Symantec Web Gateway Version 4.5 Implementation Guide

symantec™

Documentation version: 4.5.2

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's maintenance 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 Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

For information about Symantec's Maintenance Programs, you can visit our Web site at the following URL:

www.symantec.com/techsupp/

Contacting Technical Support

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

www.symantec.com/techsupp/

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 disk space and NIC information
- 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/techsupp/

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp/

Customer Service is available to assist with 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 maintenance 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

Maintenance agreement resources

If you want to contact Symantec regarding an existing maintenance agreement, please contact the maintenance 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:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security 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.
Educational Services	Educational 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

Select your country or language from the site index.

Contents

Chapter 1

Introducing Symantec Web Gateway

This chapter includes the following topics:

About Symantec Web Gateway

Symantec Web Gateway is an innovative Web security gateway appliance that protects organizations against Web 2.0 threats. These threats include malicious URLs, spyware, botnets, viruses, and other types of malware. Symantec Web Gateway provides controls for Web content and Internet applications. Backed by the Symantec Global Intelligence Network, Symantec Web Gateway is built on a scalable platform that quickly and simultaneously scans for malware and inappropriate Web content. Symantec Web Gateway helps organizations maintain critical uptime and employee productivity by blocking attacks.

Symantec Web Gateway has the following key features:

- Provides fast protection at the Web gateway across multiple protocols for inbound and outbound web traffic
- Protects against malware threats on all Web 2.0 file transfer channels
- Ability to inspect for, detect, and block active and dormant botnets
- Features URL filtering with flexible policy controls, and in-depth reporting and alerts (the URL filtering license is required)
- Advanced application control capabilities with ability to monitor and control usage by end-users spanning multiple applications

- Detects compromised endpoints by network fingerprinting and behavioral modeling
- Comprehensive Web reporting and alerting
- Flexible policy controls allow policy creation on any criteria and control over of how policies are applied across an organization

Symantec Web Gateway provides the following key benefits:

- Symantec Web Gateway includes the Symantec AntiVirus Engine, winner of over 40 consecutive VB100 Awards since 1999.
- Self-contained appliance includes all necessary components to secure the Web gateway, eliminating the need to introduce other technology into a network.
- Highly scalable technology to meet the needs of any size organization without added latency, ensuring zero impact on user browsing experience.
- The Symantec Global Intelligence Network continuously collects data and provides the data to Symantec Web Gateway. The Symantec Global Intelligence Network encompasses some of the most extensive sources of Internet threat data in the world. Symantec Web Gateway uses this threat data to offer comprehensive and up-to-date protection against the latest threats.

What you can do with Symantec Web Gateway

Table 1-1 describes what you can do with Symantec Brightmail Gateway

Table 1-1 What you can do with Symantec Web Gateway

Tasks	Description
Protect computers from spyware, botnets, and viruses	Symantec Web Gateway detects and blocks malware from Web sites and Internet downloads. Symantec Web Gateway must be installed in the inline network configuration to block downloads.
Block select Internet applications	You can configure Symantec Web Gateway to prevent peer-to-peer sharing, streaming media, games, and other Internet applications from accessing the Internet.
Block select Web sites	Symantec Web Gateway can block individual Web sites or categories of Web sites. To block Web sites by category, you must have the URL filtering license.

Table 1-1 What you can do with Symantec Web Gateway *(continued)*

Tasks	Description
Policies	You can use policies to determine which computers should have Internet applications or Web sites blocked. You can configure access by IP address or IP address ranges. If you configure Active Directory integration, you can set policies by user names and groups.
Display reports	You can display reports on a wide range of statistics. Available reports include most accessed Web sites, most active users, infected clients, most common malware, network attacks, and infection sources. Click a statistic in a report to get more information about that user, computer, Web site, category, etc.
Configure alerts	Symantec Web Gateway can issue alerts for attacks, infections, data leaks, and system events. Symantec Web Gateway transmits alerts by email, syslog, or SNMP.
Quarantine infected computers	Symantec Web Gateway can automatically block inbound and outbound Internet access for infected computers to prevent malware from spreading.

Chapter 2

Planning for installation

This chapter includes the following topics:

Steps to install Symantec Web Gateway

Table 2-1 describes the steps to install and initially configure Symantec Web Gateway. These steps are listed in the suggested order.

Table 2-1 Steps to install Symantec Web Gateway

Step	Action	Description
Step 1	Review installation checklist	Ensure that you have the appropriate hardware, license, and information about your network. See "Installation checklist" on page 17.

Table 2-1 Steps to install Symantec Web Gateway *(continued)*

Step	Action	Description
Step 2	Determine how you want to install Symantec Web Gateway in your network	The manner in which you connect Symantec Web Gateway to your network affects its capabilities. See "About inline or port span/tap network configurations" on page 21.
Step 3	Determine whether you want to initially monitor Internet traffic or block spyware as well	You set the default behavior for Symantec Web Gateway, but the default can be overridden when you configure policies. See "About blocking or monitoring modes" on page 21.
Step 4	Configure your firewall to allow traffic from Symantec Web Gateway	Ensure that the necessary ports are open in your firewall and other network devices to allow Symantec Web Gateway to function properly. See "Ports used by Symantec Web Gateway" on page 29.
Step 5	Install the Symantec Web Gateway appliance into a rack, but wait to connect Ethernet cables	You can wait to install Symantec Web Gateway into a rack, but connect the power to Symantec Web Gateway before connecting the computer to it. See "Installing the Symantec Web Gateway appliance into a rack" on page 34.
Step 6	Configure and connect a computer to Symantec Web Gateway for initial installation	You use a directly connected computer to initially configure Symantec Web Gateway. See "Configuring a computer to access Symantec Web Gateway for installation" on page 34.
Step 7	Run the setup wizard	You specify the primary administrative user, network configuration, and initial settings for Symantec Web Gateway in the setup wizard. See "Running the setup wizard for initial installation" on page 35. See "Configuring proxy settings in the setup wizard" on page 38.
Step 8	Specify your network configuration, enable features in the Web GUI, and connect Symantec Web Gateway to your network	After you run the setup wizard, there are additional tasks required to enable Symantec Web Gateway. See "Configuring Symantec Web Gateway after running the setup wizard" on page 39.

Installation checklist

Table 2-2 describes the items that you need before you install Symantec Web Gateway.

Table 2-2 Installation checklist

Item	Description
Computer with Ethernet port for initial setup	You connect a computer to the Mgmt port on Symantec Web Gateway to initially configure Symantec Web Gateway. Any modern computer and operating system works for this purpose, such as Linux, Mac OS X, and Windows.
Web browser	You configure and monitor Symantec Web Gateway using a Web browser from a computer on your local network. Most modern Web browsers are compatible with Symantec Web Gateway. The following browsers have been certified to work with Symantec Web Gateway: ■ Microsoft Internet Explorer 6.0, 7.0 ■ Mozilla Firefox 3 Symantec Web Gateway can monitor Internet traffic on user computers from any Web browser. However, the network on which the user computers reside must be configured in the Web GUI. In most cases, Symantec Web Gateway does not require changes to any end-user software including the Web browser. However, if you configure Active Directory integration using NTLM, you may have to change the Web browser configuration on end-user computers. This change prevents an authentication pop-up window.
Administrator user name and password	Choose an administrator name and password for access to the Web GUI. The primary administrator can create additional administrator accounts for access to the Web GUI.
Email address	You specify an email address in the setup wizard. Symantec Web Gateway sends alerts and reports to this email address. If you click the **Forgot Password?** link on the login page, a new password is sent to this address.

Table 2-2 Installation checklist *(continued)*

Item	Description
License file	A Symantec license file typically has the extension .slf. When you register your software license, Symantec emails you a license file. Put the license file in a location that is accessible from the computer on which you plan to run the setup wizard. Symantec provides a two week grace period with base functionality if you run the setup wizard without specifying a license. The following types of licenses are available for Symantec Web Gateway: ■ Base The base license includes detection of spyware, viruses, and botnet infections. If it is configured in the inline network configuration, Symantec Web Gateway can block malware downloads. In addition to Web browser-based malware, Symantec Web Gateway can detect malware in other Internet applications such as IM and FTP. ■ URL filtering In addition to the features in the base license, the URL filtering license lets you monitor or block access to Web pages based on policies.

Table 2-2 Installation checklist *(continued)*

Item	Description
IP address and related network settings for Symantec Web Gateway appliance	You typically configure Symantec Web Gateway with a static IP address. To specify a static IP address for Symantec Web Gateway, obtain an IP address in your network that is not in use by another computer. The following network settings are needed for a static IP address: ■ IP address ■ Subnet mask ■ Default gateway ■ Primary DNS ■ Secondary DNS (optional) ■ DNS suffix (optional) You can configure two IP addresses for Symantec Web Gateway. In this configuration the IP addresses are used as follows: 1 One IP address is used for communication with the Web GUI. 2 Symantec Web Gateway uses the other IP address for communication with the end user. For example, Symantec Web Gateway sends the end user pages and authentication requests using this IP address. This two IP address configuration is recommended if you plan to connect Symantec Web Gateway in the inline network configuration. The two IP addresses must be in different subnets.
Proxy information	A proxy is not required for Symantec Web Gateway to function. However, if Symantec Web Gateway accesses the Internet using a proxy or users access the Internet using a proxy, you must specify the following information: ■ Proxy IP address and port for Symantec Web Gateway to use for Internet access ■ Proxy ports used by users for HTTP access
List of internal subnets	You must specify your internal subnets in Symantec Web Gateway after running the setup wizard.

Table 2-2 Installation checklist *(continued)*

Item	Description
Configure DNS	You must have DNS configured to resolve Internet addresses. In most cases, Symantec Web Gateway does not require changes to DNS to function. However, if you configure Active Directory integration using NTLM, you must create a DNS A record entry for each Symantec Web Gateway appliance. These DNS entries ensure that the Web browsers used by end-users access Symantec Web Gateway as an intranet device.
Up to 4 normal and 2 crossover Ethernet cables	You need up to four normal and up to two crossover Ethernet cables. The number of cables you need depends on the network configuration that you choose and the number of LAN and WAN ports on the appliance. Crossover Ethernet cables are included with your appliance. The Ethernet cables should have the typical RJ-45 (8P8C) jacks.

Connections and indicators on Symantec Web Gateway

Connections that are not labeled are not functional or are not supported. For example, the keyboard ports and mouse ports are not functional.

Two solid (not blinking) LEDs indicate bypass mode, as shown in figures Figure 2-1 and Figure 2-2.

See "Ensuring Internet connectivity if Symantec Web Gateway is disabled" on page 45.

Figure 2-1 Symantec Web Gateway 8450

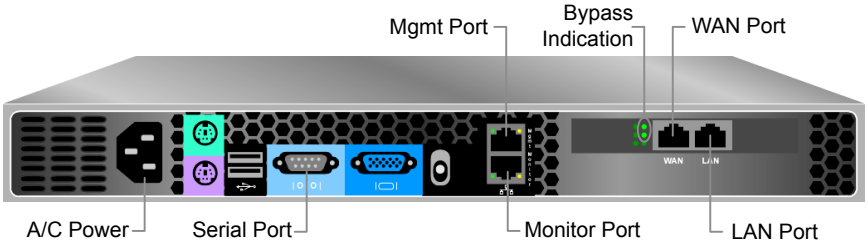
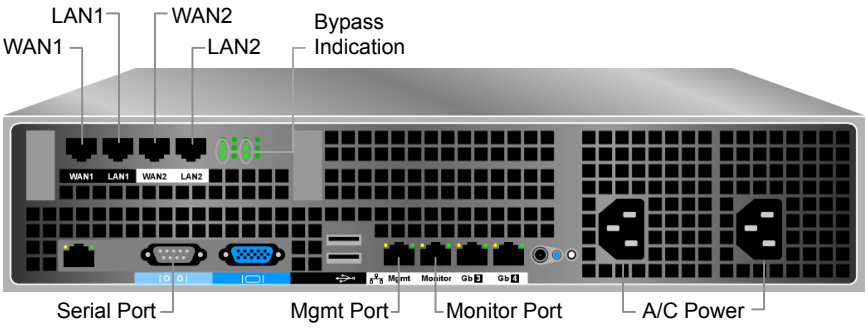


Figure 2-2 Symantec Web Gateway 8490



About inline or port span/tap network configurations

Table 2-3 describes the types of configurations that you can install in your network.

See "Port connections for typical network configurations" on page 22.

Table 2-3 Comparison of inline and port span/tap network configurations

Network configuration	Description
Inline	Symantec Web Gateway can block file downloads as well as block Web sites and phone-home attempts. Inline configuration requires more network connections than port span/tap.
Port span/tap	Symantec Web Gateway cannot block file downloads, but it can block Web sites and phone-home attempts. The port span/tap configuration is easier because it only requires one connection to your LAN. This configuration can be useful as an initial test of Symantec Web Gateway.

About blocking or monitoring modes

Table 2-4 describes the modes that are available for Symantec Web Gateway. The mode that you choose defines the default behavior of Symantec Web Gateway when you configure user policies.

Note: You can override the default mode when you configure policies. For example, if you set Symantec Web Gateway to monitoring mode, you can configure a policy that blocks Web sites.

Table 2-4 Comparison of blocking and monitoring modes

Mode	Description
Blocking	Depending on the network configuration, Symantec Web Gateway can block Web sites, phone-home attempts, and file downloads. When in blocking mode, Symantec Web Gateway also provides reports on user activity like monitoring mode. You must install Symantec Web Gateway in the inline network configuration to block file downloads. See "About inline or port span/tap network configurations" on page 21.
Monitoring	Symantec Web Gateway does not block any Internet traffic, but it provides reports on user activity. This mode can be useful as an initial test of Symantec Web Gateway.

Port connections for typical network configurations

Table 2-5 describes the port connections for typical network configurations.

Note: You may need to use a crossover Ethernet cable for the connection from the Symantec Web Gateway LAN port to the LAN switch.

See "Ensuring Internet connectivity if Symantec Web Gateway is disabled" on page 45.

Table 2-5 Port connections for typical network configurations

Network configuration	Description	Connect Mgmt to	Connect Monitor to	Connect LAN to	Connect WAN to
Port span/tap	Simple port span/tap network configuration. See Figure 2-3 on page 24.	Port on your LAN switch (required)	Network tap or a port on your LAN switch that is set to span mode (required)	Port on your LAN switch; required only for blocking and if Web GUI has separate IP address (optional)	Not used

Table 2-5 Port connections for typical network configurations *(continued)*

Network configuration	Description	Connect Mgmt to	Connect Monitor to	Connect LAN to	Connect WAN to
Simple inline with no proxy or the proxy is at the firewall	Simple inline network configuration. If a proxy exists in the network, it is connected to the firewall. See Figure 2-4 on page 25.	Port on your LAN switch (required)	Not used	Port on your LAN switch (required)	Internet firewall LAN port(required)
Inline with two firewalls and two Symantec Web Gateway appliances	You can connect two Symantec Web Gateway appliances to two firewalls as part of a high availability environment. The firewalls can be configured in active-active failover or active-standby failover. The Symantec Web Gateway appliances should be configured identically except for the network settings. See Figure 2-5 on page 26.	Port on your LAN switch (required)	Not used	Port on your LAN switch (required)	Internet firewall LAN port(required)
Inline with 1 NIC proxy that is connected to Symantec Web Gateway	If your proxy server is connected to the corporate LAN rather than the firewall, install Symantec Web Gateway between the corporate LAN and the proxy server. See Figure 2-6 on page 27.	Port on your LAN switch (required)	Not used	Port on the proxy (required)	Port on your LAN switch (required)
Inline with 2 NIC proxy that is connect twice to dual-homed Symantec Web Gateway	For greater throughput on the proxy server, you can connect a single Symantec Web Gateway appliance with two LAN and two WAN ports to a proxy server. You can also connect a single Symantec Web Gateway appliance with two LAN and two WAN ports to two proxy servers. See Figure 2-7 on page 28.	Port on your LAN switch (required)	Not used	Port on the proxy; connect LAN2 to the proxy also (required)	Port on your layer 3 switch; connect WAN2 to a separate layer 3 switch (required)

Table 2-5 Port connections for typical network configurations *(continued)*

Network configuration	Description	Connect Mgmt to	Connect Monitor to	Connect LAN to	Connect WAN to
Inline with 2 NIC proxy that is connected to Symantec Web Gateway and to the firewall	The proxy server is connected to the firewall and Symantec Web Gateway. See Figure 2-8 on page 29.	Port on your LAN switch (required)	Not used	Port on your LAN switch (required)	Port on the proxy (required)
Central Intelligence Unit	An appliance that is configured to manage other appliances is called a Central Intelligence Unit.	Port on your LAN switch (required)	Not used	Not used	Not used

