Symantec Brightmail™ Gateway 9.0 Installation Guide
The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version: 9.0

Legal Notice

Copyright © 2010 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, Brightmail™, the Brightmail™ logo, BLOC, BrightSig, The Anti-Spam Leader, Probe Network, and Norton Anti-Virus are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.
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.
Chapter 1 Installing Symantec Brightmail Gateway

About installation configurations .................................................. 11
Before you install ......................................................................... 12
About the appliance's functions ................................................. 13
Where to position your Scanners .............................................. 13
About the environmental factors that affect performance ............. 14
Installation checklist .............................................................. 15
Sample Scanner port configurations .......................................... 21
Ports that Symantec Brightmail Gateway uses ............................. 22
Required ports ....................................................................... 26
About the DNS servers required for IM filtering ....................... 27
System requirements .................................................................... 28
Features that can affect performance ........................................... 28

Chapter 2 Installing the Symantec Brightmail Gateway product

Installing the Symantec Brightmail Gateway product ......................... 31
Setting up the appliance hardware ............................................ 33
Starting the appliance software set up ....................................... 34
Specifying Ethernet interfaces .................................................. 34
Specifying a static IP address for routing .................................... 35
Specifying gateway and DNS IP addresses .............................. 36
Specifying the role for the appliance .......................................... 37
Registering your license .......................................................... 38
Troubleshooting license file registration .................................... 40
Updating to the latest software during initial setup ...................... 40
Configuring the Control Center ................................................. 41
About adding a Scanner through the Control Center ................. 43
Adding a Scanner through the Control Center ............................. 44
Configuring the Scanner for inbound and outbound mail filtering ................................................................. 46
Configuring the Scanner for inbound mail filtering only ............... 50
Configuring the Scanner for outbound mail filtering only .......... 52
Configuring the Scanner for inbound mail filtering with instant message filtering ............................................................. 54
Configuring the Scanner for outbound mail filtering with instant message filtering ............................................................. 58
Configuring the Scanner for inbound and outbound mail filtering with instant message filtering ............................................ 61

Chapter 3 Installing Symantec Brightmail Gateway Virtual Edition ............................................................................. 67
About Symantec Brightmail Gateway Virtual Edition ...................... 67
System requirements for virtual deployment ................................. 68
Deploying an OVF template on an ESX 3.5 or ESXi 3.5 Server ......... 69
Deploying an OVF template on an ESX 4.0 or ESXi 4.0 Server ............ 71
Installing from an ISO image or OS restore CD onto a virtual machine on your ESX or ESXi Server ...................................................... 72
Using an OS restore CD on your ESX or ESXi Server to boot your virtual computer ............................................................. 74
Using an ISO image on your datastore to boot your virtual computer .............................................................................. 75
Using an OS restore CD or ISO image on your local computer to boot your virtual computer ............................................................. 76
Virtual software terminology ......................................................... 77

Chapter 4 Completing your Symantec Brightmail Gateway installation ............................................................. 79
Post-installation tasks ................................................................. 79
About adjusting MX records to prevent spam ................................ 81
About message filtering policies .................................................. 81
Testing antivirus filtering ........................................................... 82
Testing the delivery of legitimate email ........................................... 82
Testing spam filtering .............................................................. 83
Testing that spam messages are quarantined .............................. 84
Logging on and logging off ....................................................... 84
Troubleshooting problems logging on and logging off ................. 88
Performing initial configuration tasks ............................................. 88
Performing optional configuration tasks ......................................... 90

Appendix A Web addresses and ports used by Symantec Brightmail Gateway ...................................................... 93
Reserved ports ............................................................................. 93
Web addresses Symantec Brightmail Gateway uses ....................... 94
Appendix B  Post-Installation tasks for instant messaging ............ 95

Post-installation tasks for instant messaging ................................ 95
About configuring DNS to route outgoing IM traffic to public IM
networks .................................................................................. 96
Configuring DNS to route internal IM traffic to a Scanner .......... 97
Blocking access to Yahoo! Messenger webcam features .......... 97
Blocking access to Web-based IM clients ................................... 98
Web-based public IM network server names .......................... 98
Blocking access to HTTP and SOCKS proxies ......................... 99
Public IM network servers .................................................... 99
Testing an IM client ............................................................... 100
Directing AIM clients to your Scanner ............................... 101
Directing MSN Messenger clients to your Scanner .......... 101
Directing Yahoo! Messenger clients to your Scanner .......... 102
Directing Google Talk clients to your Scanner .................. 102

Index ......................................................................................... 105
Installing Symantec Brightmail Gateway

This chapter includes the following topics:

■ About installation configurations
■ Before you install
■ System requirements
■ Features that can affect performance

About installation configurations

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

<table>
<thead>
<tr>
<th>Symantec Brightmail Gateway appliance</th>
<th>Install and run a physical, Symantec-supplied appliance. See “Installing the Symantec Brightmail Gateway product” on page 31.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mixed-mode</td>
<td>Install and run a combination of physical and virtual components.</td>
</tr>
</tbody>
</table>
Before you install

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

### Table 1-1 Preinstallation tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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.


