Symantec™ Web Gateway 5.1

Implementation Guide

Symantec

Symantec Web Gateway Version 5.1 Beta Implementation Guide

Documentation version: 5.1

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

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

www.symantec.com/business/support/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

- Product release level

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

Contents

Technical Support 4

Chapter 1 Introducing Symantec Web Gateway 13

About Symantec Web Gateway 13
What's new 14
What you can do with Symantec Web Gateway 15
Where to get more information 17

Chapter 2 Planning for installation 19

Preinstallation checklist 19
System requirements 23
About Symantec Web Gateway network configurations 24
About the Symantec Web Gateway operating modes 26
Port connections for typical network configurations 27
Diagrams of typical network configurations 30
Ports and settings that Symantec Web Gateway uses 37
Connections, ports, and indicators on the Symantec Web Gateway appliance 43

Chapter 3 Installing Symantec Web Gateway 45

Installing Symantec Web Gateway 46
Installing the Symantec Web Gateway appliance into a rack 47
Configuring a computer to access Symantec Web Gateway for installation 47
Running the setup wizard 48
Post-installation tasks 52
Accessing the Web GUI 54
Connecting Symantec Web Gateway to your network 55
About ensuring Internet connectivity if Symantec Web Gateway is disabled 56
Testing the bypass mode 58
Specifying internal networks 59
Enabling URL filtering, Internet program monitoring, and other features 60

Creating static routes for the inline network configuration 62
Specifying a mail server for alerts and reports 63
Specifying internal email and external proxy servers for report accuracy 64
Testing Symantec Web Gateway for successful blocking or monitoring 64
Testing Symantec Web Gateway Threat Center connectivity 65
Running the setup wizard after initial installation 66

Chapter 4 Installing Symantec Web Gateway Virtual Edition 67

About Symantec Web Gateway Virtual Edition 67
Installing Symantec Web Gateway Virtual Edition 68
System requirements for Symantec Web Gateway Virtual Edition 72
About adding the VMware LAN Network virtual switches 73
About configuring the VMware virtual switch 75

Chapter 5 Configuring the Symantec Web Gateway proxy 77

About the Symantec Web Gateway proxy 77
Available features when the Symantec Web Gateway proxy is enabled 78
Required Web browser settings for the Symantec Web Gateway proxy 80
Configuring the Symantec Web Gateway HTTP proxy and HTTPS proxy 81
How SSL Deep Inspection differs from SSL Domain Level Inspection 82
Configuring the Symantec Web Gateway proxy for SSL Deep Inspection 85
Configuring the Symantec Web Gateway proxy for SSL Domain Level Inspection 87
Specifying a Symantec Data Loss Prevention server 87
Configuring the Symantec Web Gateway SOCKS proxy 89
Configuring the Symantec Web Gateway FTP proxy 89

Chapter 6 Configuring policies 91

About policies 92
Configuring the policy precedence order 95
Download behavior in user Web browsers 95

Internet applications, malware, and URL filtering blocking behavior 97
Specifying computers or users for policies 101
About Insight reputation-based security 103
Enabling Insight reputation-based security 104
Configuring policies for Insight reputation-based security 106
Configuring policies for SSL Deep Inspection 107
Configuring policies for malware 108
Configuring policies for Internet applications 111
Malware categories for policies 113
Configuring URL filtering policies for Web sites 118
URL filtering categories 122
Upgrade considerations for Symantec Web Gateway version 5.1 133
Symantec RuleSpace URL filtering categories mapping information 134
Reporting misclassified URLs 139
Configuring embedded URL detection 139
Allowing after hours access to Web sites 140
Quarantining infected computers 141
Configuring NTLM user authentication behavior 142
Blocking or monitoring Web sites using the blacklist 143
Blocking or monitoring file transfers using the blacklist 145
Allowing Web site access using the whitelist 146
About the Blocking Feedback report 148
About end user pages 148
End user pages for blocked Web sites, file transfers, and infections 149
Variables for end user pages 152