Figure 2-3 Simple port span/tap network configuration

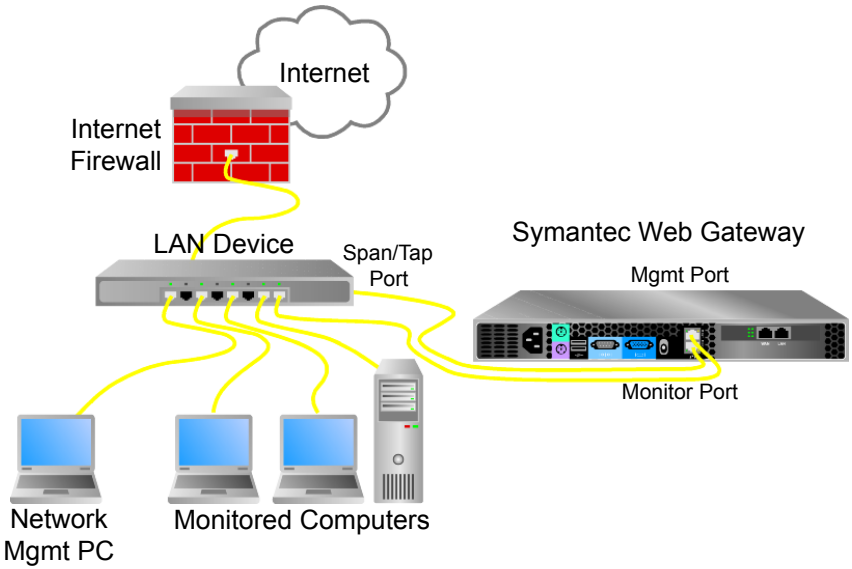


Figure 2-4 Simple inline network configuration

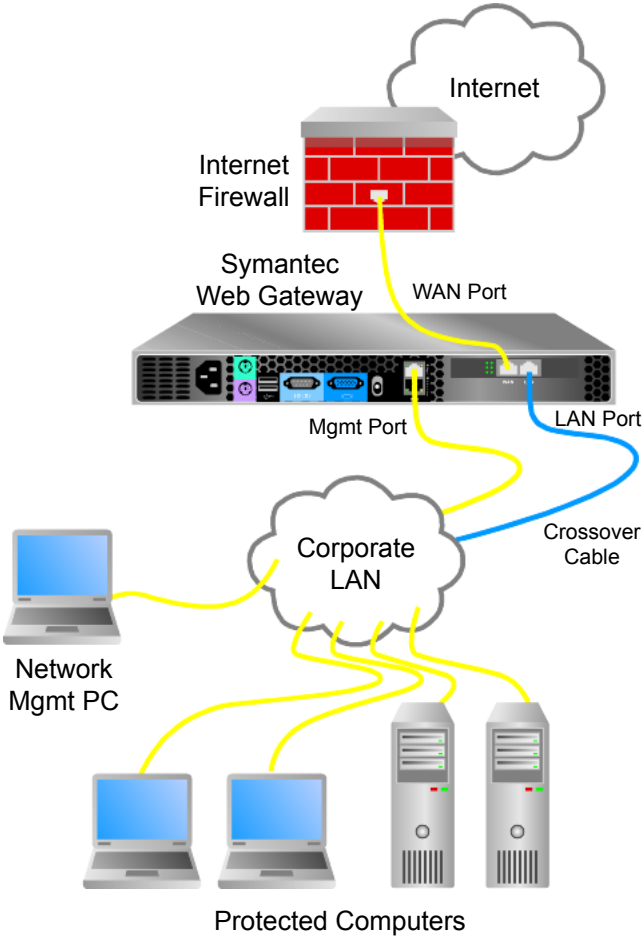


Figure 2-5 Inline with two firewalls and two Symantec Web Gateway appliances

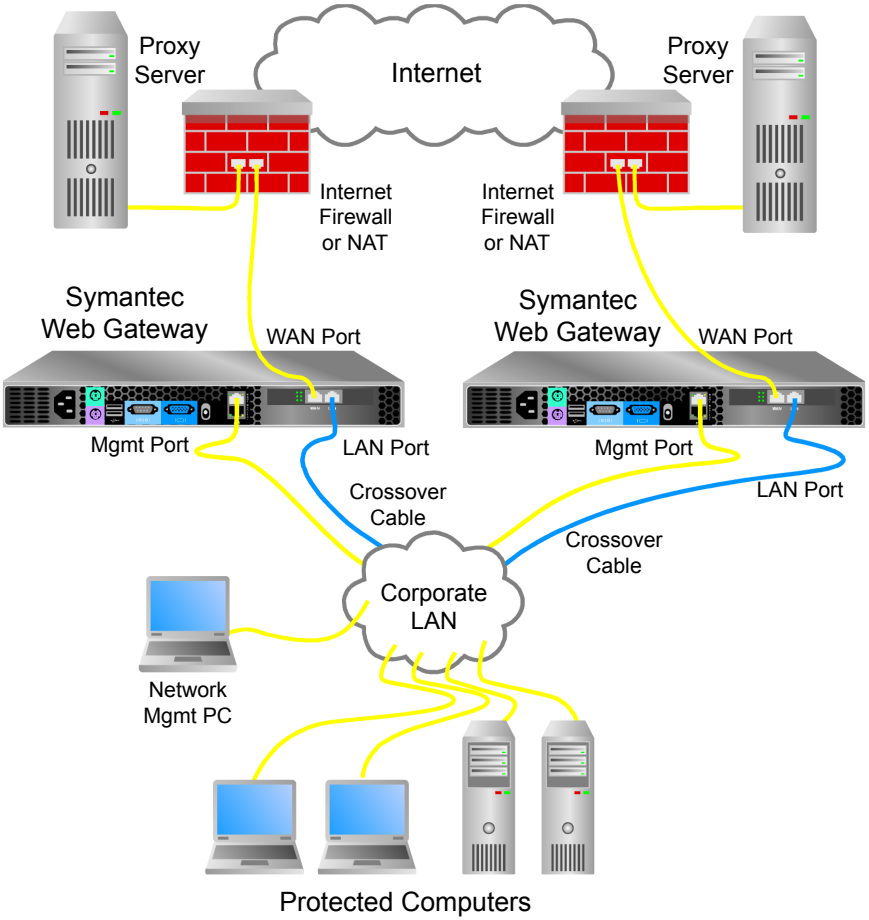


Figure 2-6 Inline with single-leg proxy server

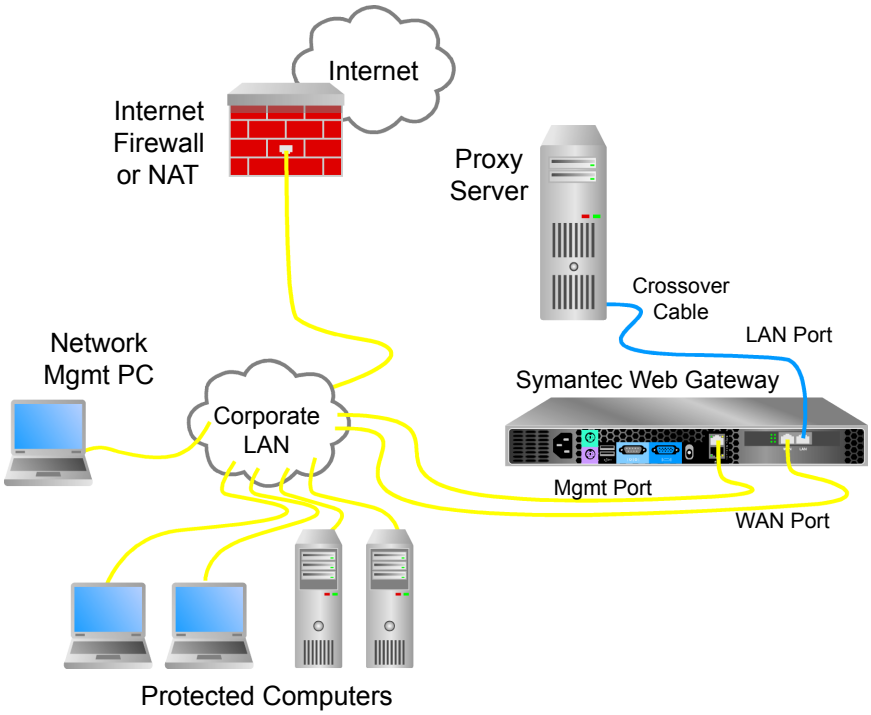


Figure 2-7 Inline with dual-homed Symantec Web Gateway

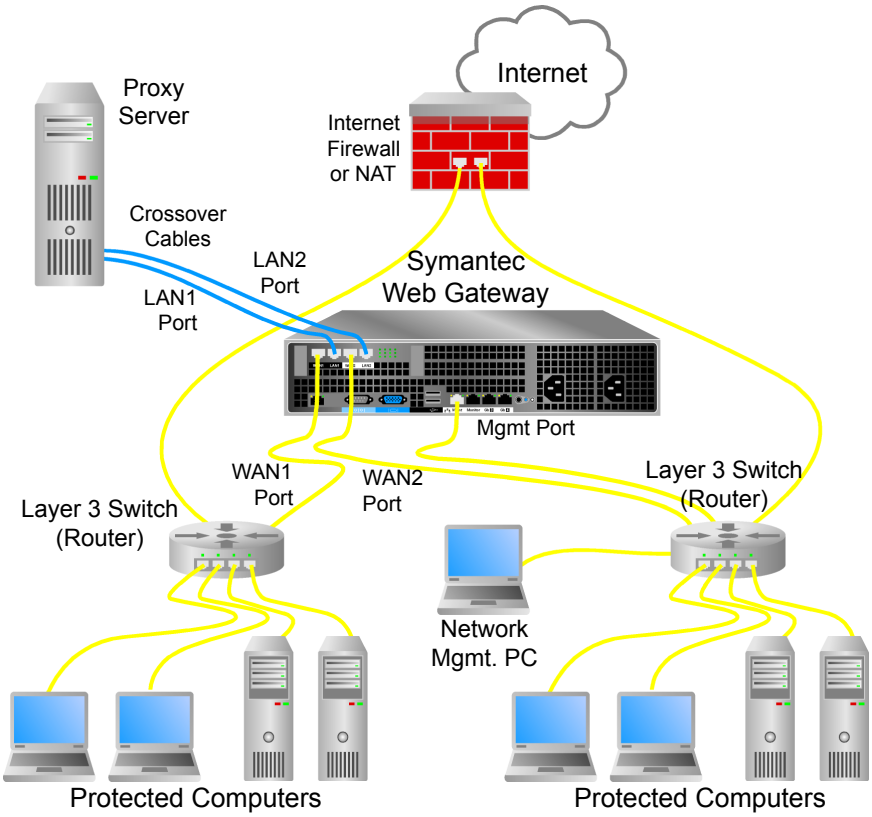
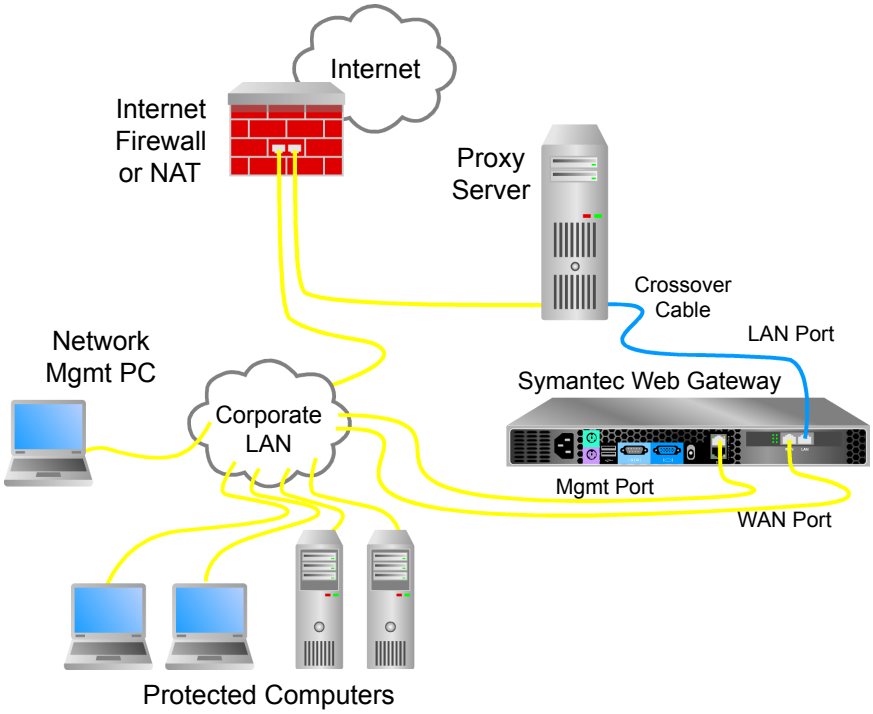


Figure 2-8 Inline with proxy server connected to firewall and Symantec Web Gateway



Ports used by Symantec Web Gateway

Table 2-6 describes the ports that Symantec Web Gateway communicates with. Ensure that your firewall allows traffic through these ports.

Table 2-6 Ports used by Symantec Web Gateway

Port	Protocol	From	To	Description
53	UDP	Symantec Web Gateway	User-defined DNS servers	External DNS lookups, if configured
80	TCP	Symantec Web Gateway	Internet	See "Web addresses used by Symantec Web Gateway" on page 30.
123	UDP	Symantec Web Gateway	pool.ntp.org (by default)	Network Time Protocol

Table 2-6 Ports used by Symantec Web Gateway *(continued)*

Port	Protocol	From	To	Description
161	UDP	Symantec Web Gateway	SNMP servers	SNMP, if configured
389	TCP	Symantec Web Gateway	Active Directory	User information from Active Directory, if configured
443	HTTPS	Symantec Web Gateway	Internet	See "Web addresses used by Symantec Web Gateway" on page 30.
443	Proprietary	Central Intelligence Unit	Symantec Web Gateway	Status polling
443	Proprietary	Symantec Web Gateway	Central Intelligence Unit	Configuration updates
514	UDP	Symantec Web Gateway	Remote syslog	Malware alerts or system alerts to remote syslog, if configured

Web addresses used by Symantec Web Gateway

Table 2-7 describes Web addresses that Symantec Web Gateway uses.

Table 2-7 Web addresses used by Symantec Web Gateway

URL	Port	Description
http://liveupdate.symantec.com	80	Download antivirus updates
http://liveupdate.symantecliveupdate.com	80	Download antivirus updates
pool.ntp.org (by default)	123	Network Time Protocol; uses NTP, not HTTP
https://license.cobion.com	443	Software license verification for URL classification data
https://filterdb.iss.net/	443	Download URL classification data

Table 2-7 Web addresses used by Symantec Web Gateway *(continued)*

URL	Port	Description
https://threatcenter.symantec.com/	443	Download software updates and database updates for botnet fingerprints, and other types of updates; system diagnosis by Symantec Technical Support, if you initiate remote assistance

Chapter 3

Installing Symantec Web Gateway

This chapter includes the following topics:

Installing the Symantec Web Gateway appliance into a rack

The Symantec Web Gateway appliance is designed to be installed into a 19-inch (483mm) rack. If you do not have a rack, the Symantec Web Gateway appliance can rest on a stable surface.

To install the Symantec Web Gateway appliance into a rack

1. Attach the included rails to the appliance.
2. Install the appliance in a 19-inch (483mm) rack.
3. Connect the power cord to the appliance and then to a power supply.
4. Connect the second power cord if your appliance came with two power cords.

   Configure a computer to access the setup wizard next. Do not connect the Ethernet cables yet.

   See "Configuring a computer to access Symantec Web Gateway for installation" on page 34.

Configuring a computer to access Symantec Web Gateway for installation

You must connect a computer to the Mgmt port to initially set up Symantec Web Gateway. You must configure the IP address and netmask of the computer as described in this section.

See "Installation checklist" on page 17.

After the initial installation, you can access Symantec Web Gateway from a browser on any computer in your network. You can disconnect the computer from the Mgmt port and reconfigure the network settings as desired after you successfully complete the initial setup.

The exact method to use to configure the computer network settings depends on the operating system. For example, on Windows XP, access **Network Connections** on the **Control Panel**. Access the properties of the **Local Area Connection** and then access the properties of **Internet Protocol (TCP/IP)**.

To configure a computer to access Symantec Web Gateway for installation

1. Copy the license file or license XML code to the local hard drive on the computer.
2. Access the network configuration settings on the computer.

3 Set the IP address of the computer to 192.168.254.253.

4 Set the subnet mask of the computer to 255.255.255.0.

   You do not have to configure any other network settings, such as default gateway or DNS.

5 Save the settings.

6 Connect an Ethernet cable from this computer to the Mgmt port on the back of the Symantec Web Gateway appliance.

   Run the setup wizard.

   See "Running the setup wizard for initial installation" on page 35.

Running the setup wizard for initial installation

After you physically install Symantec Web Gateway and connect a computer to the Mgmt port, you can run the setup wizard.

See "Installation checklist" on page 17.

See "Steps to install Symantec Web Gateway" on page 15.

This procedure describes how to configure an appliance as a Web Gateway, not as a Central Intelligence Unit.

See "Steps to install a Central Intelligence Unit" on page 120.

To run the setup wizard for initial installation

1 Press the power button on the front of the Symantec Web Gateway appliance.

   The appliance takes several minutes to start up.

2 On the computer that is connected to the Mgmt port, start a Web browser and go to the following URL:

   http://192.168.254.254

3 On the **Welcome** panel, click **Next >>**.

4 On the **License Agreement** panel, read the license agreement, check the box, and click **Accept**.

5 On the **Install License** panel, type your company name and browse to the location of the license file or paste the XML license and click **Next >>**.

The company name does not need to match the company name that you provided to Symantec when you obtained your license. The company name that you provide here is supplied to Symantec if you enable remote assistance on Symantec Web Gateway. If you do not install a license now, there is a two week grace period during which Symantec Web Gateway functions as if a base license was installed.

6 On the **Select Server Type** panel, click **Web Gateway**.

You can only change the server type in the setup wizard, not in the Web GUI after completing the setup wizard.

See "Running the setup wizard again" on page 48.

7 On the **User Information** panel, specify the following information about the primary Web GUI system user:

Login Name	Type a login name for the primary Web GUI administrator. Use ASCII characters only. The login name is case sensitive.
Password	Type a password for the primary Web GUI administrator.
Description	Optionally, you can type a description for the current user account. This description is displayed on the **Edit User** page.
Email Address	Type an email address. Type a complete email address, such as `admin@symantecs.org`. Symantec Web Gateway sends alerts and reports to this email address. If you click the **Forgot Password?** link on the login page, a new password is sent to this address.

8 Click **Next >>**.

9 On the **Server Information** panel, specify the following information:

Server Name	Type a descriptive name for Symantec Web Gateway with ASCII characters. The server name can include spaces. The server name is not used for network access to Symantec Web Gateway. The server name appears in reports and alerts. If you use a Central Intelligence Unit to manage multiple Symantec Web Gateway appliances, this name identifies each Symantec Web Gateway appliance.
Monitoring or blocking	Click one of the following options: ■ **Monitoring** Click this option if you only want to view reports on user malware activity but not block malware. ■ **Blocking** Click this option if you want to block inbound and outbound malware for user computers at your site. You can also view reports on malware activity. See "About blocking or monitoring modes" on page 21.
Port Span/Tap or Inline	Click one of the following options: ■ **Port span/tap** Click this option if you plan to connect Symantec Web Gateway in the port span/tap network configuration. ■ **Inline** Click this option if you plan to connect Symantec Web Gateway in the inline network configuration. See "About inline or port span/tap network configurations" on page 21.
Enable separate management and inline networks.	Check this check box to specify one IP address for the Web GUI and a separate IP address for the monitoring and blocking capabilities of Symantec Web Gateway. Separate management and inline networks are recommended if you plan to connect Symantec Web Gateway in the inline network configuration.