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

<table>
<thead>
<tr>
<th>Completed</th>
<th>Item</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
</table>
| ___       | 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                                                                          | OR                                        |
|           |                           | ___Serial port                                                              | ___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                                                   | New password:                            |
|           |                           | See “Starting the appliance software set up” on page 34.                     |                                           |
| ___       | IP address of Ethernet interface 1: | IP address of Ethernet interface 1:                                         |                                           |
|           |                           | _______________________________                                            |                                           |
|           | Ethertnet 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 2:      |
|           |                           | _______________________________                                            |                                           |
|           |                           | Subnet mask for Ethernet interface 1:                                       | Subnet mask for Ethernet interface 2:    |
|           |                           | _______________________________                                            | _______________________________          |

**Installing Symantec Brightmail Gateway**

Before you install
Table 1-2  |  Initial configuration checklist (continued)

<table>
<thead>
<tr>
<th>Completed</th>
<th>Item</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
</table>
|           | 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. |
|           | 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>
<thead>
<tr>
<th>Completed</th>
<th>Item</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Valid license file</td>
<td>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.</td>
<td>File location of the license file:</td>
</tr>
<tr>
<td></td>
<td>Proxy server host name and port (optional)</td>
<td>You only need to provide proxy server information if you use a proxy server to communicate with Symantec.</td>
<td>Proxy server host name:</td>
</tr>
<tr>
<td></td>
<td>Proxy server host name and port (optional)</td>
<td>See “Registering your license” on page 38.</td>
<td>Proxy server port:</td>
</tr>
<tr>
<td></td>
<td>Administrator email address (Control Center configuration only)</td>
<td>Symantec Brightmail Gateway sends alerts to this address, if alert notifications are enabled.</td>
<td>Administrator email address:</td>
</tr>
<tr>
<td></td>
<td>NTP servers (optional)</td>
<td>You can specify an Internet or internal NTP server to manage time. You can specify up to three servers.</td>
<td>NTP servers:</td>
</tr>
<tr>
<td></td>
<td>Scanner role</td>
<td>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</td>
<td>Scanner role:</td>
</tr>
</tbody>
</table>
### Table 1-2  Initial configuration checklist (continued)

<table>
<thead>
<tr>
<th>Completed</th>
<th>Item</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Scanner host name or IP address (Scanner configuration only)</td>
<td>You must provide a host name or IP address for the Scanner.</td>
<td>Scanner host name or IP address: _________________</td>
</tr>
<tr>
<td></td>
<td>Virtual IP address (Scanner configuration only)</td>
<td>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.</td>
<td>Virtual IP address: _________________ Netmask: _________________ Port: _________________</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Completed</th>
<th>Item</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Inbound mail address</td>
<td>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.</td>
<td>Inbound mail filtering IP address: _________________ Port: _________________</td>
</tr>
<tr>
<td></td>
<td>Inbound mail acceptance</td>
<td>You can accept mail from all sources or specify the domains from which you accept mail.</td>
<td>Accept mail from all sources OR IP addresses or host names of domains from which you accept mail: 1. _________________ 2. _________________ 3. _________________</td>
</tr>
</tbody>
</table>
Table 1-3  Inbound mail filtering checklist (continued)

<table>
<thead>
<tr>
<th>Completed</th>
<th>Item</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Inbound local mail</td>
<td>You can specify a specific server or you can use Enable MX Lookup.</td>
<td>IP address of mail server to accept mail relay:</td>
</tr>
<tr>
<td>delivery</td>
<td>delivery</td>
<td></td>
<td>1. _____________________________</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This server is typically a downstream mail server, such as your corporate</td>
<td>Port: ____________</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mail server.</td>
<td>2. _____________________________</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can specify up to three mail servers to accept inbound mail relay.</td>
<td>Port: ____________</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3. _____________________________</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>OR</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MX Lookup host name (do not use IP address):</td>
</tr>
<tr>
<td></td>
<td>Non-local mail delivery</td>
<td>You can use MX Lookup, add a new host, or use an existing host.</td>
<td>Host name or IP address:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>_____________________________</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If there is a separate gateway MTA between the Scanner and the Internet,</td>
<td>OR</td>
</tr>
<tr>
<td></td>
<td></td>
<td>provide that MTA’s host name or IP address and port.</td>
<td>MX Lookup host name:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>_____________________________</td>
</tr>
<tr>
<td></td>
<td>Local domains</td>
<td>These addresses are added to the Local Domains list.</td>
<td>Domain or IP address:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1. _____________________________</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2. _____________________________</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3. _____________________________</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>OR</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MX Lookup host name:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>_____________________________</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Completed</th>
<th>Item</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Outbound mail address</td>
<td>This address is the address and port to use for outbound mail filtering.</td>
<td>Outbound mail filtering IP address:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This address is most likely the address for your Ethernet 2 port.</td>
<td>Port:</td>
</tr>
<tr>
<td></td>
<td>Outbound mail acceptance</td>
<td>Provide an IP address or domain. You can specify multiple addresses and</td>
<td>IP addresses or domains:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>domains.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Outbound local mail</td>
<td>You can specify a specific server or you can use Enable MX Lookup.</td>
<td>IP address of mail server to accept mail relay:</td>
</tr>
<tr>
<td></td>
<td>delivery</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>This server is typically a downstream mail server, such as your corporate</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>mail server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Non-local mail delivery</td>
<td>You can use MX Lookup, add a new host, or use an existing host.</td>
<td>Host name or IP address:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Completed</th>
<th>Item</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Outbound IM interface</td>
<td>The address is used for routing internal IM traffic.</td>
<td>Ethernet interface for IM filtering:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can specify up to two addresses.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The secondary IP address routes AOL file transfers through the Scanner and</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>provide that MTA's host name or IP address and port.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Outbound IP addresses:
1. 
2. 