Chapter 7 Administering Symantec Web Gateway 155

About system users 156
Permissions for system users 156
About roles for system users 156
Creating roles for system users 157
Creating system users 159
Monitoring system user activity 160
About database and software updates 161
About alerts 162
About sending alerts to syslog 163
About monitoring Symantec Web Gateway using SNMP 163

About backing up and restoring the Symantec Web Gateway configuration 164
Cross-model backup and restore compatibility 164
Backup file contents 165
Creating a manual backup 166
Creating a scheduled backup 167
Restoring backups 168
Enabling and disabling remote assistance 171
Uploading diagnostic files 172
Resetting Symantec Web Gateway to factory settings 172
Restarting and turning off the Symantec Web Gateway appliance 173
Configuring incident history 173
Testing ports connectivity 174
Testing NTP server connectivity 174
Testing mail server settings 175
Resetting the Web GUI password for the primary system user 175
Serial Console access to Symantec Web Gateway 176
About traffic capture 177
Enabling and disabling network traffic capture 178
Viewing the network traffic capture files 178
Configuring the usage of network capture files 179
Filtering network traffic capture 180

Chapter 8 Reports 181

About reports 181
Exporting a report to a .csv file 184
Scheduling automatic reports 185
Monitoring user browse time 187

Chapter 9 Configuring Active Directory integration 189

About Active Directory integration 189
Active Directory compatibility with Symantec Web Gateway 190
Comparison of Active Directory integration with a domain controller and NTLM 190
Configuring Active Directory integration by using DCInterface 193
Configuring Active Directory integration 194
Installing the Symantec Domain Controller Interface software 196
Configuring the Symantec Domain Controller Interface 198
Configuring the Symantec Domain Controller Interface for remote Active Directory access 198

Starting the Symantec Domain Controller Interface 199
Moving the `DCinterface.exe` file 200
Configuring Active Directory integration with NTLM 200
Specifying the Management Interface Name in Symantec Web Gateway 202
DNS change needed for NTLM 202
Configuring Symantec Web Gateway to integrate Active Directory with NTLM 203
Web browser changes needed for NTLM 205
Ensuring compatibility with NTLMv1 and NTLMv2 206
Configuring NTLMv1 and NTLMv2 compatibility for Windows Vista and Windows 7 207
Configuring NTLMv1 and NTLMv2 compatibility for Outlook 2003 and Windows XP SP2 208
Configuring NTLMv2 compatibility for Windows XP 209
Setting up the ignore authentication in NTLM v2 client 209
Ignoring authentication when you use the NTLM v2 client to configure the whitelist 210
Sample proxy auto-configuration (PAC) file 211
Refreshing Active Directory user data in reports 212

Chapter 10 Configuring a Central Intelligence Unit to manage multiple appliances 213

About centralized management using a Central Intelligence Unit 213
Installing a Central Intelligence Unit 214
Running the setup wizard for initial installation of a Central Intelligence Unit 216
Connecting a Central Intelligence Unit to the network 219
Configuring appliances to accept management by a Central Intelligence Unit 219

Index 221

Chapter 1

Introducing Symantec Web Gateway

This chapter includes the following topics:

- About Symantec Web Gateway
- What's new
- What you can do with Symantec Web Gateway
- Where to get more information

About Symantec Web Gateway

Symantec Web Gateway is an innovative Web security gateway appliance that protects organizations against Web threats, which 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 to maintain critical uptime and employee productivity by blocking attacks.

Symantec Web Gateway contains the following key features:

- Fast protection at the Web gateway across multiple protocols for inbound and outbound web traffic
- Protection against malware threats on all Web file transfer channels
- Ability to inspect for, detect, and block active and dormant botnets
- URL filtering with flexible policy controls and in-depth reporting (the URL filtering license is required)

- Advanced application control capabilities with ability to monitor and control usage by end-users spanning multiple applications
- Detection of compromised endpoints by network fingerprinting and behavioral modeling
- Comprehensive Web reporting and alerting
- Flexible policy controls, which allow policy creation on Web-based criteria and control over of how policies are applied across an organization
- SSL-encrypted network traffic monitoring for URL content filtering, blacklisted-domain matching, and malware
- Adaptability to deploy as an appliance or as a virtual machine on VMware ESX/ESXi 4.1/4.0
- Integration with Symantec Data Loss Prevention to discover, monitor, and protect confidential data