Network Settings	Specify the network settings for Symantec Web Gateway. **Automatic (DHCP)** is not recommended. If you check **Enable separate management and inline networks**, specify the following sets of network settings: ■ Management The IP address and related network settings for the Web GUI. ■ Inline The IP address and related network settings for the monitoring and blocking capability of Symantec Web Gateway.
Proxy settings	Specify proxy settings if you use a proxy in your network. See "Configuring proxy settings in the setup wizard" on page 38.
Time zone	Select the time zone in which Symantec Web Gateway is installed.

10 Click **Finish**.

11 The appliance may reboot or the Symantec Web Gateway services may restart.

If you configured Symantec Web Gateway for blocking mode, the inline network configuration, or both, Symantec Web Gateway reboots or services restart.

Symantec Web Gateway does not reboot or restart services if you configured port span/tap monitoring mode. The Web GUI is unavailable if Symantec Web Gateway reboots or services restart. Additional configuration is necessary for Symantec Web Gateway to function properly.

See "Configuring Symantec Web Gateway after running the setup wizard" on page 39.

Configuring proxy settings in the setup wizard

If Symantec Web Gateway or user computers connect to the Internet through a proxy, configure the proxy settings.

To configure the proxy settings in the setup wizard

1 Access the setup wizard and complete the **User Information** and **Server Information** panels.

See "Running the setup wizard for initial installation" on page 35.

2 If Symantec Web Gateway connects to the Internet through a proxy, check **Use proxy for Symantec Web Gateway secure communication with Symantec Security Reponse** and specify the following information:

Proxy Server Address	Type the fully qualified domain name or IP address of the proxy server.
Proxy Port	Type the port to use on the proxy server.

3 If user computers connect to the Internet through a proxy, check **Analyze HTTP port used by proxy** and specify the port or port range.

4 Click **Finish**.

Configuring Symantec Web Gateway after running the setup wizard

After completing the setup wizard, complete the following tasks to ensure that Symantec Web Gateway functions properly.

See "Running the setup wizard for initial installation" on page 35.

To configure Symantec Web Gateway after running the setup wizard

1 On the computer that is connected to the Mgmt port, set the IP address to an IP address that is on the same network as the new IP address that you specified for Symantec Web Gateway.

Also, set the subnet mask to match the Symantec Web Gateway IP address. This process is similar to the process that you use to access the setup wizard, except that you do not use the 192.168.254.253 IP address.

See "Configuring a computer to access Symantec Web Gateway for installation" on page 34.

2 If the following conditions apply, disconnect the Ethernet cable from the Mgmt port and connect it to the LAN port on Symantec Web Gateway:

- You selected the inline networking configuration.
- You configured one IP address for the management network and a separate IP address for the inline networks.

If Symantec Web Gateway is in bypass mode in this configuration, leave the Ethernet cable connected to the Mgmt port to access the Web GUI.

With all other configurations, leave the Ethernet cable connected to the Mgmt port. In all configurations, keep the other end of the cable connected to your computer.

3 Access the Web GUI at the IP address that you specified in the setup wizard.

For example, if the IP address that you specified for the appliance is 192.168.42.24, go to the following URL:

http://192.168.42.24

4 In the Web GUI, specify your internal network and enable modules. If you plan to connect Symantec Web Gateway in the inline network configuration specify static routes.

See "Specifying internal networks" on page 41.

See "Enabling URL filtering, Internet program monitoring, and other features" on page 42.

See "Creating static routes for the inline network configuration" on page 43.

See "Specifying an email server for alerts and reports" on page 44.

See "Specifying internal email and proxy servers for report accuracy" on page 45.

5 In the Web GUI, click **Administration > Configuration > Operating Mode**, and then uncheck **Service Enabled** to disable Symantec Web Gateway.

When the service is disabled, Symantec Web Gateway is in bypass mode.

See "Ensuring Internet connectivity if Symantec Web Gateway is disabled" on page 45.

6 Disconnect your computer from the Mgmt port of the Symantec Web Gateway appliance.

You can set the TCP/IP configuration of the computer as desired and redeploy it as needed in your network.

7 Connect the LAN, WAN, and Mgmt ports as required for the network configuration and mode that you configured.

Ensure that you test that your network functions after making these connections while Symantec Web Gateway is in bypass mode.

See "Connecting Symantec Web Gateway to your network" on page 46.

8 Access the Web GUI at the IP address that you specified in the setup wizard using a computer on your LAN.

This computer does not need a special TCP/IP configuration.

9 Click **Administration > Configuration > Operating Mode**, and then check **Service Enabled** to enable Symantec Web Gateway.

10 Test Symantec Web Gateway to ensure that it is functioning properly.

See "Testing Symantec Web Gateway for successful blocking or monitoring" on page 48.

Specifying internal networks

By defining your internal networks, you specify which computers are part of your network and which computers belong to the world outside. This specification lets Symantec Web Gateway correctly identify computers with malware infections, versus potential attacks from outside the network.

To specify internal networks

1 In the Web GUI, click **Administration > Configuration > Network**.

2 If the following conditions apply, check **Apply Static Routes to Internal Networks**:

- You have configured static routes
- Your internal networks are the same as the static routes

Click **Save** and ignore the rest of this procedure.

See "Creating static routes for the inline network configuration" on page 43.

3 Under **Internal Network Configuration**, click **Add a Network**.

Normally, do not check the check box **Define internal network as addresses not in the following list**. That setting is for special cases of when Symantec Web Gateway is installed in front of a proxy.

4 In **Subnet**, type the IP address of your internal subnet.

For example, if your internal computers are in the range 10.42.24.0 to 10.42.24.255, type 10.42.24.0.

5 In **Netmask**, type the netmask for the subnet.

For example, if your internal computers are in the range 10.42.24.0 to 10.42.24.255, type 255.255.255.0.

6 In **Description**, specify a description of the internal network if desired.

7 If your internal network has computers in separate network ranges, specify additional networks.

8 Click **Save**.

Enabling URL filtering, Internet program monitoring, and other features

Some features of Symantec Web Gateway must be enabled to function. Alternatively, you can disable the features that you do not use to improve the efficiency of Symantec Web Gateway.

To enable URL filtering, Internet program monitoring, and other features

1 In the Web GUI, click **Administration > Configuration > Modules**.

2 Check the appropriate check box to enable features as follows:

Enable Application Control	Allow, monitor, or block the programs that access the Internet. Configure application control policies on the **Edit Policy** page. This feature is included in the base license. See "Configuring policies for Internet applications" on page 64.
Enable Content Filter	If you have the URL filtering license, you can enable URL filtering. Configure URL filtering policies on the **Edit Policy** page. The following setting is available for this module: ■ **Consolidation** Do not group individual URL visits under the parent domain for this time period. See "Configuring URL filtering policies for Web sites" on page 66.

Bypass Whitelist for Content Filter	If **Bypass Whitelist for Content Filter** is checked, the internal whitelist is disabled. If it is checked, the Web pages in the internal whitelist that normally would be ignored are subject to monitoring and blocking. This feature is included in the base license. The internal whitelist contains the domain names for definition and software updates of antivirus and software vendors. Due to security concerns, Symantec cannot publish the contents of the internal whitelist. If **Bypass Whitelist for Content Filter** is unchecked, URLs in the internal whitelist are not blocked or monitored for URL filtering or scanned for malware. Any subdomains of the domains in the internal whitelist are excluded from URL filtering and malware scanning also. Check the box if you do not want to omit these domains from URL filtering and malware scanning.
Record browse time	Records the approximate amount of time that each user spends using a Web browser to view Web sites. This feature is included in the base license. The following settings are available for this module: ■ **Threshold** Web browsing activity under this value is not recorded. The default is 5 minutes. ■ **Sensitivity** If no Web browsing activity is detected after this time has elapsed, stop tabulating the browse time. The browse time may be ignored or recorded, depending on the **Threshold** value. The default is 3 minutes. See "About the browse time report" on page 95.

3 Click **Save**.

Creating static routes for the inline network configuration

Static routes are required if you plan to connect Symantec Web Gateway in the inline network configuration. You must configure a static route to each internal

subnet beyond the main switch. Whenever you add an additional subnet, you must add a static route to Symantec Web Gateway. If you do not add a static route when you add a subnet, end users on that new subnet may see a "Page not found" error in their Web browsers.

A static route is a path to an internal subnet through an intermediate switch. In the inline network configuration, you connect the LAN port on Symantec Web Gateway to a main switch. If that switch connects to one or more subnets, you must configure a static route for each subnet beyond the switch that is connected to Symantec Web Gateway.

To create static routes for the inline network configuration

1. In the Web GUI, click **Administration > Configuration > Network**.
2. Click **Add a Static Route**.
3. In **Destination**, type the IP address of the subnet.

   For example, if computers on the router have IP addresses in the range 10.10.20.0 to 10.10.20.255, type 10.10.20.0.
4. In **Netmask**, type the netmask for the router.

   For example, if you specified a destination of 10.10.20.0, type 255.255.255.0.
5. In **Gateway**, type the IP address of the router or switch.

   The gateway is the IP address of the router, such as 10.10.20.100.
6. Add additional static routes for each internal subnet.
7. Click **Save**.

Specifying an email server for alerts and reports

Symantec Web Gateway requires an email server to send email to administrators, such as reports and alerts.

To specify an email server for alerts and reports

1. In the Web GUI, click **Administration > Configuration > Email**.
2. Specify the email server IP address, port, and email address from which email should appear to be from.

   The email server that you specify must support the SMTP email protocol.
3. Click **Save**.

Specifying internal email and proxy servers for report accuracy

Because of their special roles, you must specify internal email and proxy servers to ensure that report results are accurate.

To specify internal email and proxy servers for report accuracy

1. In the Web GUI, click **Administration > Configuration > Servers**.
2. Click **Add a server**.
3. Specify the server parameters.
4. Click **Save**.

Ensuring Internet connectivity if Symantec Web Gateway is disabled

When you configure the appliance in the inline network configuration, the appliance enters bypass mode if it cannot function or is turned off. In bypass mode, Internet traffic is routed through the LAN and WAN ports but no monitoring or blocking occurs. For bypass mode to function properly, ensure that you use the proper type of Ethernet cables to connect to the LAN. Bypass mode is indicated by LEDs on the back of the Symantec Web Gateway appliances if it is not turned off.

See "Connections and indicators on Symantec Web Gateway" on page 20.

Note: If you connect the wrong type of Ethernet cable from Symantec Web Gateway to the LAN, Internet connectivity can be blocked when Symantec Web Gateway is disabled or off.

In the inline network configuration, you may need to connect a crossover Ethernet cable between the LAN port on Symantec Web Gateway and the main LAN switch. One or two crossover cables are included with Symantec Web Gateway, depending on the number of LAN ports on your appliance. Most Ethernet cables are straight-through cables.

Table 3-1 Connecting the LAN cable in the inline network configuration

LAN auto sensing behavior	Cable options for Symantec Web Gateway LAN port
LAN switch connected to Symantec Web Gateway has auto sensing that detects the cable type and adjusts to properly route network traffic.	You can connect either a straight-through or a crossover Ethernet cable from the LAN port on Symantec Web Gateway to the main LAN switch. However, Symantec recommends that you install the type of cable that is recommended in the row below. If the LAN switch is unintentially turned off, auto sensing may not function.
LAN switch connected to Symantec Web Gateway does not have auto sensing and automatic correction for the Ethernet cable type.	You must connect the correct type of Ethernet cable to ensure that bypass mode works. The type of cable to use depends on the type of cable that was connected between the WAN and LAN before you installed Symantec Web Gateway, as follows: ■ If the Ethernet cable between the WAN and LAN was a straight-through cable, connect a crossover Ethernet cable to the Symantec Web Gateway LAN port. ■ If the Ethernet cable between the WAN and LAN was a crossover cable, connect a straight-through Ethernet cable to the Symantec Web Gateway LAN port. In all cases, connect a straight-through Ethernet cable from the WAN to the WAN port on Symantec Web Gateway.

If you configured Symantec Web Gateway in the port span/tap network configuration and the appliance is turned off or disabled, Internet traffic passes unchanged. In the port span/tap network configuration, the appliance will never block Internet traffic if it is turned off or disabled. Always use a straight-through Ethernet cable to connect the appliance to the network tap or port configured in span mode.

Connecting Symantec Web Gateway to your network

After completing the setup wizard and specifying your network in the Web GUI, connect Symantec Web Gateway to your network. Symantec recommends that you make the connections while Symantec Web Gateway is disabled to test that Internet connectivity works while the appliance is disabled.

See "Configuring Symantec Web Gateway after running the setup wizard" on page 39.

To connect Symantec Web Gateway to your network

1. Ensure that Symantec Web Gateway service is disabled.

   You can check the Symantec Web Gateway service status at **Administration > Configuration > Operating Mode**.

2. Connect the LAN, WAN, and Mgmt ports as required for the network configuration and mode that you configured.

   See "Port connections for typical network configurations" on page 22.

3. With Symantec Web Gateway service disabled, try to access the Internet from a computer in the LAN.

   You should be able to access the Internet. The bypass LEDs on the back of the Symantec Web Gateway appliance should be on.

   See "Connections and indicators on Symantec Web Gateway" on page 20.

Accessing the Web GUI

You use the Web GUI to configure Symantec Web Gateway. Access the Web GUI from a Web browser on any computer in the LAN connected to Symantec Web Gateway. Ensure that you have first run the setup wizard and connected the Symantec Web Gateway appliance to your network.

To access the Web GUI

1. On the computer in the LAN connected to Symantec Web Gateway, start a Web browser.

2. In the Web browser, type `http://` followed by the IP address that you specified for the Symantec Web Gateway appliance in the setup wizard.

   For example, if the IP address that you specified for the appliance is 192.168.42.24, go to the following URL:

   http://192.168.42.24

3. For certain Web browsers, you may need to configure a certificate security exception to access the Web GUI.

   Typically this step is only required at the first login per computer.

Testing Symantec Web Gateway for successful blocking or monitoring

Symantec has a Web site that you can use to test that Symantec Web Gateway blocks or monitors network data.

To test Symantec Web Gateway for successful blocking or monitoring

1. Start a Web browser on a computer in the LAN that is connected to Symantec Web Gateway.

   If Symantec Web Gateway is in blocking mode and you have enabled policy management, the computer must be included in a policy that blocks spyware access.

2. On the Internet, go to the following URL:

   www.symantec.com

   The Symantec Web site should display normally without any block messages.

3. On the Internet, go to the following URL:

   testwebgateway.com/test/bltest.htm

   Blocking mode or monitoring mode should be indicated as follows:

Blocking mode	If you have configured Symantec Web Gateway in blocking mode, a block page appears in your Web browser. If the block page does not appear, Symantec Web Gateway is not correctly configured to block access to spyware.
Monitoring mode	If you have configured Symantec Web Gateway in monitoring mode, the test page appears in your Web browser. To check for successful monitoring, find the computer in the Web GUI. The report should show that the computer accessed a malware page. If the Web GUI does not indicate that the computer accessed a malware page, Symantec Web Gateway is not correctly configured to monitor access to spyware.

Running the setup wizard again

You can run the setup wizard after running it the first time. You might want to run the setup wizard again to address the following problems:

- You forgot the password for the primary system user and do not have access to the email address that you specified in the setup wizard. However, if you do have access to the email address that you specified, you can have the password emailed to the account.
  See "Resetting the Web GUI password for the primary system user" on page 99.
- You forgot the logon name for the primary system user.

If you have access to another system user account with **Administration** permission, you can resolve these two issues. Log on to the Web GUI and change the logon name or password for the primary system user.

To run the setup wizard again you must first access Symantec Web Gateway using the Serial Console. Your initial configuration choices are retained when you run the setup wizard again.

To run the setup wizard again

1. Connect a computer to the Serial Console on Symantec Web Gateway.

   See "Serial Console access to Symantec Web Gateway" on page 99.
2. Log on to the Serial Console.
3. In the Serial Console, select the option to unlock the setup wizard.
4. Exit from the Serial Console.
5. On a computer that is connected to Symantec Web Gateway, open a Web browser and go to the URL that you typically use to access Symantec Web Gateway.

   The setup wizard should display. Complete the setup wizard.

   See "Running the setup wizard for initial installation" on page 35.

Chapter 4

Configuring policies

This chapter includes the following topics:

About policies

Table 4-1 describes the types of actions that you can configure using Symantec Web Gateway policies. If you configure Active Directory integration, you can also create policies by user names, workgroups, organizational units, or departments.

If you plan to block Web sites by category, you should initially configure a policy to monitor that category of Web sites. After a period of time, check the reports to see what Web sites have been monitored. That way you can be sure that your policy matches only the types of Web sites that you had in mind. Also, test that the desired action occurs by accessing the Symantec Web Gateway test page from a computer in each policy work group.

See "Testing Symantec Web Gateway for successful blocking or monitoring" on page 48.

Note: You must install Symantec Web Gateway in the inline network configuration to block file downloads. If you configure Symantec Web Gateway in the port span/tap network configuration, the block action is not available in the Web GUI.

See "About inline or port span/tap network configurations" on page 21.

Table 4-1 Policies

Action	Description
Block or allow select Internet applications	Block, monitor, or allow access to individual Internet applications or categories of Internet applications. See "Configuring policies for Internet applications" on page 64.
Block or allow Web sites by category	Block, monitor, or allow access to individual Web sites or categories of Web sites. To block or allow access to Web sites by category, you must have the URL filtering license. See "Configuring URL filtering policies for Web sites" on page 66.