OR
MX Lookup host name:

Non-local mail delivery:

Host name or IP address:

OR
MX Lookup host name:
### Table 1-5
Instant message filter configuration checklist (continued)

<table>
<thead>
<tr>
<th>Completed</th>
<th>Item</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Inbound IM interface</td>
<td>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.</td>
<td>Ethernet interface to communicate with public servers:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Inbound IP address:</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Port configuration</th>
<th>Example IP addresses and port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two physical ports (eth0 and eth1)</td>
<td>192.0.32.1:25, 192.0.47.255:25</td>
<td>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.</td>
</tr>
<tr>
<td>Each port has one IP address</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| One physical port                   | 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.        |
| One IP address                      |                              | This configuration can result in network bottlenecks, but is suitable for sites with relatively low email traffic.                  |
| Two different TCP ports             |                              |                                                                                                                                 |
Table 1-6  Scanner port configurations examples (continued)

<table>
<thead>
<tr>
<th>Port configuration</th>
<th>Example IP addresses and port</th>
<th>Notes</th>
</tr>
</thead>
</table>
| ■ 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 additional, 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>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Origin</th>
<th>Destination</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>TCP</td>
<td>Your management hosts</td>
<td>Control Center/Scanners</td>
<td>SSH connectivity to the appliance</td>
<td>This port provides access to the command line interface.</td>
</tr>
<tr>
<td>25</td>
<td>TCP</td>
<td>Control Center/Scanners</td>
<td>Internal mail servers</td>
<td>Inbound internal email traffic</td>
<td>The Control Center uses internal mail hosts to send alerts and reports.</td>
</tr>
<tr>
<td>25</td>
<td>TCP</td>
<td>Scanners</td>
<td>Internal mail servers</td>
<td>IM user self-registration</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>TCP</td>
<td>Internal mail servers</td>
<td>Scanners</td>
<td>Outbound internal mail traffic</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>TCP</td>
<td>Internet</td>
<td>Scanners</td>
<td>Inbound Internet mail traffic</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>TCP</td>
<td>Scanners</td>
<td>Internet</td>
<td>Outbound Internet mail traffic</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>TCP</td>
<td>Scanners</td>
<td>Internal SMTP server</td>
<td>SMTP authentication forwarding</td>
<td></td>
</tr>
<tr>
<td>53</td>
<td>UDP</td>
<td>Scanners</td>
<td>Internet</td>
<td>DNS lookups</td>
<td>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.</td>
</tr>
<tr>
<td>80</td>
<td>TCP</td>
<td>Control Center</td>
<td>Internet</td>
<td>ThreatCon updates</td>
<td>The ThreatCon level appears on the Dashboard page.</td>
</tr>
<tr>
<td>80</td>
<td>TCP</td>
<td>Scanners</td>
<td>Internet</td>
<td>Default automatic antivirus updates and rapid response antivirus updates</td>
<td></td>
</tr>
<tr>
<td>80</td>
<td>TCP</td>
<td>IM clients</td>
<td>Scanners with IM filtering</td>
<td>Yahoo! Messenger</td>
<td>This port is used for instant messaging file transfers.</td>
</tr>
<tr>
<td>80</td>
<td>TCP</td>
<td>Scanners with IM filtering</td>
<td>Internet</td>
<td>Yahoo! Messenger</td>
<td>This port is used for instant messaging file transfers.</td>
</tr>
</tbody>
</table>
### Table 1-7  Ports to open in your network for Symantec Brightmail Gateway (continued)