Symantec Web Gateway provides the following key benefits:

- Symantec AntiVirus Engine, the winner of over 40 consecutive VB100 Awards since 1999

  Insight is a Symantec reputation-based technology that can flag probable malware not previously known to Symantec.
- Highly scalable technology to meet the needs of any size organization without added latency, which ensures minimal affect on user browsing performance
- The Symantec Global Intelligence Network, which 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's new

Table 1-1 describes the major new features or enhancements in Symantec Web Gateway 5.1.

Table 1-1 What's new in Symantec Web Gateway

New feature or enhancement	Description
Effective URL filtering	Symantec Web Gateway uses Symantec's RuleSpace Web Categorization Solution (Symantec RuleSpace) to classify URL filtering categories. Symantec RuleSpace has several new URL categories and classes and makes URL filtering more effective than the previous URL filtering database. See "URL filtering categories" on page 122. See "Upgrade considerations for Symantec Web Gateway version 5.1" on page 133.
Embedded URL detection	You can configure Symantec Web Gateway to detect embedded URLs. See "Configuring embedded URL detection" on page 139.
Network traffic capture	Symantec Web Gateway lets you capture traffic on your network. The captured information helps you troubleshoot any issues that are related to network traffic. See "About traffic capture" on page 177.
User name authentication through Symantec Data Loss Prevention server	Symantec Web Gateway transfers user name to Symantec Data Loss Prevention server, when a user posts a message or uploads a file over HTTPS. You can view the user name on the **Custom Reports** page. See "Specifying a Symantec Data Loss Prevention server" on page 87.

What you can do with Symantec Web Gateway

Table 1-2 describes what you can do with Symantec Web Gateway.

Table 1-2 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 or as a proxy server to block downloads. See "Configuring policies for malware" on page 108.

Table 1-2 What you can do with Symantec Web Gateway *(continued)*

Tasks	Description
Block selected Internet applications by category	You can configure Symantec Web Gateway to prevent peer-to-peer sharing, streaming media, games, and other Internet applications from accessing the Internet. See "Configuring policies for Internet applications" on page 111.
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. See "Configuring URL filtering policies for Web sites" on page 118.
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, and so on. See "About reports" on page 181.
Configure alerts	Symantec Web Gateway can issue alerts for attacks, infections, and system events. Symantec Web Gateway transmits alerts by email, syslog, or SNMP. See "About alerts" on page 162.
Quarantine infected computers	Symantec Web Gateway can automatically block inbound and outbound Internet access for infected computers to prevent malware from spreading. See "Quarantining infected computers" on page 141.
Integrate with Symantec Data Loss Prevention	Symantec Web Gateway can pass outbound Web traffic through Symantec Data Loss Prevention to protect your company's data assets. You must have a separate Symantec Data Loss Prevention appliance. See "Specifying a Symantec Data Loss Prevention server" on page 87.

Table 1-2 What you can do with Symantec Web Gateway *(continued)*

Tasks	Description
Inspect SSL-encrypted Internet traffic	Symantec Web Gateway can monitor SSL-encrypted Internet traffic for malware or pass the encrypted traffic to Symantec Data Loss Prevention. You must have a separate Symantec Data Loss Prevention appliance to analyze SSL-encrypted traffic for data loss. See "Configuring the Symantec Web Gateway proxy for SSL Deep Inspection" on page 85.

Where to get more information

Table 1-3 provides sources where you can get more information about Symantec Web Gateway.

Table 1-3 More information about Symantec Web Gateway

Source	Description and location
Documentation	The Symantec Web Gateway documentation set consists of the following materials: ■ *Symantec Web Gateway Implementation Guide* ■ *Symantec Web Gateway Getting Started Guide* ■ *Symantec Web Gateway Release Notes*
Product Help system	Symantec Web Gateway includes a comprehensive Help system.