Table 4-1 Policies *(continued)*

Action	Description
Block specific Web sites or downloads	Use the blacklist to block access to specific Web sites or downloads. You must use a blacklist in a policy for it to take effect. See "Blocking or monitoring Web sites using the blacklist" on page 72. See "Blocking or monitoring file transfers using the blacklist" on page 73.
Allow specific Web sites or downloads	Use the whitelist to allow access to a specific Web site or download. See "Allow Web site access using the whitelist" on page 75.
Block, monitor, or ignore spyware by category, severity, or detection type	Block, monitor, or ignore certain categories of spyware. Generally you should block all spyware for all users. If necessary, you can configure exceptions for certain categories of spyware for certain computers. See "Configuring policies for malware" on page 61.
Quarantine infected computers	Prevent malware infected computers from accessing the Internet. See "Quarantining malware infected computers" on page 70.
Enforce user authentication	Require authentication before users access Web sites. You must configure Active Directory integration with NTLM for this policy to function. The authentication is typically invisible to users. In some cases users may see an authentication request in their Web browsers. You can only configure authentication policies for IP addresses and subnets because Active Directory information is not available before authentication. See "Configuring NTLM user authentication behavior" on page 71.

Table 4-1 Policies *(continued)*

Action	Description
Allow after hours access	Allow users to access categories of Web sites outside of normal working hours. For example, you can block access to entertainment Web sites during working hours but allow access after working hours. You specify the times for after hours access and also non-working days. To allow after hours access, you must have the URL filtering license. See "Allowing after hours access to Web sites" on page 69.

Configuring policy precedence order

Policies are evaluated in the order that they appear on the **Policies > Configuration** page. The policy at the top of the page is evaluated first. If more than one policy applies to the same computer, only the rules in the first matching policy determine what action to take. Symantec Web Gateway ignores the policies after the matching policy.

Assume that you define a policy for malware that applies to subnet 192.168.0.0 and a separate policy for malware that applies to VLAN ID 2. If a computer on VLAN 2 using IP address 192.168.0.5 encounters malware, only the first matching policy determines the action to take.

Adjusting the precedence is usually only necessary if you mix policy work groups of different network types. If you consistently use subnet, IP range, or VLAN ID to define all of your work groups, new policies are inserted in the correct order. If you use work groups of different network types in your policies, ensure that the policies are ordered as you desire. Test that the desired action occurs by accessing the Symantec Web Gateway test page from a computer in each policy work group.

See "Testing Symantec Web Gateway for successful blocking or monitoring" on page 48.

You can also change the order of **Spyware Category**, **Spyware Severity**, and **Detection Type** within a policy.

To configure policy precedence order

1. In the Web GUI, click **Policies > Configuration**.
2. Click an arrow symbol next to a policy to move the policy up or down.

3 Repeat this process for other policies until the policies are the order that you want.

4 Click **Save and Activate Changes**.

Download behavior in user Web browsers

You can configure Symantec Web Gateway policies to scan file downloads from the Internet for malware such as spyware and viruses. The **File and Active Content Detection** setting for policies determines the Web browser download behavior. The **Block** and **Use Default** actions are not available for the port span/tap network configuration.

See "About inline or port span/tap network configurations" on page 21.

For both the **Block** or **Monitor** actions, if the download takes longer than a few seconds, Symantec Web Gateway displays a message in the user Web browser. The message indicates that Symantec Web Gateway is scanning the download. The contents of this patience page cannot be changed. However, you can change the language used on this page and the image that is displayed on the page.

See "End user pages for blocked Web sites, file transfers, and infections" on page 77.

Table 4-2 Download behavior in user Web browsers

Action	Inline network configuration	Port span/tap network configuration	Description
Block	Available	Not available	Symantec Web Gateway scans the download. If malware is detected, Symantec Web Gateway displays a message in the user browser. See "End user pages for blocked Web sites, file transfers, and infections" on page 77.
Monitor	Available	Available	Symantec Web Gateway scans the download. If malware is detected, it is recorded for display in reports.
Ignore	Available	Available	Symantec Web Gateway does not scan the download.
Use Default	Available	Not available	The action that you set for the **Spyware Default** is used.

Blocking behavior for Internet applications, malware, and URL filtering

Symantec Web Gateway can block file transfers, Internet applications, malware phone home attempts, and Web pages. You can configure blocking in the following types of policies:

Application control policy	You can allow, block, or monitor Internet access for applications with the application control policy settings. See "Configuring policies for Internet applications" on page 64.
Malware policy	Malware includes spyware, viruses, worms, Trojans, botnets, keyloggers, and so on. See "Configuring policies for malware" on page 61.
URL filtering policy	Symantec Web Gateway can block, monitor, or allow access to categories of Web sites. To block categories of Web sites, you must have the URL filtering license. See "Configuring URL filtering policies for Web sites" on page 66. See "Installation checklist" on page 17.
Blacklist	You can block file downloads by file extension using the blacklist. See "Blocking or monitoring file transfers using the blacklist" on page 73.

See "About policies" on page 52.

The method that Symantec Web Gateway uses to block file transfers, Internet applications, malware phone home attempts, and Web pages depends on the source, action, and the policy that applies.

Table 4-3 Blocking methods

Blocking method	Description	Examples
End user blocking page	For downloads and URL access that a user initiates in a Web browser, Symantec Web Gateway displays an end user blocking page to block access. The requested action does not occur and the blocking page is displayed instead.	A user's computer is part of a malware policy. The user attempts to download a file using a Web browser. Symantec Web Gateway detects a virus in the file. Symantec Web Gateway displays a blocking page instead of allowing the file download.
File corruption	For file uploads in a Web browser and file downloads not in a Web browser, Symantec Web Gateway intentionally corrupts the contents of a file to disable malware.	A user's computer is part of a malware policy. The user attempts to download a file using FTP. Symantec Web Gateway detects a virus in the file. The download proceeds. However, Symantec Web Gateway corrupts the contents of the file to disable the virus.
Interrupted connection	For malware phone home attempts, application control, and IM file transfers, Symantec Web Gateway interrupts the connection to block access.	A user attempts to use a peer-to-peer file sharing application that is blocked in an application control policy. The peer-to-peer file sharing application does not work for the user. The peer-to-peer file sharing application may display an error.

If you configure Symantec Web Gateway in the port span/tap network configuration, it cannot provide the same level of blocking as the inline network configuration.

See "About inline or port span/tap network configurations" on page 21.

Table 4-4 Blocking behavior for policies

Application	Application action	Policy	Browser patience page	Blocking method	Supported network configurations
Web browsers	Download .exe, .zip, .rar, .dll, and .cab files that are over 50,000 bytes	Antivirus scan from malware policy	Yes	End user blocking page	Inline only

Table 4-4 Blocking behavior for policies *(continued)*

Application	Application action	Policy	Browser patience page	Blocking method	Supported network configurations
Web browsers	Download file	Antivirus scan from malware policy	No	End user blocking page	Inline only
Web browsers	Download file	Blacklist block by file extension	No	End user blocking page	Inline and port span/tap
Web browsers	Upload file	Antivirus scan from malware policy	No	Corrupts file	Inline only
Web browsers	Upload file	Blacklist block by file extension	No	End user blocking page	Inline only
Web browsers	Browse to URL	Malware or URL filtering	No	End user blocking page	Inline and port span/tap
FTP	Upload file or download file	Antivirus scan from malware policy	No	Corrupts file	Inline only
Malware phone home	Any network activity	Malware	No	Interrupts connection	Inline and port span/tap
Applications available for application control	Any network activity	Application control	No	Interrupts connection	Inline and port span/tap Some limitations for port span/tap as noted in Web GUI
IM applications	Upload file or download file	Application control	No	Interrupts connection	Inline and port span/tap Some limitations for port span/tap as noted in Web GUI
IM applications	Upload file or download file	Antivirus scan from malware policy	No	Corrupts file	Inline only

Table 4-4 Blocking behavior for policies *(continued)*

Application	Application action	Policy	Browser patience page	Blocking method	Supported network configurations
Applications that access the Internet, such as for software updates	Download file	Antivirus scan from malware policy	No	Corrupts file	Inline only
Unknown Web browser applications	Download file	Antivirus scan from malware policy	No	Corrupts file	Inline only

Specifying computers or users for policies

Policies can act on all computers that Symantec Web Gateway is aware of or policies can act on particular groups of computers. If you configure Active Directory integration, you can also create policies by user names, workgroups, etc.

If you attempt to configure a policy that includes an Active Directory user or workgroup, Symantec Web Gateway may display an error if the user or workgroup was recently added. To correct this situation, access the user in a report and click **Refresh**. In the Web GUI, click **Reports > Enterprise Summary** and then click the user.

To specify computers or users for policies

1. In the Web GUI, click **Policies > Configuration**.
2. At the top of the page, ensure that **Enable Policy Management** is checked.

   All policies are deactivated if **Enable Policy Management** is unchecked.
3. Click **Create a New Policy**.
4. At the top of the page, specify the following information:

Base Policy On: (optional)	Optionally, click an existing policy or policy template on which to base your new policy. If you click an existing policy or policy template, the page is updated with the settings from that policy or policy template.

Policy Name:	Type a name for the policy. The name appears on the **Policies > Configuration** page.
Policy Description:	Type a description for the policy. The description appears on the **Policies > Configuration** page.
Block Page Message Group:	Click the group of messages to display in the Web browsers of users for a blocked Web site, blocked file download, or a malware infection. You configure message groups on **Administration > End User Pages**. If you have not configured message groups, click **Default**. See "End user pages for blocked Web sites, file transfers, and infections" on page 77.
Applies to:	Click one of the following options: ■ **All computers** This policy applies to all computers that are specified as part of the **Internal Network Configuration** on the **Administration > Configuration > Network** page. ■ **Specific Work Groups** This policy applies to the computers that you specify under **Work Groups** on this page.

5 If you clicked **Specific Work Groups** for **Applies to:**, under **Work Groups** click a **Network Type** and specify the computers or users for the group.

To use any of the LDAP options, you must have configured Active Directory integration. The ability to choose departments, organizational units, or workgroups depends on your Active Directory configuration.

See "About Active Directory integration" on page 101.

Subnet	Specify the following options: ■ **Subnet:** Type the IP address for the subnet. ■ **Netmask:** Type a subnet mask for the subnet.

IP Range	Specify the following options: ■ **First IP:** Type the IP address for lowest numbered IP address in the range. ■ **Last IP:** Type the IP address for highest numbered IP address in the range. The first and last IP addresses that you specify are included in the range.
VLAN ID	Type a VLAN ID.
LDAP Department	Click a department. The departments are populated from Active Directory. For the **Other** option, type a department.
LDAP Organizational Unit	Click an organizational unit. The organizational units are populated from Active Directory. For the **Other** option, type an organizational unit.
LDAP Workgroup	Click a workgroup. The workgroups are populated from Active Directory. For the **Other** option, type a workgroup.
LDAP User Name	Type an Active Directory user name using the form that is configured in Active Directory.

6 Continue configuring the policy.

See "About policies" on page 52.

Configuring policies for malware

Symantec Web Gateway can block file uploads and file downloads when it detects malware in the file. Symantec Web Gateway can also block infected computers from accessing the Internet. Symantec Web Gateway can block, monitor, or ignore malware by category. Generally you should block all malware for all users. If necessary, you can configure exceptions for certain categories of malware for certain computers.

See "Blocking behavior for Internet applications, malware, and URL filtering" on page 56.

Note: Malware blocking for all computers is not enabled by default. To enable malware blocking for all computers, configure a policy for all computers and set the **Spyware default** action to **Block**.

The following actions are available for the **File and Active Content Detection**, **Spyware Category**, **Spyware Severity**, **Detection Type**, and **Spyware Default** settings:

Use Default	Use the **Spyware Default** action for this type of malware. This action is not applicable to the **File and Active Content Detection** or **Spyware Default** setting.
Block	Block this type of malware and record detected malware of this type for reports.
Monitor	Allow this type of malware but record detected malware of this type for reports.
Ignore	Allow this type of malware and do not record detected malware of this type for reports.

Note: You must install Symantec Web Gateway in your network in the inline network configuration to block file downloads. If you configure Symantec Web Gateway in the port span/tap network configuration, the block action is not available in the Web GUI.

See "About inline or port span/tap network configurations" on page 21.

To configure policies for malware

1. Specify the policy name and the range of computers to include in the policy.

   See "Specifying computers or users for policies" on page 59.

2. Continuing on the **Policies > Configuration** page, locate **File and Active Content Detection**, **Spyware Category**, **Spyware Severity**, **Detection Type**, and **Spyware Default**.

3. Under **Spyware Default**, click **Block**, **Monitor**, or **Ignore**.

   The **Spyware Default** action is the default action for the **Spyware Category**, **Spyware Severity**, and **Detection Type** settings. When you click **Use Default** for any of those settings, the **Spyware Default** action is used.

4 To configure the action for file downloads, click an action next to **File and Active Content Detection**.

See "Download behavior in user Web browsers" on page 55.

5 To specify an action for a specific malware category, click **Add Category** next to **Spyware Category**, click a category, and click an action.

6 To specify the action for malware severities, click an action under **Spyware Severity**.

Symantec Web Gateway groups malware into the following severities:

Critical	Critical malware poses an imminent security risk that can result in theft of confidential data, loss of control over the computer, or both.
Major	Major malware changes the expected system behavior, uses system resources in an unwanted manner, or both. Major malware may affect productivity.
Minor	Minor malware is a nuisance and a potential privacy risk. It primarily affects the user's browsing experience by displaying pop-ups and other ads, and may also send out browsing information.

7 To specify the action for malware detection types, click an action under **Detection Type**.

Symantec Web Gateway detects Internet traffic to and from malware on computers in your network. You can configure actions for the following detection types:

Infection	Malware has attempted to phone home to a computer outside the network. The malware is on a computer on your network.
Attack	A remote computer has attempted to access an infected computer on your network or to send a malicious network element such as a network worm.
Malware URL	Malware has attempted to access a known malware Web site. The malware is on a computer on your network.

8 Configure other policy settings as desired.

9 Click **Save**.

10 On the **Policies > Configuration** main page, click **Save and Activate Changes**.

Configuring policies for Internet applications

Symantec Web Gateway can allow, block, or monitor Internet access for applications with the application control policy settings. For example, you can prevent peer-to-peer sharing, streaming media, and Internet-dependent games from accessing the Internet for some or all computers in your network. You can configure access by category or by the specific programs that are known to Symantec Web Gateway.

See "About policies" on page 52.

See "Blocking behavior for Internet applications, malware, and URL filtering" on page 56.

Note: You must enable the application control module to monitor or block applications.

See "Enabling URL filtering, Internet program monitoring, and other features" on page 42.

Symantec Web Gateway contains network signatures for a large number of commonly used Internet applications. However, you cannot monitor or block any Internet applications that Symantec Web Gateway is not aware of.

If you block Internet access for an application, the application typically does not function normally or displays an error to the user. The cause of the malfunction may not be apparent to the user. As a best practice, you should notify users of the types of applications that you block as part of your site policy.

To configure policies for Internet applications

1. Specify the policy name and the range of computers to include in the policy.

   See "Specifying computers or users for policies" on page 59.

2. Continuing on the **Policies > Configuration** page, locate **Application Control Categories**.

3. To specify the default action type for all Internet applications that are known to Symantec Web Gateway, click one of the following options:

Block All	By default, block all applications from accessing the Internet. Attempts to use blocked applications are displayed in reports.
Allow All	By default, allow all applications to access the Internet.
Monitor All	By default, monitor all applications that access the Internet. Internet access for applications is allowed but application usage is displayed in reports.
Details All	Expand the categories to display the actions for specific applications.

   You can individually set the action options for specific categories or applications after selecting one of these options.

4 To specify the action type for categories, click one of the following options for the category:

Block	By default, block applications in this category from accessing the Internet. Attempts to use blocked applications are displayed in reports.
Allow	By default, allow applications in this category to access the Internet.
Monitor	By default, monitor Internet applications in this category . Internet access for applications is allowed but application usage is displayed in reports.
Details	Expand the category to display the actions for specific applications. To discard individual application settings, click **Block**, **Allow**, or **Monitor** next to the category.

5 Configure other policy settings as desired.

6 Click **Save**.

7 On the **Policies > Configuration** main page, click **Save and Activate Changes**.

Configuring URL filtering policies for Web sites

Symantec Web Gateway can block, monitor, or allow access to categories of Web sites. For example, you can block access to gambling Web sites, allow access to business Web sites, and monitor access to entertainment Web sites. To block Web sites by category, you must have the URL filtering license.

See "Installation checklist" on page 17.

Note: You must enable the content filter module to monitor or block Web sites.

See "Enabling URL filtering, Internet program monitoring, and other features" on page 42.

When a user attempts to access a Web site in a blocked category, a message displays in the Web browser instead of the Web site. You can configure the message.

See "End user pages for blocked Web sites, file transfers, and infections" on page 77.

See "Blocking behavior for Internet applications, malware, and URL filtering" on page 56.

You can configure content filter exceptions for specific Web sites. Content filter exceptions apply to a single policy. You set Symantec Web Gateway to allow, block, or monitor the Web site in each content filter exception. For example, assume that you set the **Spam URLs** filtering category to **Block** and that www.blocksads.com is in that category. For that policy, if you want to monitor access instead of block access, set a content filter exception for www.blocksads.com to **Allow**. These content filter exceptions act like a policy-specific blacklist or whitelist. Symantec Web Gateway also provides separate blacklist and whitelist functionality that provide more global behavior.

See "Blocking or monitoring Web sites using the blacklist" on page 72.

See "Allow Web site access using the whitelist" on page 75.

To configure policies for Web sites

1. Specify the policy name and the range of computers to include in the policy.

   See "Specifying computers or users for policies" on page 59.

2. Continuing on the **Policies > Configuration** page, locate **Multiple Categories**.

   To configure after hours access, check **Allow After Hours Configuration** and specify those settings.

   See "Allowing after hours access to Web sites" on page 69.

3. Under **Multiple Categories**, click one of the following:

Restrictive: Block takes precedence	If a block action and an allow action both apply to a Web site category, the Web site is blocked. **Restrictive: Block takes precedence** is the default setting.
Permissive: Allow takes precedence	If a block action and an allow action both apply to a Web site category, the Web site is allowed.

   Web sites can be classified under more than one category. For example, a Web site selling sports equipment might be categorized as both a sports Web site and a shopping Web site. This option determines the action that Symantec Web Gateway takes if conflicting actions apply to a Web site.