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Origin</th>
<th>Destination</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>123</td>
<td>UDP</td>
<td>Control Center/Scanners</td>
<td>Internet/ internal NTP Servers</td>
<td>Time sync servers for the appliance</td>
<td></td>
</tr>
<tr>
<td>161</td>
<td>UDP</td>
<td>SNMP servers</td>
<td>Control Center/ Scanners</td>
<td>SNMP management</td>
<td>The default port for SNMP communications. This port can be changed to match your SNMP configuration. This port is disabled by default.</td>
</tr>
<tr>
<td>389</td>
<td>TCP</td>
<td>Control Center/Scanners</td>
<td>LDAP servers</td>
<td>LDAP server access to lookup users, groups, and distribution lists if the directory data service is enabled.</td>
<td>Both Control Center and Scanners use this port if directory data service is enabled.</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>Control Center/Scanners</td>
<td>Internet</td>
<td>Rule updates, software updates, and license registration</td>
<td>Symantec sends rule updates to your appliances.</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>IM clients</td>
<td>Internet</td>
<td>HTTPS connection from Google Talk, MSN Messenger, and Yahoo! Messenger clients for user authentication</td>
<td></td>
</tr>
<tr>
<td>587</td>
<td>TCP</td>
<td>Internet</td>
<td>Scanners</td>
<td>SMTP authentication traffic</td>
<td></td>
</tr>
<tr>
<td>636</td>
<td>TCP</td>
<td>Control Center/ Scanners</td>
<td>LDAP servers</td>
<td>SSL encrypted LDAP server access to lookup users, groups, and distribution lists if the directory data service is enabled.</td>
<td>Both Control Center and Scanners use this port if directory data service is enabled.</td>
</tr>
<tr>
<td>1863</td>
<td>TCP</td>
<td>IM clients</td>
<td>Scanners with IM filtering</td>
<td>MSN Messenger</td>
<td>This port is used for instant messaging and instant messaging file transfers.</td>
</tr>
<tr>
<td>1863</td>
<td>TCP</td>
<td>Scanners with IM filtering</td>
<td>Internet</td>
<td>MSN Messenger</td>
<td>This port is used for instant messaging and instant messaging file transfers.</td>
</tr>
<tr>
<td>Port</td>
<td>Protocol</td>
<td>Origin</td>
<td>Destination</td>
<td>Description</td>
<td>Notes</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>--------</td>
<td>-------------</td>
<td>-------------</td>
<td>-------</td>
</tr>
<tr>
<td>3268</td>
<td>TCP</td>
<td>Control Center/Scanners</td>
<td>LDAP servers</td>
<td>Active Directory Global Catalog server (LDAP)</td>
<td></td>
</tr>
<tr>
<td>3269</td>
<td>TCP</td>
<td>Control Center/Scanners</td>
<td>LDAP servers</td>
<td>SSL encrypted Active Directory Global Catalog server (LDAP)</td>
<td></td>
</tr>
<tr>
<td>41000</td>
<td>TCP</td>
<td>MTA/Scanners</td>
<td>MTA/Scanners</td>
<td>Bidirectional</td>
<td></td>
</tr>
</tbody>
</table>
| 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. |
| 5050 | TCP | IM clients with IM filtering | 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)

