.

- Configure your internal DNS to resolve webcam.yahoo.com to a non-existent IP address (such as 127.0.0.1).

Blocking access to Web-based IM clients

Most public IM networks offer Web-based versions of their IM clients, which permit IM users to communicate online through a Web browser. To prevent your IM users from using Web-based IM clients, you can block access to the public IM network servers that support them.

Blocking access to Web-based IM clients

- To block access to these servers, do either of the following tasks:
  - Configure your Web proxy to block access to the server names that are listed in Table B-2.
  - Configure your internal DNS to resolve the server names that are listed in Table B-2 to a non-existent IP address (such as 127.0.0.1).

Web-based public IM network server names

Table B-2 lists the network server names of the more common Web-based public IM networks.

Table B-2 Web-based public IM network server names

Public IM Network	Server Name
AIM	AIM server names include the following: ■ aimexpress.aol.com ■ aimexpress.oscar.aol.com ■ aimhttp.oscar.aol.com ■ beta.aimexpress.aol.com ■ aimexpress.aim.com ■ toc.oscar.aol.com

Table B-2 Web-based public IM network server names *(continued)*

Public IM Network	Server Name
Yahoo! Messenger	Yahoo! Messenger server names include the following: ■ http.msg.yahoo.com ■ shttp.msg.yahoo.com ■ ypager.yahoo.com ■ http.chat.yahoo.com ■ jcs.chat.yahoo.com ■ messenger.yahoo.com ■ vcs.msg.yahoo.com ■ vcs1.msg.yahoo.com ■ vcs2.msg.yahoo.com
MSN Messenger	MSN Messenger server names include the following: ■ gateway.messenger.hotmail.com ■ messenger.hotmail.com ■ webmessenger.hotmail.com
Google Talk	Google Talk server names include the following: ■ mail.google.com ■ gmail.google.com

See "Blocking access to Web-based IM clients" on page 98.

Blocking access to HTTP and SOCKS proxies

Most public IM clients can be configured to communicate through an HTTP or SOCKS proxy server. However, you can block these communications.

To block access to HTTP and SOCKS proxies

- Configure your HTTP or SOCKS proxy server to block access to the public IM network servers.

  See "Public IM network servers" on page 99.

Public IM network servers

Table B-3 lists the common public IM network server names.

Table B-3 Public IM network server names

IM Network	Server/Host Names
AIM	The AIM names are as follows: ■ login.oscar.aol.com ■ toc.oscar.aol.com ■ ats.byoa.aol.com ■ slogin.oscar.aol.com
MSN Messenger	messenger.hotmail.com
Yahoo! Messenger	The Yahoo! Messenger names are as follows: ■ relay.msg.yahoo.com ■ scs.msg.yahoo.com ■ scsa.msg.yahoo.com ■ scsb.msg.yahoo.com ■ scsc.msg.yahoo.com ■ scsd.msg.yahoo.com ■ scse.msg.yahoo.com ■ scsf.msg.yahoo.com ■ scsg.msg.yahoo.com ■ scsh.msg.yahoo.com ■ cn.scs.msg.yahoo.com ■ vcs.msg.yahoo.com ■ vcs1.msg.yahoo.com ■ vcs2.msg.yahoo.com
Google Talk	The Google Talk names are as follows: ■ talk.google.com ■ talkx.l.google.com

Testing an IM client

After you enable IM filtering, you can test an IM client to ensure that it is routed to that Scanner. To perform this test, configure individual IM clients or their workstations to direct IM messages to your IM filtering Scanner.

AIM is the only protocol that lets you configure its IM client to connect to a specified server. To configure the remaining protocols, edit the hosts file of the client workstations where the IM clients reside. (The hosts file is a local text file that maps specified host names to specified IP addresses.)

After the test, remember to configure the IM clients or workstations back to their original settings.

See "Directing AIM clients to your Scanner" on page 101.

See "Directing MSN Messenger clients to your Scanner" on page 101.

See "Directing Yahoo! Messenger clients to your Scanner" on page 102.

See "Directing Google Talk clients to your Scanner" on page 102.

To test an IM client

1. Log on one or more IM clients from the workstations that you directed to your Scanner.
2. From the Control Center, click **Status > Instant Messaging > Active Users**.
3. Click **Display Filtered**.

   The IM users should appear on the **Active IM Users** page.

Directing AIM clients to your Scanner

Configure each AIM client that you want to direct to your Scanner.

See "Testing an IM client" on page 100.

To direct AIM clients to your Scanner

1. From the AIM client, click **My Aim > Edit Options > Edit Preferences**.
2. From the **Category** list, click **Sign On/Off**.
3. Click **Connections**.
4. Under **Server** in the **Host** field, type the host name or IP address of your Scanner.
5. In the **Port** field, type **5190**.
6. Click **OK**, and then click **OK** again.

   For the change to take effect, you must log off and then log on again.

Directing MSN Messenger clients to your Scanner

Configure each MSN Messenger client workstation that you want to direct to your Scanner.

See "Testing an IM client" on page 100.

To direct MSN Messenger clients to your Scanner

1. From the client workstation, open the following file using a text editor:

   C:\WINDOWS\system32\drivers\etc\hosts

2. Insert the following line:

   <Scanner IP address> messenger.hotmail.com

3. Save and close the file.

Directing Yahoo! Messenger clients to your Scanner

Configure each Yahoo! Messenger client or workstation that you want to direct to your Scanner.

See "Testing an IM client" on page 100.

To direct Yahoo! Messenger clients to your Scanner

1. From the client workstation, open the following file using a text editor:

   C:\WINDOWS\system32\drivers\etc\hosts

2. Type the following lines:

   <Scanner IP address> scs.msg.yahoo.com

   <Scanner IP address> scsa.msg.yahoo.com

   <Scanner IP address> scsb.msg.yahoo.com

   <Scanner IP address> scsc.msg.yahoo.com

   <Scanner IP address> scsd.msg.yahoo.com

   <Scanner IP address> scse.msg.yahoo.com

   <Scanner IP address> scsf.msg.yahoo.com

3. Save and close the file.

Directing Google Talk clients to your Scanner

Configure each Google Talk client workstation that you want to direct to your Scanner.

See "Testing an IM client" on page 100.

To direct Google Talk clients to your Scanner

1. From the client workstation, open the following file using a text editor:

   C:\WINDOWS\system32\drivers\etc\hosts

2. Type the following line:

   <Scanner IP address> talk.google.com

3. Save and close the file.

Index

M

P

R

S

T

V

W

Y