4 To specify the default action type for all Web site categories, click one of the following options:

Block All	By default, block all Web site categories. Attempts to access blocked Web sites are displayed in reports.
Allow All	By default, allow access to all Web site categories.
Monitor All	By default, monitor all Web site categories. Access to all Web sites is allowed but Symantec Web Gateway records visits by category for display in reports.

You can individually set the action options for specific categories or subcategories after selecting one of these options.

5 To specify the action type for categories, click one of the following options for the category:

Block All	By default, block Web sites in this category. Attempts to access blocked Web sites are displayed in reports.
Allow All	By default, allow access to Web sites in this category.
Monitor All	By default, monitor Web sites in this category. Symantec Web Gateway allows access to Web sites in this category. Symantec Web Gateway records visits by category for display in reports.

6 To specify the action type for subcategories, click **Block**, **Allow**, or **Monitor**.

7 To configure access for a specific Web site or IP address, click **Add an Exception**.

Specify a domain name or IP address and then click an action type. If you specify a domain name, type only the domain name. Omit the `http://` prefix and any slashes such as for folders in the URL.

Alternatively, you can click an action type and import a text file that contains one domain name or IP address per line. The action type you click is set for all addresses in the file.

8 Configure other policy settings as desired.

9 Click **Save**.

10 On the **Policies > Configuration** main page, click **Save and Activate Changes**.

Allowing after hours access to Web sites

You can configure Symantec Web Gateway to allow users to access categories of Web sites outside of normal working hours. For example, you can block access to entertainment Web sites during working hours but allow access after working hours. You specify non-working days and the times for after hours access. To allow after hours access, you must have the URL filtering license. The after hours setting applies to URL filtering only.

See "Configuring URL filtering policies for Web sites" on page 66.

To allow after hours access to Web sites

1 Specify the policy name and the range of computers to include in the policy.

See "Specifying computers or users for policies" on page 59.

2 Continuing on the **Policies > Configuration** page, locate **After Hours Settings**.

3 Click **Allow After Hours Configuration**.

4 To assign an entire day as a non-working day, check the box for that day of the week next to **Non-Working Days**.

The 24 hour period for a day is considered the after hours period.

5 For **After Hours Start**, click the hour and minute after which after hours exceptions apply on working days.

Working days are the days unchecked next to **Non-Working Days**.

6 For **After Hours End**, click the hour and minute before which after hours exceptions apply on working days.

7 Specify the after hours behavior for **Content Filter Categories** under **After Hours Exception**.

See "Configuring URL filtering policies for Web sites" on page 66.

To copy the working hour settings to the **After Hours Exception**, click **Copy from At All Times**.

8 Configure other policy settings as desired.

9 Click **Save**.

10 On the **Policies > Configuration** main page, click **Save and Activate Changes**.

Quarantining malware infected computers

You can configure a policy to quarantine infected computers. When a computer is quarantined, users on that computer see a blocking page in the Web browser for every URL. Symantec recommends that you create a specific blocking page for quarantined computers. The blocking page for quarantined computers can include malware clean up information and contact information for your site's IT help desk.

To quarantine infected computers you must create two policies:

1. One policy to assign infected computers to the quarantine
2. Another policy to perform some action for computers in the quarantine, such as to block

You may want to configure a **Block Page Message Group** specific to the quarantined computers.

See "End user pages for blocked Web sites, file transfers, and infections" on page 77.

To assign infected computers to the quarantine

1. Specify the policy name and the range of computers to include in the policy.

   See "Specifying computers or users for policies" on page 59.
2. Continuing on the **Policies > Configuration** page, locate **Infected Client Cleanup**.
3. Optionally, click **Use this policy for cleanup settings only** to hide other policy settings.
4. Next to **Prompt Infected Clients in Work Groups**, click **Quarantine**.
5. Configure other policy settings as desired.
6. Click **Save**.
7. On the **Policies > Configuration** main page, click **Save and Activate Changes**.

To configure a policy for computers in the quarantine

1. Specify the policy name and the range of computers to include in the policy.

   If you created a **Block Page Message Group** for quarantined computers, select that when you specify the policy name and work group.

   See "Specifying computers or users for policies" on page 59.
2. Continuing on the **Policies > Configuration** page, click **Use this policy for quarantined users only.**
3. Under **Detection Type** and next to **Infection**, click **Block**.

4 Click **Save**.

5 On the **Policies > Configuration** main page, click **Save and Activate Changes**.

Configuring NTLM user authentication behavior

If you have configured Active Directory integration with NTLM, you can control authentication behavior with a policy. By periodically authenticating users, Symantec Web Gateway can enforce policies that employ Active Directory user names or groups and track user activity in reports.

See "About Active Directory integration" on page 101.

To configure NTLM user authentication behavior

1 Specify the policy name and the range of computers to include in the policy.

   You can configure the range of computers using IP range and subnet based work groups but not using any of the LDAP **Network Types**.

   See "Specifying computers or users for policies" on page 59.

2 Continuing on the **Policies > Configuration** page, locate **User Authentication**.

3 Click **Authentication settings policy.**

4 Click one of the following:

Ignore Authentication	Never authenticate the specified range of computers. This option may be appropriate for configuring exceptions for administrators.
Enforce Authentication	When user credentials expire, check for and enforce authentication. Selecting this option may result in authentication request in user Web browsers. If users fail authentication, a blocking page displays in the Web browser. See "Ensuring compatibility with NTLM" on page 115.

Authenticate, No Enforce	When user credentials expire, check for but do not enforce authentication. To prevent authentication dialog boxes if you select this option, ensure that the following conditions are met: ■ User Web browsers are set to automatically logon to the intranet ■ Symantec Web Gateway has a host name ■ The **Use Interface Name for NTLM Authentication** box is checked on the **Administration > Configuration > Authentication** page

5 Click **Save**.

6 On the **Policies > Configuration** main page, click **Save and Activate Changes**.

Blocking or monitoring Web sites using the blacklist

You can block or monitor specific Web sites by adding them to the blacklist. When you add a Web site to the blacklist, it affects all policies. If a URL access occurs that matches the blacklist entry, Symantec Web Gateway checks for a matching policy for the computer. The **Spyware Severity** and **Spyware Category** in the matching policy determine the action that Symantec Web Gateway takes.

You can also block and monitor specific Web sites for a single policy using content filter exceptions. Because they act on single policies only, content filter exceptions provide a more targeted method of blocking and monitoring Web sites. You need the URL filtering license to configure content filter exceptions. You do not need the URL filtering license to block or monitor Web sites using the blacklist.

See "Configuring URL filtering policies for Web sites" on page 66.

To block or monitor Web sites using the blacklist

1 In the Web GUI, click **Policies > Blacklist**.

2 Click **Add a Blacklist Entry**.

You can also add blacklist entries from a text file. List one domain name or IP address per line in the file. You assign the same **Category** and **Severity** for all domain names and IP addresses in the file.

3 Type a **Name** for the blacklist entry.

The name is displayed on the blacklist page and in reports.

4 For **Block Type**, click **Block by URL**.

5 For **Domain or IP**, type the Web site domain name or IP address.

For example, type **www.example.com** to monitor or block all URLs that start with `www.example.com`. Use an asterisk as a wildcard for part of the domain. For example, type ***.example.com** to match URLs that start with `example.com`, `www.example.com`, and `mail.example.com`. Do not include the `http://` part of a URL. Do not include any part of a URL other than the domain name.

6 For **Keyword** you can optionally type a partial URL to associate with the domain specified in **Domain or IP**.

For example, if you type **warez**, the following URLs would match: `www.example.com/warez/index.html` and `www.example.com/folder/warez.html`. The asterisk wildcard is not valid for **Keyword**. Do not include slashes in the **Keyword**.

7 For **Description**, type a description.

The **Description** is displayed on the blacklist page and in reports.

8 Click a **Severity**.

The blacklist **Severity** relates to the policy **Spyware Severity**. The action set for **Spyware Severity** in a matching policy applies to the blacklist entry. The **Severity** is also recorded and used in reports.

9 Click a **Category**.

The blacklist **Category** relates to the policy **Spyware Category**. The action set for **Spyware Category** in a matching policy applies to the blacklist entry. In addition to the predefined categories, you can assign the URL to one of the three Custom Restricted Lists. The **Category** is also recorded and used in reports.

10 Click **Save**.

Blocking or monitoring file transfers using the blacklist

You can block or monitor file downloads and file uploads by specifying the file extension and, optionally, file contents in the blacklist. Symantec Web Gateway does not verify that the contents of the file match the extension.

If a file transfer occurs that matches the blacklist entry, Symantec Web Gateway checks for a matching policy for the computer. The **Spyware Severity** and **Spyware**

Category in the matching policy determine the action that Symantec Web Gateway takes on the file transfer.

To block or monitor file downloads using the blacklist

1. In the Web GUI, click **Policies > Blacklist**.
2. Click **Add a Blacklist Entry**.
3. Type a **Name** for the blacklist entry.

   The name is displayed on the blacklist page and in reports.
4. For **Block Type**, click **Block by File Extension**.
5. You can optionally click a **File Type** to populate **File Extension** with commonly used extensions for that file type.
6. Type file extensions to match in the **File Extension** box.

   If you clicked a **File Type**, you can add or delete file extensions. Separate each file extension with a comma. The asterisk wildcard is not valid for **File Extension**. Do not include periods when typing a file extension.
7. For **Keyword** you can optionally type text to match in the contents of files.

   Only files with the extensions that you specify that contain at least one of the keywords match. Separate multiple keywords with commas. The asterisk wildcard is not valid for **Keyword**.
8. For **File Direction**, click one of the following:

Outbound	Block the matching files that users attempt to upload to a remote computer.
Inbound	Block the matching files that users attempt to download.
Any	Block the matching files that users attempt to upload or download.

9. For **Description**, type a description.

   The **Description** is displayed on the blacklist page and in reports.
10. Click a **Severity**.

    The blacklist **Severity** relates to the policy **Spyware Severity**. The action set for **Spyware Severity** in a matching policy applies to the blacklist entry. The **Severity** is also recorded and used in reports.

11 Click a **Category**.

The blacklist **Category** relates to the policy **Spyware Category**. The action set for **Spyware Category** in a matching policy applies to the blacklist entry. The **Category** is also recorded and used in reports.

12 Click **Save**.

Allow Web site access using the whitelist

You can allow access to Web sites or network locations using the whitelist. Whitelist entries are globally allowed. You do not have to configure a policy to activate whitelist entries. Access to a Web site or network on the whitelist is allowed despite any matching policies and the visit is not recorded for reports.

Warning: When you add an address to the whitelist, network traffic to and network traffic from that address is not scanned for malware. If the address is a Web site domain, any URL that starts with that domain is excluded from malware scanning.

You can also allow access to specific Web sites for a single policy using content filter exceptions. Because they act on single policies only, content filter exceptions provide a more targeted method of allowing access to Web sites.

See "Configuring URL filtering policies for Web sites" on page 66.

To allow Web site access using the whitelist

1 In the Web GUI, click **Policies > Whitelist**.

2 Click **Add a Whitelist Entry**.

You can also add whitelist entries from a text file. List one domain name or IP address per line in the file.

3 Type a domain name, IP address, or subnet specified in CIDR notation for the whitelist entry.

For a Web site, do not type a complete URL. Only type the domain name part of the URL.

4 Under **Actions**, check **Whitelist**.

5 Under **Actions**, check **Ignore Authentication** if you do not want Symantec Web Gateway to authenticate end users when they access the address.

This option is applicable if you have configured Active Directory integration with NTLM.

See "About Active Directory integration" on page 101.

6 Under **Comment**, optionally type a comment.

The comment is displayed on the whitelist page.

7 Click **Save**.

About the blocking feedback report

The blocking feedback report lists the blocked Web sites or files that users at your site think have been blocked in error. If you configure policies to block spyware or Web sites, Symantec Web Gateway displays a blocking page instead of the original content. By default, the blocking page includes a link for users to click if they think that the content should not have been blocked. You can disable the link if necessary.

See "About end user pages" on page 76.

See "About policies" on page 52.

The blocking feedback report is located at **Policies > Blocking Feedback**. On the blocking feedback report you can add a Web site or file to the whitelist or delete the request. You can also submit Web sites to Symantec's Web site categorization service for review.

See "Allow Web site access using the whitelist" on page 75.

About end user pages

Symantec Web Gateway displays a message in the Web browser of a user to indicate a blocked Web site, lengthy file download, blocked file upload or download, or a malware infection. The page that is displayed is called an end user page. For example, you can configure Symantec Web Gateway to display an end user page if a user attempts to access a gambling Web site. If a user attempts to view a gambling Web site, Symantec Web Gateway displays the end user page instead of the gambling Web site. You can change the text that Symantec Web Gateway displays for a blocked Web site, blocked file transfer, or a malware infection.

See "End user pages for blocked Web sites, file transfers, and infections" on page 77.

To block Web sites, you must have purchased the URL filtering license. To block file transfers, Symantec Web Gateway must be installed in the inline network configuration, not the port span/tap network configuration. For both Web site blocking and file transfer blocking, you must configure policies to allow or block access.

See "About policies" on page 52.

End user pages for blocked Web sites, file transfers, and infections

Table 4-5 describes the settings for the messages that Symantec Web Gateway displays to end users. You configure these settings on **Administration > End User Pages**.

See "About end user pages" on page 76.

For downloads longer than a few seconds, Symantec Web Gateway displays a patience page if blocking or monitoring applies to the Web page. The text of this patience page cannot be changed. However, you can change the language used on this page and the image that is displayed on the page. The **Language** and **New Image** settings described in Table 4-5 apply to the patience page.

See "Download behavior in user Web browsers" on page 55.

Text that is enclosed in percent signs represents variables. These variables are replaced with specific text when a user sees the message.

See "Variables for end user pages" on page 79.

Table 4-5 Blocked URL or File Message Configuration

Item	Default	Description
Message Group	**Default**	The blocked Web site message group to edit. By configuring multiple message groups, you can display different messages for different blocked Web site policies. See "Specifying computers or users for policies" on page 59.
Language	**English**	Display the default text in the selected language. In the Web page that is displayed to the user, supporting text, such as the text for user feedback, is displayed in the selected language.
Header Image	Symantec Web Gateway logo	The default image that is located at the top of the Web page that is displayed to the user.

Table 4-5 Blocked URL or File Message Configuration *(continued)*

Item	Default	Description
New Image	No default	Import a different image than the Symantec Web Gateway logo for the top of the Web page that is displayed to the user.
URL Block text	`This URL, %domain%, is a known %category% location and violates company policy.`	Text that is displayed when the user attempts to access a blocked Web site.
Download Block Text	`The file, %filename%, contains %category% and violates company policy.`	Text that is displayed when the user attempts to upload or download a blocked file.
Allow user feedback	Checked	Include text and a link in the Web page to allow users to request access to a blocked Web site or file. The following text is displayed in the Web page if the box is checked: `If you think this detection was in error, please click here.` When users click the link, a dialog box indicates that the IT department has been notified. To check for these user submissions, click **Policies > Blocking feedback**.

Table 4-6 Spyware Detected Page & Scheduled Cleaning Configuration

Item	Default	Description
Detected Page Header Text	`Spyware activity has been detected coming from your current IP address %IP%`	Text that is displayed in bold font at the top of the end user page when spyware has been detected on a computer.
Detected Page Body Text	`Your system may be infected by the following or other unidentified spyware:`	Text that is displayed in normal font when spyware has been detected on a computer. In the default text, the detected spyware is listed.
Scheduled Cleaning Header Text	`An Anti-Spyware scan has been scheduled for your current IP address %IP%`	Deprecated for Symantec Web Gateway customers. It applies only to legacy Mi5 Networks customers.
Scheduled Cleaning Body Text	No default	Deprecated for Symantec Web Gateway customers. It applies only to legacy Mi5 Networks customers.
Allow user cleanup	Checked	Deprecated for Symantec Web Gateway customers. It applies only to legacy Mi5 Networks customers.
Allow cleanup bypass	Checked	Deprecated for Symantec Web Gateway customers. It applies only to legacy Mi5 Networks customers.
Show Symantec Logo	Checked	Display the Symantec logo on the top of the Web page that is displayed to the user when spyware has been detected on a computer.

Variables for end user pages

Table 4-7 describes variables available for the messages in end user pages. These variables are replaced with specific text when a user sees the end user page. For example, if a user attempts to access a gambling Web site in violation of policy,

the %category% variable is replaced with the word gambling. The variables are not case sensitive, so %ip% and %IP% are equivalent.

See "End user pages for blocked Web sites, file transfers, and infections" on page 77.

To use variables in a URL that displays in the end user page, type the encoded version. For example, to display the threat name, category, and severity in a URL, type the URL as follows:

```
<a href=http://myserver/myscript?name=%threat-name-encoded%
&category=%category-encoded%&severity=%severity-encoded%">Click here</a>
```

Table 4-7 Variables for end user pages

Variable	Encoded version	Description	Blocked URL	Blocked file	Detected page	Scheduled cleaning page
%category%	%category-encoded%	The threat category, such as spyware.	Yes	Yes	No	No
%domain%	–	The domain name of the blocked URL, including subdomains. The prefix, such as http://, and any part of the URL after the domain name is omitted from %domain%.	Yes	No	No	No
%filename%	%filename-encoded%	The name of the file that was blocked.	No	Yes	No	No
%ip%	–	The IP address of the computer.	Yes	Yes	Yes	Yes
%policy%	%policy-encoded%	The name of the policy group that the IP address or user belongs to.	Yes	Yes	Yes	Yes
%severity%	–	The severity of the threat: minor, major, or critical.	Yes	Yes	No	No

Table 4-7 Variables for end user pages *(continued)*

Variable	Encoded version	Description	Blocked URL	Blocked file	Detected page	Scheduled cleaning page
%threat-description%	–	A sentence or short paragraph describing the threat.	Yes	Yes	No	No
%threat-id%	–	The unique identification number of the threat.	Yes	Yes	No	No
%threat-name%	%threat-name-encoded%	The name of the threat.	Yes	Yes	No	No
%url%		The URL that was blocked.	Yes	No	No	No

Chapter 5

Administering Symantec Web Gateway

This chapter includes the following topics:

About system users

You create the primary system user logon name and password when you run the setup wizard. You can create additional accounts for users to access Symantec Web Gateway. You can distribute the primary account name and password to all users who need to access the Web GUI at your site. However, by assigning a system user account to everyone with access to the Web GUI, you can track who has made which changes to Symantec Web Gateway. You can also set permissions and roles for system users to control access to Web GUI pages and reports.