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

Required ports

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

Table 1-8  Required ports

<table>
<thead>
<tr>
<th>Protocols needed</th>
<th>Name</th>
<th>Protocol</th>
<th>Default port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote access to the appliance</td>
<td>SSH</td>
<td>TCP</td>
<td>22</td>
<td>This port provides access to the command line interface.</td>
</tr>
<tr>
<td>Access to name service</td>
<td>DNS</td>
<td>UDP (TCP)</td>
<td>53</td>
<td>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.</td>
</tr>
<tr>
<td>Protocols needed</td>
<td>Name</td>
<td>Protocol</td>
<td>Default port</td>
<td>Notes</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>---------------</td>
<td>----------</td>
<td>--------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Access to the Control Center and outbound access to external Internet</td>
<td>HTTP</td>
<td>TCP</td>
<td>80</td>
<td>See “Ports that Symantec Brightmail Gateway uses” on page 22.</td>
</tr>
<tr>
<td>Access to time service</td>
<td>NTP</td>
<td>UDP</td>
<td>123</td>
<td></td>
</tr>
<tr>
<td>Access to Control Center (secured)</td>
<td>HTTPS</td>
<td>TCP</td>
<td>443</td>
<td></td>
</tr>
<tr>
<td>Outbound access to external Internet (secured)</td>
<td>HTTPS</td>
<td>TCP</td>
<td>443</td>
<td></td>
</tr>
<tr>
<td>MTA to Scanner (bi-directional)</td>
<td>---</td>
<td>TCP</td>
<td>41000</td>
<td></td>
</tr>
<tr>
<td>Control Center to Scanner (bi-directional)</td>
<td>---</td>
<td>TCP</td>
<td>41002</td>
<td>Traffic on 41002 (the agent port), flows as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>■ BCC to scanner (session request)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>■ Scanner to BCC (session accept)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>■ BCC to scanner (agent request)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>■ Scanner to BCC (agent response)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>■ BCC to scanner (terminate session)</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Item</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web browsers</td>
<td>The Control Center supports the following browsers:</td>
</tr>
<tr>
<td></td>
<td>■ Microsoft Internet Explorer 6, 7, and 8</td>
</tr>
<tr>
<td></td>
<td>■ Mozilla Firefox 3 and 3.5</td>
</tr>
<tr>
<td>LDAP</td>
<td>Symantec Brightmail Gateway supports the following LDAP directory types:</td>
</tr>
<tr>
<td></td>
<td>■ Windows 2008 Active Directory (both LDAP and Global Catalog)</td>
</tr>
<tr>
<td></td>
<td>■ Windows 2003 Active Directory (both LDAP and Global Catalog)</td>
</tr>
<tr>
<td></td>
<td>■ Windows 2000 Active Directory (both LDAP and Global Catalog)</td>
</tr>
<tr>
<td></td>
<td>■ Sun Directory Server 6.3</td>
</tr>
<tr>
<td></td>
<td>■ Sun Directory Server 6.0</td>
</tr>
<tr>
<td></td>
<td>■ Sun Directory Server 5.2 (formerly known as iPlanet, SunONE, and Java directory servers)</td>
</tr>
<tr>
<td></td>
<td>■ Lotus Domino LDAP Server 8.5</td>
</tr>
<tr>
<td></td>
<td>■ Lotus Domino LDAP Server 8.0</td>
</tr>
<tr>
<td></td>
<td>■ Lotus Domino LDAP Server 7.0</td>
</tr>
<tr>
<td></td>
<td>■ Lotus Domino LDAP Server 6.5</td>
</tr>
<tr>
<td></td>
<td>■ OpenLDAP 2.4</td>
</tr>
<tr>
<td></td>
<td>■ OpenLDAP 2.3</td>
</tr>
<tr>
<td></td>
<td>■ OpenLDAP 2.2</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Feature</th>
<th>How performance can be affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy groups</td>
<td>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.</td>
</tr>
<tr>
<td>Scanners</td>
<td>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.</td>
</tr>
<tr>
<td>Logs</td>
<td>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.</td>
</tr>
<tr>
<td>Reports</td>
<td>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.</td>
</tr>
<tr>
<td>Appliance roles</td>
<td>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.</td>
</tr>
</tbody>
</table>
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 can 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.

<table>
<thead>
<tr>
<th>Feature</th>
<th>How performance can be affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam Quarantine</td>
<td>The following are Spam Quarantine performance implications:</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td>- The more users that access Spam Quarantine, the more performance overhead that is required. Not allowing end user access to Spam Quarantines can increase performance significantly.</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td>DKIM signing</td>
<td>Enabling DKIM signing can impact outbound messaging performance. Using a shorter encryption key can reduce this impact.</td>
</tr>
<tr>
<td>SMTP authentication</td>
<td>SMTP authentication adds overhead that can impact outbound messaging performance.</td>
</tr>
</tbody>
</table>

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

This chapter includes the following topics:

- Installing the Symantec Brightmail Gateway product

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>
<thead>
<tr>
<th>Table 2-1 Symantec Brightmail Gateway installation process</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step</strong></td>
</tr>
<tr>
<td>---</td>
</tr>
</tbody>
</table>
| 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)

<table>
<thead>
<tr>
<th>Step</th>
<th>Task and description</th>
</tr>
</thead>
</table>
| 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)

<table>
<thead>
<tr>
<th>Step</th>
<th>Task and description</th>
</tr>
</thead>
</table>
| 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.
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 add 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.

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**.
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.

Click **Next**.

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.

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.

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.
On the **Setup Summary** page, select any of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Finish</strong></td>
<td>You are satisfied with the settings and do not want to make changes. This option is the default setting.</td>
</tr>
<tr>
<td><strong>Back</strong></td>
<td>You want to modify your settings.</td>
</tr>
<tr>
<td><strong>Cancel</strong></td>
<td>You want to end the setup without saving your changes. You cannot use the appliance until you complete the setup.</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Step</th>
<th>Task description</th>
</tr>
</thead>
</table>
| 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)

<table>
<thead>
<tr>
<th>Step</th>
<th>Task description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>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.</td>
</tr>
<tr>
<td>3</td>
<td>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.</td>
</tr>
<tr>
<td>4</td>
<td>Check the status of the Scanner to ensure that it functions properly. See the Symantec Brightmail Gateway Administration Guide for more information.</td>
</tr>
</tbody>
</table>

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 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 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 MXlookup 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.
Installing Symantec Brightmail Gateway Virtual Edition

This chapter includes the following topics:

- About Symantec Brightmail Gateway Virtual Edition
- System requirements for virtual deployment
- Deploying an OVF template on an ESX 3.5 or ESXi 3.5 Server
- Deploying an OVF template on an ESX 4.0 or ESXi 4.0 Server
- Installing from an ISO image or OS restore CD onto a virtual machine on your ESX or ESXi Server
- Using an OS restore CD on your ESX or ESXi Server to boot your virtual computer
- Using an ISO image on your datastore to boot your virtual computer
- Using an OS restore CD or ISO image on your local computer to boot your virtual computer
- Virtual software terminology

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

<table>
<thead>
<tr>
<th>Description</th>
<th>Recommended</th>
<th>Minimum</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware ESX Server</td>
<td>Version 4.0</td>
<td>Version 3.5, update 4</td>
<td>For Scanner-only virtual machines.</td>
</tr>
<tr>
<td>VMware ESXi Server version</td>
<td>Version 4.0</td>
<td>Version 3.5, update 4</td>
<td>For Control Center–only virtual machines.</td>
</tr>
<tr>
<td>Disk space</td>
<td>For more information, consult the Symantec Knowledge Base article, <em>Disk Space Recommendations for Symantec Brightmail Gateway Virtual Edition</em></td>
<td>90 GB 90 GB 90 GB For more information, consult the Symantec Knowledge Base article, <em>Disk Space Recommendations for Symantec Brightmail Gateway Virtual Edition</em></td>
<td>For combined Scanner and Control Center virtual machines.</td>
</tr>
<tr>
<td>Memory</td>
<td>4 GB</td>
<td>2 GB</td>
<td>A minimum of 2 GB is necessary to run Symantec Brightmail Gateway and the virtual machine.</td>
</tr>
<tr>
<td>CPUs</td>
<td>4</td>
<td>2</td>
<td>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.</td>
</tr>
<tr>
<td>NICs</td>
<td>1</td>
<td>1</td>
<td>Only one network interface card is required per virtual machine.</td>
</tr>
</tbody>
</table>

### 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.


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

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.

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.

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.

Click Finish.

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.
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.

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.
<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO image or OS restore CD</td>
<td>An image that lets you install Symantec Brightmail Gateway onto a computer that runs VMware ESX Server or ESXi Server.</td>
</tr>
<tr>
<td>OVF template</td>
<td>A virtual machine that includes a set of software. For example, an OVF template can include the Symantec Brightmail Gateway software.</td>
</tr>
<tr>
<td>vSphere client</td>
<td>A desktop virtual machine platform that 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.</td>
</tr>
</tbody>
</table>
Completing your Symantec Brightmail Gateway installation

This chapter includes the following topics:

- **Post-installation tasks**
- **Performing initial configuration tasks**
- **Performing optional configuration tasks**

### 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

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify DNS MX records to block spam.</td>
<td>Modify DNS mail exchange (MX) records when you implement Symantec Brightmail Gateway in front of a separate MTA that receives inbound messages.</td>
</tr>
<tr>
<td></td>
<td>See “About adjusting MX records to prevent spam” on page 81.</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Modify the default filtering policies.</td>
<td>Symantec Brightmail Gateway installs with default policies. Review these policies to ensure that they meet your needs. If not, modify the policies as needed.</td>
</tr>
<tr>
<td></td>
<td>See “About message filtering policies” on page 81.</td>
</tr>
<tr>
<td>Test antivirus filtering.</td>
<td>To ensure that your environment is protected against viruses, test to ensure that antivirus filtering works properly.</td>
</tr>
<tr>
<td></td>
<td>See “Testing antivirus filtering” on page 82.</td>
</tr>
<tr>
<td>Test message delivery.</td>
<td>Test to ensure that users receive legitimate email messages.</td>
</tr>
<tr>
<td></td>
<td>See “Testing the delivery of legitimate email” on page 82.</td>
</tr>
<tr>
<td>Test spam filtering.</td>
<td>If you filter spam, test to ensure that spam filtering works properly.</td>
</tr>
<tr>
<td></td>
<td>See “Testing spam filtering” on page 83.</td>
</tr>
<tr>
<td>Test Spam Quarantine.</td>
<td>If you configured Symantec Brightmail Gateway to use Spam Quarantine, you can test to ensure that the messages are properly quarantined.</td>
</tr>
<tr>
<td></td>
<td>See “Testing that spam messages are quarantined” on page 84.</td>
</tr>
<tr>
<td>Fine-tune features to enhance performance.</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>See “Features that can affect performance” on page 28.</td>
</tr>
<tr>
<td>Specify the administrator email address</td>
<td>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.</td>
</tr>
<tr>
<td>email address for email notifications.</td>
<td>See the Symantec Brightmail Gateway Administration Guide for more details.</td>
</tr>
</tbody>
</table>
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 Dashboard 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 log 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.
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.