See “Creating system users” on page 86.

See “Creating roles for system users” on page 85.

See "Monitoring system user activity" on page 87.

Permissions for system users

When you create or edit a system user, you choose the type of permission to grant the system user. Permissions control access to certain areas of the Web GUI. You can control access specifically to reports by creating and assigning roles.

See "About roles for system users" on page 84.

Table 5-1 Permissions for system users

Permission type	Blocked Web GUI areas	Read-only Web GUI areas	Editable Web GUI areas
Read Only	■ **Administration > System Users** ■ **Administration > Configuration**	■ **Administration > System Status** ■ **Administration > Updates** ■ **Administration > End User Pages**	■ **Reports**
Read & Write	■ **Administration > System Users** ■ **Administration > Configuration**	■ **Administration > System Status** ■ **Administration > Updates** ■ **Administration > End User Pages**	■ **Reports** ■ **Policies**
Administration	All areas are accessible.	No areas are read only.	All areas can be edited.

About roles for system users

You can create and assign roles to system users to permit access to certain types of report data. For example, you can create a role that only allows a system user to access report data for accounting computers. If you have configured Active Directory integration, you can configure access to report data by Active Directory departments or organizational units.

See "About Active Directory integration" on page 101.

Only the report data that matches the role restrictions is displayed to system users. System users can display all the Web GUI reports, but the data in each report is limited to the configured role restrictions. If a system user has a role, the Web GUI does not indicate that the report data is limited.

Table 5-2 Examples of role behavior

Example number	Role settings	Effect
Example 1	■ **Role Name**: **AD_department** ■ **Select Filter Data**: **Department** ■ **Select Filter Condition**: **Equals** ■ Filter-specific data: **Marketing**	If a system user with the role of **AD_department** views any report, only the report data for users in the **Marketing** department is displayed. You must configure Active Directory integration to employ any role restrictions that use Active Directory groups or user names. See "About Active Directory integration" on page 101.
Example 2	■ **Role Name**: **ip_range** ■ **Select Filter Data**: **Local IP address** ■ **Select Filter Condition**: **In Subnet** ■ Filter-specific data: **10.10.10.0/24**	If a system user with the role of **ip_range** views any report, only the report data for users in the **10.10.10.0/24** subnet is displayed.

Permissions are another way to control the type of Web GUI access allowed to system users.

See "Permissions for system users" on page 84.

Creating roles for system users

You can create and assign roles to system users to control system user access to report data. After you create a role, you can assign a role to a new system user or existing system user.

See "About roles for system users" on page 84.

You must be logged into the Web GUI as a system user with **Administration** permissions to configure a role.

You can create global or local roles on a Central Intelligence Unit. Global roles are available for system users on all managed appliances and system users that were created on the Central Intelligence Unit. Local roles are only available for system users on specific managed appliances.

To configure roles for system users

1 In the Web GUI, click **Administration > System Users**.

2 Next to **User Roles**, click **Define a New Role**.

3 For **Role Name**, type a name for the role.

The **Role Name** is displayed in the **Role** list when you create or edit a system user. The **Role Name** is also displayed in the **Role** column on the list of users on the **Administration > System Users** page.

4 You can optionally type a **Description** for the role.

The **Description** that you type for a role is displayed in the **Description** column on the list of roles on the **Administration > System Users** page.

5 Under **Role Restrictions**, set the following filter attributes for the role.

Select Filter Data	Click the type of report data to make available to system users assigned this role, such as the URL filtering category or protocol type.
Select Filter Condition	Click the filter condition such as equals, contains, etc.
Filter-specific data	For some filter data, an option may be displayed to select a specific type of data, such as the category for URL filtering.

6 If you want to add an additional filter to the role, click **Add Restriction**.

The conditions in all filters must be true for system users with that role to see report data of that type. For example, if you specify two filters for a role, only report data matching both filters is displayed for system users with that role.

7 Click **Save**.

You can assign a role to a new system user when you create that system user account.

See "Creating system users" on page 86.

Creating system users

You create the primary system user logon name and password when you run the setup wizard. You can create additional accounts for users to access Symantec Web Gateway. When you create a system user, you assign a permission to the system user. You can also assign a role to a system user to limit access to report data.

See "Permissions for system users" on page 84.

See "Creating roles for system users" on page 85.

You can configure password restrictions on the **Administration > Configuration > Security** page.

To create system users

1. In the Web GUI, click **Administration > System Users**.
2. Click **Create a User**.
3. Specify the following information for the new system user:

Name	The name that users type on the logon page to logon to the Web GUI.
Password	Password for the system user.
Reenter Password	Confirm the password that you typed.
Role	If you have created roles, you can assign a role to the new system user. Click **N/A** to not assign a role to a system user. See "About roles for system users" on page 84.
Description	The **Description** is displayed when you edit a system user.
Email Address	Default email address to send reports to. If this system user chooses to email a report, this email address is placed in the **Email Address(es)** box, but can be edited.
Permissions	Set access to parts of the Web GUI. See "Permissions for system users" on page 84.

4. Click **Save**.

Monitoring system user activity

You can view a list of all major changes to Symantec Web Gateway sorted by system user and time.

To monitor system user activity

1 In the Web GUI, click **Administration > System Status**.

The most recent changes to Symantec Web Gateway are listed at the bottom of the page.

2 To view the complete list of changes to Symantec Web Gateway, click **more** next to **Recent System Changes**.

About database and software updates

Table 5-3 describes the types of updates that Symantec provides for Symantec Web Gateway. For both types of updates, you can configure Symantec Web Gateway to check for and install updates automatically or you can check for and install updates manually.

Table 5-3 Database and software updates

Update type	Frequency of updates	Typical update size	Default setting	Appliance restart required?	Description
Database	About twice per week	About 15 megabytes	Automatically check for updates hourly	No	Definitions of known malware
Software	■ Minor releases (w.x.y.z): About once per month ■ Major releases (x.y and x.y.z): About two to four times per year	About 40 megabytes	Automatically check for updates daily; by default at 3:30 A.M.	Yes, for some updates	Fixes for software issues and new features

You can configure the update check frequency, enable notification of new software updates, and read software update release notes on the **Administration > Updates** page. If you enable automatic updates, Symantec Web Gateway checks for updates at the frequency you specify. If a new update is available, Symantec Web Gateway immediately downloads and installs the update.

Note: Symantec Web Gateway restarts without warning if you configure automatic software updates and the software update requires a restart. The restart occurs shortly after the configured automatic update time. The default automatic update time is 3:30 A.M. If you check for a software update manually and the update requires a restart, Symantec Web Gateway notifies you that a restart is required before installing the update. You can choose to install the software update immediately or at a later time.

You may need to disable automatic software updates to conform to administrative procedures at your site. In that case, Symantec recommends that you specify an email address to receive notifications about new software updates. Symantec recommends that you enable automatic database updates to ensure that your network is protected from the latest malware threats.

About alerts

You can configure Symantec Web Gateway to send the following types of alerts:

Malware alerts	Alerts for malware attacks and malware infections
System alerts	Alerts for software and hardware events and issues on the Symantec Web Gateway appliance

You can send alerts to one or more of the following destinations:

- One or more email addresses
- A remote syslog server
- SNMP Network Management System as SNMP trap

Symantec Web Gateway can send email alerts as CSV or HTML.

You must configure a remote syslog or SNMP Network Management System to send alerts to those systems. Consult the documentation for those systems for configuration information. You must also configure Symantec Web Gateway to send alerts to a remote syslog or SNMP Network Management System.

See "About sending alerts to syslog" on page 90.

See "About monitoring Symantec Web Gateway using SNMP" on page 90.

About sending alerts to syslog

Symantec Web Gateway can send malware alerts and system alerts to a remote syslog server. You cannot store syslog data on the Symantec Web Gateway appliance. Consult your syslog documentation for configuration information. Specify the syslog server and facility on the **Administration > Configuration > Syslog** page.

See "About alerts" on page 89.

About monitoring Symantec Web Gateway using SNMP

Simple Network Management Protocol (SNMP) is a standard protocol for network monitoring. You can use SNMP to monitor Symantec Web Gateway.

See "About alerts" on page 89.

Symantec Web Gateway supports SNMP version v2 and version v3. Symantec provides Symantec Web Gateway MIB files to import into your Network Management System. These MIB files define what monitoring information Symantec Web Gateway provides the Network Management System. The following Symantec Web Gateway information is available by SNMP:

- Appliance model number
- Appliance serial number
- Software version number
- Database version number
- CPU utilization
- Appliance temperature in Celsius
- Hard disk usage
- Operating status
- License status
- Operating mode
- Cumulative raw traffic processed expressed in bytes

Note: On your Network Management System, set the query timeout for polling to Symantec Web Gateway to five seconds or more.

Consult your SNMP documentation for configuration information. Specify the SNMP information on download MIB files on the **Administration > Configuration**

> SNMP page. You can configure Symantec Web Gateway to send malware alerts or system alerts as SNMP traps. Symantec Web Gateway sends alerts as SNMP traps in real time. Alerts indicate changes and minor to serious issues on Symantec Web Gateway.

Symantec Web Gateway does not support management by SNMP. You cannot use a Network Management System to make changes to a Symantec Web Gateway appliance. Instead, you can use a Central Intelligence Unit to make changes to one or more Symantec Web Gateway appliances.

See "About centralized management using a Central Intelligence Unit" on page 119.

About reports

You can display reports on a wide range of statistics such as the following information:

- Most accessed Web sites
- Most active users
- Spyware-infected computers
- Most common malware
- Network attacks
- Infection sources

You can click linked statistics on the reports to get more information about that user, computer, Web site, category, etc.

If you have configured Active Directory integration, Symantec Web Gateway displays some report statistics by Active Directory user name. If you have not configured Active Directory integration, Symantec Web Gateway displays those report statistics by host name instead.

See "About Active Directory integration" on page 101.

Table 5-4 Overview of reports

Report	Description
Executive Summary	Lists the summary spyware incident statistics for your network. The report includes traffic processed, spyware trends, sources of spyware infections, and infected computers.

Table 5-4 Overview of reports *(continued)*

Report	Description
Enterprise Summary	Summarizes the activity that Symantec Web Gateway detected organized by host name.
Browse Time	Lists the time that users spent Web browsing. Located on the **Enterprise Summary** report. You must enable browse time recording to activate this report. See "Enabling URL filtering, Internet program monitoring, and other features" on page 42.
Custom Reports	Create your own reports based on time period and various event statistics. Allows full queries of report log data.
Infected Clients	Lists all malware-infected computers that Symantec Web Gateway detected.
Infections by Spyware Name	Lists all malware infections that Symantec Web Gateway detected in your site. The report includes the number of infected computers, and number of times these infections have attempted to contact master Web sites. The report also shows how many infections have occurred for each malware name, and the category and severity of each infection.
Potential Attacks	The following potential attack reports are available: **Spyware**, **IP Scanning**, and **Spamming**. The **Spyware** report lists the attempts by remote systems to access an infected computer or send a malicious network element such as a worm. The **IP Scanning** report lists the IP addresses that attempted to scan IP address at your site. The **Spamming** report lists the IP address that attempted to send spam within your site.

Table 5-4 Overview of reports *(continued)*

Report	Description
Infection Sources	Lists all of the monitored or blocked URLs, spyware Web sites, and spyware file downloads attempted by users at your site. Also lists the number of computers and the number of times these accesses were attempted.
Client Applications	Lists the usage details of various applications and protocols at your site. This report also lists the number of computers and number of times network transmissions of those applications were detected.
Web Destinations	Lists all attempts to contact monitored or blocked Web sites by users at your site. This report also lists the number of computers and the number of times access to these destinations was attempted.
Botnets	Lists the detected activity that may indicate a botnet.
File Uploads	Lists the files that have been uploaded from your site. The report lists the uploaded files by type.
Saved Reports	Lists the reports that you saved.

Exporting a report to a .csv file

You can export a report to a comma-separated values (.csv) file. You can import the .csv file into a database program or spreadsheet program like Microsoft Excel that can import .csv files.

If you export the **Executive Summary** report, the .csv file contains report data for the five reports that are displayed in the **Executive Summary** report. All other reports contain the one type of report data specific to that report.

To export a report to a CSV file

1. In the Web GUI, click the report that you want to export.
2. In the upper right part of the page, click **Report Options** and then click one of the following:

Export Page...	Exports only the data that is visible on the current Web GUI page.
Export All...	Exports all the data available for the report.

3. In the dialog box that the Web browser displays, save the file.

Scheduling automatic reports

Symantec Web Gateway can deliver reports at set intervals to email addresses, a remote computer by file transfer, or both. Symantec Web Gateway emails reports as .csv or .html files. When you configure an automatic report, the report is saved in the **Reports > Saved Reports** page.

To schedule automatic reports

1. In the Web GUI, click the report that you want to run automatically.
2. In the upper right part of the page, click **Report Options** and then click **Save and Schedule...**.
3. Type a **Report Name** and **Report Description**.

   The **Report Name** is displayed in the **Reports > Saved Reports** page and in the report that is emailed or saved to the remote computer. **Report Name** and **Report Description** are displayed if you edit a saved report.
4. Next to **Selected Data** click one of the following:

Include the first *number* entries.	Delivers the number of entries that you specify from the report.
Include all entries.	Delivers all the data available for the report.

5. Next to **Report Frequency**, click one of the following:

Save Only	Do not schedule the report for delivery. Instead, save the report to the **Reports > Saved Reports** page for later use.

Once	Schedule the report to be delivered once at the date and time that you specify. The report is still saved to the **Reports > Saved Reports** page for later use
■ **15 minutes** ■ **30 minutes** ■ **Hourly** ■ **Daily** ■ **Weekly** ■ **Monthly**	Schedule the report to be delivered at the interval that you specify. The 15 minute, 30 minute, and hourly reports are delivered starting on the hour. For example, Symantec Web Gateway delivers the 30 minute report at :00 and :30 of the hour. Symantec Web Gateway prompts you for when to deliver the daily, weekly, and monthly reports.

6 Next to **Type of Delivery**, check one or both of the following check boxes:

Email	Delivers the report to one or more email addresses in HTML or CSV format. The recipients receive a static version of the report in an email message that includes a link to the live report. To see the live report, the recipient must have network access and logon privileges to the Symantec Web Gateway.
File Transfer	Delivers the report by **FTP**, **SFTP**, or **FTPS**. Specify a file path on the remote computer, computer address, and account information. Symantec Web Gateway adds a timestamp suffix to the file path. Do not specify the computer address starting with a URI like `ftp://`.

7 Click **Save**.

About the browse time report

Symantec Web Gateway can record the approximate amount of time that each computer or user spends using a Web browser to view Web sites. You must configure Active Directory integration to display the browse time by user. Otherwise the browse time is listed by computer.

See "About Active Directory integration" on page 101.

To enable and configure the browse time report	**Administration > Configuration > Modules** See "Enabling URL filtering, Internet program monitoring, and other features" on page 42.
To view the browse time report	**Reports > Enterprise Summary > Browse Time**

You can configure the threshold and sensitivity to determine how Symantec Web Gateway records browse time.

Table 5-5 Browse time threshold and sensitivity

Example	Browsing behavior	Result
Example 1 with threshold at 5 minutes and sensitivity at 3 minutes	■ At 9:00 A.M., the user accesses www.symantec.com. ■ At 9:07 A.M., the user clicks a link in www.symantec.com. ■ The user does not use the Web browser for 30 minutes.	Total browse time recorded is 0 minutes. The 3 minute sensitivity applied starting at 9:00 and 9:07 is still less than the 5 minute threshold. Since those browse times are not continuous, 0 minutes is recorded.
Example 2 with threshold at 5 minutes and sensitivity at 3 minutes	■ At 9:00 A.M., the user accesses www.symantec.com. ■ At 9:02 A.M., the user clicks a link in www.symantec.com. ■ At 9:04 A.M., the user clicks a link in www.symantec.com. ■ At 9:06 A.M., the user clicks a link in www.symantec.com. ■ The user does not use the Web browser for 30 minutes.	Total browse time recorded is 6 minutes. Between 9:00 and 9:06 is counted as 6 minutes.

About backing up and restoring the Symantec Web Gateway configuration

You can back up the Symantec Web Gateway configuration to a file on your local computer. If something happens to your Symantec Web Gateway appliance, you can restore the configuration to an appliance. You should include backing up Symantec Web Gateway as part of your network backup scheme.

See "Backing up Symantec Web Gateway" on page 97.

See "Restoring Symantec Web Gateway" on page 98.

Note: You must restore from a backup file saved from the same Symantec Web Gateway. You cannot restore a backup file from a different Symantec Web Gateway. You cannot use a Central Intelligence Unit to run a backup or restore. You must run a backup or restore from each managed appliance.

The following configuration information is saved when you back up Symantec Web Gateway:

- Symantec Web Gateway administrative users
- Saved reports
- Blacklist and whitelist policies
- Alert settings
- Network settings
- Active Directory integration settings
- End user pages
- SNMP settings

The following is not saved when you back up Symantec Web Gateway:

- Report data

Symantec Web Gateway saves the backup file with the current date and time in the following format:

`backup_`*`date_month_year_hour_minute_second`*`.sql`

For example, Symantec Web Gateway saves a backup on October 17 , 2009 at 11:10:15 P.M. as:

`backup_17_10_09_11_10_15.sql`

The hour in the backup name is in 12-hour format. The morning hours and evening hours are not represented differently. You can rename the backup file. Renaming the backup file does not affect the restore process.