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>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>After installing Symantec Brightmail Gateway, test message flow.</td>
<td>Ensure that your appliance is filtering and delivering mail.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Configure optional communications and monitoring features.</td>
<td>Symantec Brightmail Gateway provides a variety of powerful communications and monitoring features. You can control SMTP and IM communications parameters and security. You can control end user access and communications between your Control Center and your Scanners. You can set up alerts, logs, and reports, as well as SNMP monitoring and UPS backup. See Table 4-3 on page 90.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Configure optional directory integration features.</td>
<td>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.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Configure optional email management and filtering features.</td>
<td>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.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure additional Scanner settings</td>
<td>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.</td>
</tr>
<tr>
<td>Set up alerts, log settings, and report settings</td>
<td>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.</td>
</tr>
<tr>
<td>Set up certificates and domain keys</td>
<td>Enable certificates to provide secure communications via HTTPS and TLS. Set up domain keys to use for DKIM authentication.</td>
</tr>
<tr>
<td>Configure Control Center settings</td>
<td>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.</td>
</tr>
<tr>
<td>Set up SNMP and UPS</td>
<td>Set up System Network Management Protocol (SNMP) monitoring of your appliances, and set up a Universal Power Supply (UPS) automated backup power facility.</td>
</tr>
</tbody>
</table>
### Table 4-4  Directory integration

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure directory integration</td>
<td>Create and configure LDAP directory data sources. Some Symantec Brightmail Gateway features require you to configure a directory data source.</td>
</tr>
</tbody>
</table>

### Table 4-5  Email management and filtering

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure email settings</td>
<td>Configure additional local and non-local domains, address masquerading, aliasing, invalid recipient handling, bad message handling, SMTP greetings, postmaster address, and container limits.</td>
</tr>
<tr>
<td>Enable reputation filtering</td>
<td>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.</td>
</tr>
<tr>
<td>Configure spam, virus, and IM settings and policies</td>
<td>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.</td>
</tr>
<tr>
<td>Set up email authentication</td>
<td>You can set up four different types of email authentication: SPF, Sender ID, DKIM, and SMTP.</td>
</tr>
<tr>
<td>Create policy groups</td>
<td>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.</td>
</tr>
<tr>
<td>Set up content filtering</td>
<td>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.</td>
</tr>
</tbody>
</table>
Completing your Symantec Brightmail Gateway installation

Performing optional configuration tasks
Web addresses and ports used by Symantec Brightmail Gateway

This appendix includes the following topics:

- Reserved ports
- Web addresses Symantec Brightmail Gateway uses

## 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>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Listens on</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>199</td>
<td>TCP</td>
<td>All enabled interfaces</td>
<td>SNMP multiplexing protocol</td>
</tr>
<tr>
<td>953</td>
<td>TCP</td>
<td>Loopback interface</td>
<td>DNS</td>
</tr>
<tr>
<td>3306</td>
<td>TCP</td>
<td>Loopback interface</td>
<td>MySQL database</td>
</tr>
<tr>
<td>7007</td>
<td>TCP</td>
<td>Loopback interface</td>
<td>IM relay</td>
</tr>
<tr>
<td>8005</td>
<td>TCP</td>
<td>Loopback interface</td>
<td>Internal Control Center communication</td>
</tr>
<tr>
<td>8080</td>
<td>TCP</td>
<td>Loopback interface</td>
<td>Software update</td>
</tr>
<tr>
<td>41015</td>
<td>TCP</td>
<td>All enabled interfaces</td>
<td>Transformation Engine</td>
</tr>
</tbody>
</table>
Table A-1  Symantec Brightmail Gateway reserved ports (continued)

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Listens on</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>41016</td>
<td>TCP</td>
<td>All enabled interfaces</td>
<td>Inbound internal Suspect Virus Quarantine communication</td>
</tr>
<tr>
<td>41017</td>
<td>TCP</td>
<td>All enabled interfaces</td>
<td>Outbound internal Suspect Virus Quarantine communication</td>
</tr>
<tr>
<td>41018</td>
<td>TCP</td>
<td>Loopback interface</td>
<td>Directory data service</td>
</tr>
<tr>
<td>41019</td>
<td>TCP</td>
<td>Loopback interface</td>
<td>Directory data service shutdown</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>URL</th>
<th>Protocol</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>swupdate.brightmail.com</td>
<td>TCP</td>
<td>443</td>
<td>Used to retrieve new software</td>
</tr>
<tr>
<td>register.brightmail.com</td>
<td>TCP</td>
<td>443</td>
<td>Used to register the appliance</td>
</tr>
<tr>
<td>aztec.brightmail.com</td>
<td>TCP</td>
<td>443</td>
<td>Used to retrieve filters</td>
</tr>
<tr>
<td>liveupdate.symantecliveupdate.com</td>
<td>TCP</td>
<td>80</td>
<td>Default automatic antivirus updates</td>
</tr>
<tr>
<td>liveupdate.symantec.com</td>
<td>TCP</td>
<td>80</td>
<td>Default automatic antivirus updates</td>
</tr>
<tr>
<td>relay.msg.yahoo.com</td>
<td>TCP</td>
<td>80</td>
<td>Yahoo file transfer</td>
</tr>
<tr>
<td>definitions.symantec.com</td>
<td>TCP</td>
<td>80</td>
<td>Rapid response antivirus updates</td>
</tr>
</tbody>
</table>
Post-Installation tasks for instant messaging

This appendix includes the following topics:

- Post-installation tasks for instant messaging
- About configuring DNS to route outgoing IM traffic to public IM networks
- Configuring DNS to route internal IM traffic to a Scanner
- Blocking access to Yahoo! Messenger webcam features
- Blocking access to Web-based IM clients
- Blocking access to HTTP and SOCKS proxies
- Testing an IM client

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 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.