Backing up Symantec Web Gateway

You should back up Symantec Web Gateway periodically in case of a critical problem with the Symantec Web Gateway software or appliance. When you run a backup, your Web browser prompts you for the location to save the backup file. You can store the backup file on the computer on which your Web browser is running. Alternatively, you can store the backup file to a network location that is accessible from the computer on which your Web browser is running. You cannot store the backup file on Symantec Web Gateway.

See "About backing up and restoring the Symantec Web Gateway configuration" on page 96.

To back up Symantec Web Gateway

1. In the Web GUI, click **Administration > Configuration > Maintenance**.
2. Next to **Backup Current Settings to File**, click **Backup**.
3. In the Web browser save file dialog box, save the file to an appropriate location.

   In general, every time you back up Symantec Web Gateway, save the backup files in the same location.

Restoring Symantec Web Gateway

If you have made backups of Symantec Web Gateway, you can restore an appliance in case of a critical problem with the Symantec Web Gateway software or appliance. You must restore from a backup file saved from the same Symantec Web Gateway. You cannot restore a backup file from a different Symantec Web Gateway.

See "About backing up and restoring the Symantec Web Gateway configuration" on page 96.

Restoring Symantec Web Gateway

1. In the Web GUI, click **Administration > Configuration > Maintenance**.

   If you cannot access the Web GUI, reset access to the setup wizard using the Serial Console and run the setup wizard again.

   See "Running the setup wizard again" on page 48.

   See "Running the setup wizard for initial installation" on page 35.
2. Next to **Restore Settings From File**, click **Restore**.
3. In the Web browser open file dialog box, navigate to the backup file and open the file.

   Check the settings in the Web GUI to ensure that they are appropriate. In particular, check the settings on the **Administration > Configuration > Network** page.

Resetting Symantec Web Gateway to factory settings

Occasionally you may need to reset Symantec Web Gateway to the factory settings. For example, if you have an appliance configured as a Symantec Web Gateway, to use that appliance as a Central Intelligence Unit, you must reset the appliance.

After you reset an appliance to the factory defaults, you run the setup wizard again.

If you created a backup for an appliance, you can restore the backup to the same appliance after you reset it. Restore the appliance after running the setup wizard.

See "About backing up and restoring the Symantec Web Gateway configuration" on page 96.

Warning: This procedure erases all data from Symantec Web Gateway.

To reset Symantec Web Gateway to factory settings

1. In the Web GUI, click **Administration > Configuration > Maintenance**.
2. Next to **Restore Default Settings**, click **Restore**.

   The appliance restarts. All existing settings are erased. Use the setup wizard to configure the appliance.

   See "Running the setup wizard for initial installation" on page 35.

   See "Running the setup wizard for initial installation of a Central Intelligence Unit" on page 122.

Resetting the Web GUI password for the primary system user

If you lost the password for the primary system user, Symantec Web Gateway can email a password to the address that you specified in the setup wizard. If you forgot the primary system user logon name or do not have access to the email address, you must run the setup wizard again.

See "Running the setup wizard again" on page 48.

To reset the Web GUI password

1. Access the Web GUI logon page.
2. Click **Forgot Password?**

   The Web GUI password is emailed to the address for the primary system user that you specified in the setup wizard.

Serial Console access to Symantec Web Gateway

You can access Symantec Web Gateway through the Serial Console. The Serial Console can be useful if you cannot access Symantec Web Gateway through the

Web GUI. The Serial Console has a character-based interface. Many of the Web GUI settings are available in the Serial Console.

Table 5-6 Requirements for Serial Console access to Symantec Web Gateway

Item	Description
Computer with serial port and monitor	You can use any modern computer and operating system (such as Linux, Mac OS X, and Windows) for this purpose. The computer must have a serial port.
Serial cable (included)	A serial cable is included with Symantec Web Gateway. Connect one end to your computer. Connect the other end to the serial port on the back of the Symantec Web Gateway appliance. To locate the serial port, refer to the diagram for your appliance. See "Connections and indicators on Symantec Web Gateway" on page 20.
Terminal emulation software	You interact with the Symantec Web Gateway console in terminal emulation software on your computer. On Windows XP, you can use the included HyperTerminal program. HyperTerminal is located at **Start > All Programs > Accessories > Communications > HyperTerminal**. Set the terminal emulation software to the following parameters: ■ 9600 bits per second ■ 8 data bits ■ 1 stop bit ■ No parity ■ No flow control On Windows, ensure that the terminal emulation software is set to use the correct COM port.
Console login name and password	By default, the login name and password for console access is as follows: ■ Login name: `admin` ■ Password: `admin1!`

If the cable is connected and the terminal emulation software is configured properly, Symantec Web Gateway displays a login prompt in the terminal emulation software. You can leave the computer attached to the serial port while you run the setup wizard and the Web GUI.

Chapter 6

Configuring Active Directory integration

This chapter includes the following topics:

About Active Directory integration

You can configure Symantec Web Gateway to integrate with Active Directory. Active Directory is a Microsoft product that stores user account information and provides authentication on Windows networks. Integration with Active Directory provides the following benefits:

Users are displayed in reports	User names are displayed in reports.
User-based policies	You can create policies based on Active Directory user names and group categories.

See "Steps to configure Active Directory integration with a domain controller" on page 103.

See "Steps to configure Active Directory integration with NTLM" on page 110.

Note: Active Directory integration only works with Active Directory running on Windows Server 2003. Symantec Web Gateway does not support any other type of LDAP directory service. Symantec Web Gateway does not support global catalogs if you configure domain controller integration. Symantec Web Gateway does not integrate with Active Directory running on a virtual machine such as VMware or Citrix.

You can configure Active Directory integration using a domain controller interface, using NTLM, or both. Table 6-1 compares the two methods of Active Directory integration.

Table 6-1 Comparing Active Directory integration with a domain controller and NTLM

Consideration	Domain controller	NTLM
User identification method	The domain controller sends user name to Symantec Web Gateway	Symantec Web Gateway queries user Web browser for authentication.
User attribute queries	The appliance queries Active Directory using the OpenLDAP protocol.	The appliance queries Active Directory using the OpenLDAP protocol.
Scalability	Best for environments with less than 1000 users in Active Directory.	Supports any number of users in Active Directory, assuming that the environment is scaled appropriately.
Affect on network load and Symantec Web Gateway load	Potentially significant load due to real-time authentication.	Minimal if the 15-minute default polling interval is retained.
Configuration changes required outside of Symantec Web Gateway	You must install Symantec domain controller interface on each domain controller that users log on to.	No additional software installation is required but a change to your DNS configuration may be necessary.
Change required to user computers	None.	Changes to the user Web browser may be necessary.

Table 6-1 Comparing Active Directory integration with a domain controller and NTLM *(continued)*

Consideration	Domain controller	NTLM
User experience	Transparent to users. No special logon for Symantec Web Gateway is required.	Usually transparent to users running Internet Explorer on Microsoft Windows. In some cases Outlook or the Web browser displays a dialog box that requires users to log on . See "Ensuring compatibility with NTLM" on page 115.
Speed of recognition for reporting purposes	Users are identified immediately upon logon.	User identification occurs by polling. A delay occurs between the time that users logon and the time that Symantec Web Gateway registers the logon. The default polling frequency is 15 minutes but you can configure the frequency.

You can use a Central Intelligence Unit to configure Active Directory integration on managed appliances. With a Central Intelligence Unit, the communication with Active Directory occurs with the managed appliances, not with the Central Intelligence Unit.

Steps to configure Active Directory integration with a domain controller

Table 6-2 describes the steps to configure Active Directory integration with a domain controller.

Table 6-2 Steps to configure Active Directory integration using a domain controller

Step	Action	Description
Step 1	Create an Active Directory account	Create a read-only Active Directory account for Symantec Web Gateway. Configure the account to have access to the full Active Directory catalog.

Table 6-2 Steps to configure Active Directory integration using a domain controller *(continued)*

Step	Action	Description
Step 2	Specify your Active Directory settings	Specify your Active Directory settings in the Symantec Web Gateway Web GUI. See "Configuring Active Directory integration" on page 104.
Step 3	Install the Symantec domain controller interface	Download the Symantec domain controller interface from the Web GUI and install it. See "Installing the Symantec domain controller interface" on page 107.
Step 4	Configure the Symantec domain controller interface	Edit a text file to configure the Symantec domain controller interface. See "Configuring the Symantec domain controller interface" on page 108.
Step 5	Remote domain controller access only: specify the Active Directory user account	If you did not install the Symantec domain controller interface directly on the domain controller, you must specify the Active Directory user account in Services. See "Configuring the Symantec domain controller interface for remote Active Directory access" on page 108.
Step 6	Start the Symantec domain controller interface	Start the Symantec domain controller interface in Services. See "Starting the Symantec domain controller interface" on page 109.
Step 7	Test the Active Directory integration	If the Active Directory integration works correctly, user names display in the Web GUI reports.

Configuring Active Directory integration

You specify your Active Directory configuration in the Web GUI for both domain controller authentication and NTLM authentication. Ensure that you created an Active Directory account for use by Symantec Web Gateway before you configure

domain controller authentication in the Web GUI. Configure the account to have access to the full Active Directory catalog.

To configure Active Directory integration

1. In the Web GUI, click **Administration > Configuration > Authentication**.
2. Under **LDAP Configuration**, specify the following information about your Active Directory environment:

LDAP Server IP or Hostname	Type the IP address or host name of the Active Directory server.
LDAP Port	Type the communication port number for the Active Directory server. Port 389 is the default port by Microsoft convention.
Authentication Method	Click one of the following options: ■ **Simple** The user name (bind DN) and password are transmitted in plaintext. ■ **Kerberos** The user name (bind DN) and password are encrypted using the encrypted Kerberos protocol.
LDAP Search Base (Base DN)	Type the base DN for authentication queries to your Active Directory. A typical base DN for a simple Active Directory configuration is `dc=domain,dc=com` where *domain* is the domain name of your company. You may need to add additional parameters to the base DN, such as the organizational unit (`ou=department`).
User Name	Type the user name (bind DN) that you created for use by Symantec Web Gateway. Type the user name using one of the following forms: ■ sAMAccountName, for example: `john_smith` Valid for simple and Kerberos authentication. ■ sAMAccountName@domain, for example: `john_smith@symantecdomain.com` Valid for simple and Kerberos authentication ■ Distinguished name (DN), for example: `cn=john smith,dc=symantecdomain,dc=com` or `CN=John Smith,OU=accounting,OU=finance,DC=symantecdomain,DC=com` Valid for simple but not Kerberos authentication
Password	Type the password for the user account.

Group Users by	Click one of the following grouping options: ■ **Department** ■ **Organizational unit**
UID Attribute	Click one of the following UID attributes: ■ **sAMAccountName** ■ **uid** This attribute form is no longer supported. ■ **Other** If you select **Other**, specify the UID.
Age out	The number of hours after which Symantec Web Gateway assumes that a user has logged out from a computer if no logon information is received. Active Directory does not indicate to Symantec Web Gateway when a user logs out from a computer. Symantec Web Gateway uses the **Age out** time to determine how long to associate a user name with a computer for reporting purposes. If another user logs into the computer, Symantec Web Gateway assumes that the original user has logged out. The default is 168 hours (one week).

3 If you selected Kerberos as the authentication method, click **Configure Kerberos settings automatically** or manually configure the Kerberos settings. If you click **Configure Kerberos settings automatically**, Symantec Web Gateway uses the following settings for Kerberos authentication:

LDAP Server IP or Hostname	The data in this field is used for the Kerberos key distribution center (KDC) and Admin Server.
LDAP Search Base (Base DN)	The data in this field is used for the Kerberos realm and domain.

If those substitutions do not match your Kerberos environment, manually configure Kerberos settings by specifying the following information:

- **Kerberos Realm**
- **Default Domain**
- **Key distribution center (KDC)**
- **KDC Port**
- **Kerberos Admin Server**

- **Admin Server Port**

4 Click **Test** next to **Test LDAP**.

The results of the test are displayed at the top of the page. If there is an error, correct the settings and test again.

5 Click **Save**.

Installing the Symantec domain controller interface

For Active Directory integration with a domain controller to work, you must install Symantec domain controller interface. Install the Symantec domain controller interface on one of the following:

- All domain controllers that users may log on to
- A dedicated Windows computer with access permission to the domain controller log
  You can only install the Symantec domain controller interface once per computer. If you have multiple domain controller logs that you want to access remotely, you must have one dedicated Windows computer per domain controller log.

Note: The domain controller must be running on Windows Server 2003. Symantec Web Gateway does not support global catalogs.

If you plan to upgrade an existing Symantec domain controller interface, refer to the `README.txt` in the zip file for the recommended procedure. The following procedure is for new installations only.

To install the Symantec domain controller interface

1 In the Web GUI, click **Administration > Configuration > Authentication**.

If possible, access the Web GUI from the computer on which you plan to install the Symantec domain controller interface.

2 Click **Download domain controller interface software**.

3 Move the zip file to a permanent location on the computer on which you plan to install the Symantec domain controller interface and unzip it.

For example, you can put the zip file in C:\.

4 On the computer where you unzipped the zip file, open a command prompt window.

5 In the command prompt window, navigate to the folder where you unzipped the zip file using the `cd` command.

6 At the command prompt, type the following:

```
DCinterface.exe -install
```

The message `Service Does not exist` is displayed. You can ignore this message. Do not move the `DCinterface.exe` file after you run this command.

7 Close the command prompt window.

Next, configure the Symantec domain controller interface.

See "Configuring the Symantec domain controller interface" on page 108.

Configuring the Symantec domain controller interface

After installing the Symantec domain controller interface, you must configure it.

See "Installing the Symantec domain controller interface" on page 107.

To configure the Symantec domain controller interface

1 Use Notepad to open the `dcinterface.txt` file that was included in the zip file.

2 In the `dcinterface.txt` file, add a line at the bottom for each Symantec Web Gateway appliance in the following format:

```
host appliance-name
```

Type the fully qualified domain name or IP address for the *appliance-name*.

3 If the Symantec domain controller interface is not installed on the Domain controller, add the following line at the bottom of the `dcinterface.txt` file:

```
remoteserver domaincontroller-name
```

Type the fully qualified domain name or IP address for the *domaincontroller-name*.

4 Save and exit from the `dcinterface.txt` file.

Next, start the service.

See "Starting the Symantec domain controller interface" on page 109.

Configuring the Symantec domain controller interface for remote Active Directory access

Follow this procedure if you installed the Symantec domain controller interface on a computer with access permission to the domain controller log. Do not follow this procedure if you installed the Symantec domain controller interface directly on a domain controller.

The Active Directory user that you specify in this procedure should have domain administrator rights to access the Active Directory log. If that does not work in your Active Directory environment, the Active Directory user may need full administrator rights.

To configure the Symantec domain controller interface for remote Active Directory access

1. On the Windows computer that you installed the Symantec domain controller interface on, click **Start > Administrative Tools > Services**.
2. Double-click **Symantec Domain Controller Interface**.
3. On the **Log on** tab, click **This account**.
4. To specify the user name next to **This account**, do one of the following:

To specify a user name in the form *DOMAIN\username*	Type the user name
To specify a user name in the form *username@domain*	Click **Browse** and type the user name
To browse for a user name	Click **Browse** and browse the network for a user name

   Symantec Web Gateway uses the user name to access the Active Directory catalog.
5. Type the password for the user name.
6. Click **OK**.

   Next, start the service.

Starting the Symantec domain controller interface

After installing and configuring the Symantec domain controller interface, start it in Services. If you installed the Symantec domain controller interface on a computer with access permission to the domain controller log, configure that computer first.

See "Configuring the Symantec domain controller interface for remote Active Directory access" on page 108.

To start the Symantec domain controller interface

1. On the Windows computer that you installed the Symantec domain controller interface on, click **Start > Administrative Tools > Services**.
2. Click **Symantec Domain Controller Interface**.

3 Click **Start the service**.

4 Close Services.

5 To test that it is running, open the Windows Task Manager and look for **Symantec Domain Controller Interface**.

The Symantec domain controller interface writes log information to the `errorlog.txt` file in the folder where `dcinterface.txt` resides.

Moving the `DCinterface.exe` file

After you install the `DCinterface.exe` file, you should leave it in the same folder. If you need to move the `DCinterface.exe` file or the folder that it is in, follow these steps. If you move the `DCinterface.exe` file without following these steps, Active Directory integration can fail to work properly.

To move the `DCinterface.exe` file

1 Click **Start > Administrative Tools > Services**.

2 Click **Symantec Domain Controller Interface**.

3 Click **Stop the service**.

4 Close Services.

5 Open a command prompt window.

6 Type the following:

```
DCinterface.exe -remove
```

7 Move the folder containing `DCinterface.exe` to the new location.

8 In the new location, type the following in a command prompt:

```
DCinterface.exe -install
```

9 Open Services again and start **Symantec Domain Controller Interface**.

Steps to configure Active Directory integration with NTLM

Table 6-3 describes the steps to configure Active Directory integration with NTLM. When you configure Active Directory integration with NTLM, Symantec Web Gateway communicates with user browsers to perform the following:

- To extract an Active Directory name
- To correlate the user's Active Directory name with the user's IP address

- To reenforce user authentication to the domain controllers when the user's credentials expire

Table 6-3 Steps to configure Active Directory integration with NTLM

Step	Action	Description
Step 1	Specify **Management Interface Name** in the Web GUI	To avoid making changes to user Web browsers, specify the **Management Interface Name** in the Web GUI. See "Specifying the Management Interface Name in Symantec Web Gateway" on page 112.
Step 2	Add A record to DNS for each Symantec Web Gateway	To avoid making changes to user Web browsers, add an A record in DNS for each appliance on which you specified the **Management Interface Name**. See "DNS change needed for NTLM" on page 112.
Step 3	Specify your NTLM settings	Specify your Active Directory and NTLM settings in the Web GUI. See "Configuring Active Directory integration" on page 104. See "Configuring Active Directory integration with NTLM" on page 113.
Step 4	If necessary, make Web browser changes	You may need to make changes to user Web browsers depending on how you configured NTLM and the user Web browser and operating system. See "Web browser changes needed for NTLM" on page 114.
Step 5	If necessary, make Outlook, Windows Vista, or other operating system changes	You may need to make changes to Outlook, Windows Vista, or other operating systems to ensure compatibility with NTLM. See "Ensuring compatibility with NTLM" on page 115.
Step 6	Test the Active Directory integration	If the Active Directory integration works correctly, user names display in the Web GUI reports.

Specifying the Management Interface Name in Symantec Web Gateway

To avoid making changes to user Web browsers when using NTLM authentication, specify the **Management Interface Name** in the Web GUI. You also need to add an A record to DNS for this method to work properly.

See "DNS change needed for NTLM" on page 112.

If you manage appliances using a Central Intelligence Unit, you can perform this task for each appliance in the Central Intelligence Unit. However, you must specify the **Management Interface Name** for each appliance individually.

To specify the Management Interface Name in Symantec Web Gateway

1. In the Web GUI, click **Administration > Configuration > Network**.
2. Type the **Management Interface Name**.

   The name must be 16 characters or less and must not contain the domain or top-level domain. In other words, the name should be of the form `mymibname` and not `mymibname.symantecs.org`.
3. Click **Save**.

DNS change needed for NTLM

You must add an A record in your DNS server for each appliance on which you specified the **Management Interface Name**. Consult the documentation for your DNS server software to determine how to add A records. Table 6-4 describes the information to specify in your DNS server software. The examples for DNS record type and DNS record class are shown for the BIND DNS server software.

Table 6-4 DNS A record for the Management Interface Name

DNS A record component	Description	Example
Name	The **Management Interface Name** typed as a short form host name without any periods	`mymibname`
DNS record type	Internet	`IN`
DNS record class	A record	`A`
IP address	IP address of the appliance on which you specified the **Management Interface Name**	`192.168.2.100`

Configuring Active Directory integration with NTLM

Follow these steps to configure Active Directory integration with NTLM. You may need to change the Web browsers on users' computers.

See "Steps to configure Active Directory integration with NTLM" on page 110.

See "Web browser changes needed for NTLM" on page 114.

To configure Active Directory integration with NTLM

1. In the Web GUI, click **Administration > Configuration > Authentication**.
2. Under **NTLM Configuration**, specify the following information about your Active Directory environment:

Default Realm	Type the domain name of your realm, such as **symantecexample.com**. IP addresses are not valid. A partial domain name is valid if **DNS Suffix** is specified on the **Administration > Configuration > Network** page.
Primary/Secondary Domain Controller	Type the fully qualified domain name of your primary domain controller and secondary domain controller, such as **controller.symantecexample.com**. IP addresses are not valid. A partial domain name is valid if **DNS Suffix** is specified on the **Administration > Configuration > Network** page.
Use Interface Name for NTLM Authentication	■ Check the box if you configured a **Management Interface Name** and added an A record for it to DNS. See "Specifying the Management Interface Name in Symantec Web Gateway" on page 112. ■ Uncheck the box if you do not want to modify DNS. You must modify end-user browsers. See "Web browser changes needed for NTLM" on page 114. The default is unchecked but checked (with proper configuration) is recommended.
Authentication TTL	Type the time between authentication requests from Symantec Web Gateway. The default is 15 minutes. A shorter time results in increased load on Symantec Web Gateway.

User Authentication Re-tries	Type the number of times that the Web browser allows the user to try to supply the user name and password after failed attempts. If the user fails to correctly log on after this number of attempts, only IP-based policies or default policies apply. After the authentication failure, reports display activity based on IP address only and not user names. If you have configured an **Enforce Authentication** policy for a user and the user fails authentication, Symantec Web Gateway denies Web access. See "Configuring NTLM user authentication behavior" on page 71.

3 Click **Test** next to **Test NTLM**.

The results of the test are displayed at the top of the page. If there is an error, correct the settings and test again.

4 Click **Save**.

Web browser changes needed for NTLM

When you employ Active Directory integration with NTLM, Symantec Web Gateway queries user Web browsers for authentication. In many cases, no special configuration is needed. Table 6-5 describes cases in which you must configure user Web browsers.

Manually making changes to the Web browsers on each user's computer may be a lengthy task. You may be able to distribute changes to Internet Explorer on all user computers using Active Directory tools. Altiris software from Symantec or similar software can also automate configuration changes for user Web browsers.

Table 6-5 Web browser changes needed for NTLM

Scenarios	Change needed in Web browsers

The following conditions apply:
■ Users access the Internet using a proxy that does not support 401 authentication pass through
■ The **Use Interface Name for NTLM Authentication** box is checked
	Web browsers must be configured to access the Web Gateway interface name directly and not through the proxy. For Internet Explorer, you can make this change centrally using `.pac` files. The following is a sample `.pac` file script:
	`function FindProxyForURL(url, host)`
	`{`
	`if (isPlainHostName(host))`
	`return "DIRECT";`
	`else`
	`return "PROXY 192.168.0.70:8080";`
	`}`

The **Use Interface Name for NTLM Authentication** box is unchecked	If you do not want to modify DNS, leave **Use Interface Name for NTLM Authentication** unchecked. Add the IP address of Symantec Web Gateway to the **Local Intranet** configuration in Internet Explorer. Use the following format: `http://num1.num2.num3.num4`, such as `http://192.168.2.1`. You should be able to use Active Directory to push this browser configuration to the end users' browsers.
Web browsers other than Microsoft Internet Explorer, such as Mozilla Firefox, Apple Safari, or Google Chrome	You may need to make a configuration change in the Web browser to support transparent NTLM authentication. For example, in Firefox add the IP address of each Symantec Web Gateway in your network to **network.automatic-ntlm-auth.trusted-uris** on the **about:config** page. See the Web browser documentation for more information.

Ensuring compatibility with NTLM

Some operating system require configuration changes to work with NTLM. If you do not make the necessary changes, you may encounter the following issues:

- Active Directory may deny user access due to failed authentication attempts. This can occur even if users were not presented with an authentication dialog box due to internal authentication failures.
- Outlook or the Web browser may display a dialog box that requires users to log on.

See "Web browser changes needed for NTLM" on page 114.

See "Configuring NTLM user authentication behavior" on page 71.

Table 6-6 Ensuring compatibility with NTLM

Environment	Description
Microsoft Windows Vista	Windows Vista requires a group policy change to use the NTLMv1 protocol instead of NTLMv2. Windows 7 may require a similar change. See "Configuring NTLM compatibility for Windows Vista" on page 116.
Operating systems that are not sold by Microsoft, such as Mac OS X or Linux	Refer to your operating system documentation for information about NTLM integration.
Windows XP SP2 and Outlook 2003	Users running Outlook 2003 on Windows XP SP2 may see an authentication dialog box . See "Configuring NTLM compatibility for Outlook 2003 and Windows XP SP2" on page 117.

Configuring NTLM compatibility for Windows Vista

Windows Vista requires a group policy change to use the NTLMv1 protocol instead of NTLMv2. Other versions of Windows can also have this issue if your organization's security policy does not support NTLMv1. If you do not make this change, it can affect authentication for users at your site.

See "Ensuring compatibility with NTLM" on page 115.

For more information, on the Internet go to the following URL and refer to section 10:

support.microsoft.com/kb/823659

You must perform this procedure on every computer that runs Windows Vista in your network. You can use the Active Directory group policy to make this change for all computers.

To configure NTLM compatibility for Windows Vista

1. Click **Start > All Programs > Accessories > Run** and type **secpol.msc** in the **Open** box, and then click **OK**.
2. Click **Local Policies > Security Options > Network Security: LAN Manager authentication level**.
3. Click **Send LM & NTLM - use NTLMv2 session security if negotiated**.
4. Click **Apply**.

Configuring NTLM compatibility for Outlook 2003 and Windows XP SP2

In Windows XP SP2, Outlook 2003 email windows other than the preview pane may not pass NTLM credentials transparently. If a user opens a message that contains embedded HTML and the user is not currently authenticated, an authentication dialog box is displayed. To prevent the dialog box, get Windows XP SP3 or a hotfix and modify the registry. These changes must be made to every user computer.

To modify Windows XP to support transparent NTLM authentication with Outlook 2003

- Do one of the following:
  - Request Hotfix 895948 from Microsoft.
  - Install Windows XP SP3, which contains Hotfix 895948.

To modify the registry to support transparent NTLM authentication with Outlook 2003

1. In Windows, click **Start > Run**, type regedit, and click OK.
2. Expand the following subkey:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl
3. Right-click **FeatureControl** and then click **New > Key**.
4. Type the following and press Enter:

   KB895948_DISABLE_MAIL_SUBDOWNLOAD_LOCKDOWN
5. Right-click **KB895948_DISABLE_MAIL_SUBDOWNLOAD_LOCKDOWN**, and then click **New > DWORD Value**.
6. Type **outlook.exe** and press Enter.
7. Right-click **outlook.exe**, and then click **Modify**.
8. In the **Value** data box, type **00000001**, and then click **OK**.
9. Exit from registry editor .

Chapter 7

Configuring a Central Intelligence Unit to manage multiple appliances

This chapter includes the following topics:

About centralized management using a Central Intelligence Unit

Any Symantec Web Gateway appliance can be configured to manage one or more other Symantec Web Gateway appliances. An appliance that is configured to manage other appliances is called a Central Intelligence Unit. On the Central Intelligence Unit, most Web GUI pages let you make changes or view reports for all managed appliances or individual managed appliances.

You can continue to log on to the Web GUI of managed appliances after you configure a Central Intelligence Unit. Managed appliances can be configured in inline network configuration or port span/tap network configuration. When you configure an appliance as a Central Intelligence Unit, that appliance cannot function as a Symantec Web Gateway.

See "Steps to install a Central Intelligence Unit" on page 120.

Table 7-1 Central Intelligence features

Feature	Description
Centralized management	Make the same change to multiple appliances at the same time or make unique changes to individual appliances from the Central Intelligence Unit
Centralized reporting	View consolidated reports from all managed appliances

Table 7-2 describes the frequency of data exchange between a Central Intelligence Unit and managed appliances.

Table 7-2 Data exchange between Central Intelligence Unit and managed appliances

Direction	Type of data	Port	Protocol	Frequency
Central Intelligence Unit to managed appliances	Configuration data	443	SSL	After you click **Save** on a Web GUI page on the Central Intelligence Unit
Managed appliances to Central Intelligence	Statistics for reports	443	SSL	Five minutes by default, depends on the **Upload Frequency** setting See "Configuring appliances to accept management by a Central Intelligence Unit" on page 125.

Steps to install a Central Intelligence Unit

Table 7-3 describes the steps to install a Central Intelligence Unit. These steps are listed in the suggested order.

See "About centralized management using a Central Intelligence Unit" on page 119.

Note: If you want to use an appliance that was previously configured as a Web Gateway, you must reset it to the factory settings.

See "Resetting Symantec Web Gateway to factory settings" on page 98.

Table 7-3 Steps to install a Central Intelligence Unit

Step	Action	Description
Step 1	Install and configure appliances to be managed by the Central Intelligence Unit	Install and configure the appliances to be managed by the Central Intelligence Unit. Ensure that each appliance functions independently before configuring it as a managed appliance. Alternatively, you can run the setup wizard on the managed appliances and immediately configure them to accept management by the Central Intelligence Unit. After that you can configure each appliance using the Central Intelligence Unit. See "Steps to install Symantec Web Gateway" on page 15.
Step 2	Install the Central Intelligence Unit into a rack	Install the Central Intelligence Unit into a rack, but wait to connect Ethernet cables. See "Installing the Symantec Web Gateway appliance into a rack" on page 34.
Step 3	Connect a computer for initial installation	Configure and connect a computer to the Central Intelligence Unit for initial installation. See "Configuring a computer to access Symantec Web Gateway for installation" on page 34.
Step 4	Run the setup wizard	Run the setup wizard for the Central Intelligence Unit. See "Running the setup wizard for initial installation of a Central Intelligence Unit" on page 122.
Step 5	Connect the Central Intelligence Unit to the network	Connect the Central Intelligence Unit to the network. See "Connecting a Central Intelligence Unit to the network" on page 124.
Step 6	Review the network ports used by Symantec Web Gateway	Open ports between Central Intelligence Unit and managed appliances. See "Ports used by Symantec Web Gateway" on page 29.
Step 7	Configure managed appliances	Configure managed appliances to accept management by the Central Intelligence Unit. See "Configuring appliances to accept management by a Central Intelligence Unit" on page 125.

Running the setup wizard for initial installation of a Central Intelligence Unit

After you physically install Symantec Web Gateway and connect a computer to the Mgmt port, you can run the setup wizard. This procedure describes how to configure an appliance as a Cental Intelligence Unit.

See "Steps to install a Central Intelligence Unit" on page 120.

Note: For the Central Intelligence Unit to communicate with managed appliances, the Central Intelligence Unit and managed appliances must be running the same software version. For example, if the Central Intelligence Unit is running 4.5.2, then all managed appliances must be running 4.5.2 also.

To run the setup wizard for initial installation of a Central Intelligence Unit

1. Press the power button on the front of the Symantec Web Gateway appliance.

   The appliance takes several minutes to start up.

2. On the computer that is connected to the Mgmt port, start a Web browser and go to the following URL:

   http://192.168.254.254

3. On the **Welcome** panel, click **Next >>**.

4. On the **License Agreement** panel, read the license agreement, check the box, and click **Accept**.

5. On the **Install License** panel, type your company name and navigate to the license file or paste the XML license and click **Next >>**.

   The company name does not need to match the company name that you provided to Symantec when you obtained your license. The company name that you provide here is supplied to Symantec if you enable remote assistance on Symantec Web Gateway. If you do not install a license now, there is a two week grace period. During the two week grace period Symantec Web Gateway functions as if a base license was installed.

6. On the **Select Server Type** panel, click **Central Intelligence Unit**.

   You can only change the server type in the setup wizard, not in the Web GUI after completing the setup wizard.

7 On the **User Information** panel, specify the following information about the primary Web GUI administrator:

Login Name	Type a login name for the primary Web GUI administrator. Use ASCII characters only. The login name is case sensitive.
Password	Type a password for the primary Web GUI administrator.
Description	Optionally, you can type a description for the current user account. This description is displayed on the **Edit User** page.
Email Address	Type an email address. Type a complete email address, such as `admin@symantecs.org`.Symantec Web Gateway sends alerts and reports to this email address. If you click the **Forgot Password?** link on the logon page, a new password is sent to this address.

8 Click **Next >>**.

9 On the **Server Information** panel, specify the following information:

Network Settings	Specify the following network settings for Symantec Web Gateway: ■ **Automatic (DHCP)** or **Manual** **Automatic (DHCP)** is not recommended. ■ **IP address** ■ **Subnet Mask** ■ **Default Gateway** ■ **Primary DNS** ■ **Secondary DNS (Optional)** ■ **DNS Suffix (Optional)** You can specify a DNS suffix so that you can type the short form of other host names in the Central Intelligence Unit Web GUI.

Central Management Settings	Specify the following network settings for Symantec Web Gateway: ■ **Local Management Address** The network address that managed appliances use to connect to the Central Intelligence Unit. Normally you specify the same address for the **IP address** in **Network Settings** and the **Local Management Address**. If you change this address after you run the setup wizard, the new address is propagated to all managed appliances. ■ **Management Password** The password that managed appliances use to authenticate to the Central Intelligence Unit.
Proxy settings	The following proxy settings may be desired if you have a proxy in your network: ■ **Use proxy for Central Intelligence Unit secure communication (SSL) with Symantec Threat Center** ■ **Analyze ports used by proxy**
Time zone	Select the time zone in which Symantec Web Gateway is installed.

10 Click **Finish**.

11 The appliance restarts.

Additional configuration is necessary for Symantec Web Gateway to function properly.

See "Configuring Symantec Web Gateway after running the setup wizard" on page 39.

Connecting a Central Intelligence Unit to the network

Connect a Central Intelligence Unit to a part of the network where the managed appliances can reach the Central Intelligence Unit. The managed appliances access the Central Intelligence Unit using the **Local Management Address** that you specified in the setup wizard for the Central Intelligence Unit.

To connect a Central Intelligence Unit to the network

- Connect a straight-through (not crossover) Ethernet cable from the Mgmt port of the Central Intelligence Unit to a LAN switch port.

  Do not connect the Monitor, LAN, or WAN ports on the Central Intelligence Unit to the network.

Configuring appliances to accept management by a Central Intelligence Unit

Each Symantec Web Gateway appliance that you want to manage with a Central Intelligence Unit must be configured to accept management. You can still log on to the Web GUI of the managed appliances if necessary.

See "Steps to install a Central Intelligence Unit" on page 120.

If the setup wizard has not been run on the appliance, complete that procedure before this procedure.

See "Steps to install Symantec Web Gateway" on page 15.

Note: For the Central Intelligence Unit to communicate with managed appliances, the Central Intelligence Unit and managed appliances must be running the same software version. For example, if the Central Intelligence Unit is running version 4.5.2, then all managed appliances must be running version 4.5.2 also.

To configure appliances to accept management by a Central Intelligence Unit

1. In the Web GUI of an appliance that you want a Central Intelligence Unit to manage, click **Administration > Configuration > Central Mgmt**.
2. Click **Enable Central Management**.
3. In **Local Management Address**, type the address for the Central Intelligence Unit to contact this Web Gateway.

   You can type an IP address or hostname that the Central Intelligence Unit can resolve. Normally the address you specify for the **Local Management Address** is the same address that you specified for this appliance in the setup wizard. If the managed appliance is separated from the Central Intelligence Unit by a NAT server, specify an address that the Central Intelligence Unit can resolve.
4. In **Management Password**, type the management password that you specified on the Central Intelligence Unit.

5 In **Upload Frequency**, type the frequency in minutes that the appliance uploads events to the Central Intelligence Unit.

   A lower number results in more current data in the Central Intelligence Unit but also places load on the appliance and the Central Intelligence Unit. The default upload frequency is 5 minutes. The recommended upload frequency is also 5 minutes.

6 Click **Add a Central Manager**.

7 Type the host name or IP address of the Central Intelligence Unit.

   If the managed appliance is separated from the Central Intelligence Unit by a NAT server, specify an address that the managed appliance can resolve. Specify a fully qualified domain name if you did not specify the **DNS Suffix** on the **Administration > Configuration > Network** page.

8 Click **Save**.

Index