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>
<thead>
<tr>
<th>Public IM Network</th>
<th>Server Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIM</td>
<td>AIM server names include the following:</td>
</tr>
<tr>
<td></td>
<td>■ aimexpress.aol.com</td>
</tr>
<tr>
<td></td>
<td>■ aimexpress.oscar.aol.com</td>
</tr>
<tr>
<td></td>
<td>■ aimhttp.oscar.aol.com</td>
</tr>
<tr>
<td></td>
<td>■ beta.aimexpress.aol.com</td>
</tr>
<tr>
<td></td>
<td>■ aimexpress.aim.com</td>
</tr>
<tr>
<td></td>
<td>■ toc.oscar.aol.com</td>
</tr>
</tbody>
</table>
Table B-2  Web-based public IM network server names (continued)

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

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.
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.
Testing an IM client
A
access, blocking
  proxies
    HTTP 99
    SOCKS 99
  Web-based IM clients 98
  webcam features 97
Active Directory 84
administrator email address 41
antivirus filters 82
AOL (American Online) 98–99, 101
Appliance
  hardware setup 33
  initial setup 34
  roles 13, 37

C
Control Center
  configuring 41
  function 13
  logging on and off 84, 88
  registration 38, 40

D
deployment considerations 14
DNS (Domain Name Server) 27, 36, 96–97
Domain Name Server. See DNS
Domino 84

E
e-mail delivery 82
ESX Server 72
ESXi Server 72
Ethernet settings 34
Exchange. See Microsoft Exchange

F
fallback encoding 41

G
gateway IP address 36
Google Talk 98–99, 102

H
hardware 33
HTTP, blocking access to 99

I
installation
  checklist 15
  configurations 11
  ports 22, 26, 93
  post-installation tasks 79
  pre-installation tasks 12
  process 31
instant messaging
  AIM 101
  blocking public IM networks 96
  DNS server 97
  Google Talk 102
  MSN Messenger 101
  public IM network 99
  required DNS servers 27
  testing clients 100
  Web-based clients 98
  Web-based public IM network server names 98
  Yahoo IM 102
iPlanet. See Sun Directory Server

L
license 38, 40
load balancing 13
logon
  bypassing credentials 84
  Control Center 84, 88
logon, Control Center 84, 88
Lotus Domino. See Domino
M
mail filtering
  configuring
    inbound and outbound 46
    inbound and outbound with instant messaging 61
    inbound only 50
    inbound with instant messaging 54
    outbound only 52
    outbound with instant messaging 58
Microsoft Exchange 84
MSN Messenger 98–99, 101
MTA
  MX records, adjusting 81
  Scanner placement 13
MX records 81

P
password 34
performance 14, 28
policies, default 81
port 21–22, 26, 93
post-installation 79
pre-installation 12
proxy 99
public IM network 99
public IM networks 96

R
registration 38, 40

S
Scanners
  adding 43
    through the Control Center 44
  configuring
    inbound and outbound mail filtering 46
    inbound and outbound mail filtering with instant messaging 61
    inbound mail filtering 50
    inbound mail filtering with instant messaging 54
    outbound mail filtering with instant messaging 58
    outbound mail filtering 52
directing clients to
  AIM 101
  Google Talk 102
Scanners (continued)
directing clients to (continued)
  MSN Messenger 101
  Yahoo IM 102
  function 13
  placement 13
  port configuration 21
SOCKS, blocking access to 99
software 40
spam 83
  MX records, adjusting 81
  testing
    filters 83
    quarantine 84
static IP address 35
Sun Directory Server 84
SunOne. See Sun Directory Server
Symantec Brightmail Gateway Web addresses 94
Symantec Brightmail Gateway Virtual Edition about 67
deployment 69, 72
ISO image 75–76
OSrestore CD 74
system requirements 68
terminology 77
system locale 41
system requirements 28, 68

T
tests
  antivirus filtering 82
  legitimate mail delivery 82
  spam filtering 83
  spam quarantine 84
time settings 41
troubleshooting
  licensing 40
  logging on or off 88

V
virtual computer
  about 67
terminology 77
virtual IP address 46, 54, 61
VMware 67
W
Web addresses 94
Web-based public IM network server names 98
webcam 97

Y
Yahoo IM 97–99, 102