Table 1-3 More information about Symantec Web Gateway *(continued)*

Source	Description and location
Symantec Web site	Visit the following Symantec Web sites for more information about Symantec Web Gateway: ■ Knowledge base articles Articles to help you troubleshoot issues with Symantec Web Gateway www.symantec.com/business/support/index?page=landing&key=58161 ■ SymConnect Forum Users post the questions that other users and Symantec Technical Support answer www.symantec.com/connect/security/forums/web-gateway ■ Product alerts Subscribe to late-breaking news about new releases and hot issues http://www.symantec.com/business/support/index?page=content&key=58161&channel=ALERTS ■ English PDF documentation All available .pdf document for Symantec Web Gateway in English www.symantec.com/business/support/index?page=content&key=58161&channel=DOCUMENTATION ■ Technical Support Contact information and downloads www.symantec.com/enterprise/support ■ Licensing Information about how to register, activate, and manage existing license https://licensing.symantec.com/acctmgmt/index.jsp ■ Virus encyclopedia Information about all known threats; information about hoaxes and access to white papers about threats www.symantec.com/business/security_response/index.jsp ■ Documentation about data loss prevention Information about how to configure and use Symantec Data Loss Prevention See the *Symantec Data Loss Prevention Administration Guide*, which available with the download of the Symantec Data Loss Prevention software.

Chapter 2

Planning for installation

This chapter includes the following topics:

- Preinstallation checklist
- System requirements
- About Symantec Web Gateway network configurations
- About the Symantec Web Gateway operating modes
- Port connections for typical network configurations
- Diagrams of typical network configurations
- Ports and settings that Symantec Web Gateway uses
- Connections, ports, and indicators on the Symantec Web Gateway appliance

Preinstallation checklist

Table 2-1 contains the decisions that you should make and the items that you should have on hand before you install Symantec Web Gateway.

Table 2-1 Preinstallation checklist

Item	Description
Review the system requirements.	Ensure that you have met all of the system requirements. See "System requirements" on page 23.

Table 2-1 Preinstallation checklist *(continued)*

Item	Description
Determine if you intend to use the Symantec Web Gateway proxy.	The use of the Symantec Web Gateway proxy dictates which operating modes you can use and requires you to use the management port. See "About the Symantec Web Gateway proxy" on page 77.
Determine how you want to install Symantec Web Gateway in your network.	The manner in which you connect to your network affects its capabilities. See "About Symantec Web Gateway network configurations" on page 24. See "Port connections for typical network configurations" on page 27. See "Diagrams of typical network configurations" on page 30.
Determine which operating mode you intend to use.	The operating modes let you either monitor Internet traffic or monitor traffic and block traffic. See "About the Symantec Web Gateway operating modes" on page 26.
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 and settings that Symantec Web Gateway uses" on page 37.
Have a computer with an Ethernet port for initial setup. (Required for physical appliance only.)	Connect a computer to the management port on Symantec Web Gateway to initially configure it. Any computer and operating system works for this purpose. This computer must have a supported Web browser to access the Web GUI. See "Connections, ports, and indicators on the Symantec Web Gateway appliance" on page 43. See "System requirements" on page 23.
Decide on an administrator user name and password.	Decide on 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.

Table 2-1 Preinstallation checklist *(continued)*

Item	Description
Decide on an email address.	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 **Logon** page, and Symantec Web Gateway sends a new password to this address.
Have your license file in an accessible location.	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 Symantec Web Gateway functionality if you run the setup wizard without a license. The following types of licenses are available for Symantec Web Gateway: ■ Symantec Web Gateway license file The Symantec Web Gateway license enables Symantec Web Gateway to detect spyware, viruses, botnet infections, enforce application control, and enable Insight reputation-based security. ■ URL filtering license file In addition to the features in the Symantec Web Gateway license, the URL filtering license lets you monitor or block access to Web pages based on categorization.

Table 2-1 Preinstallation checklist *(continued)*

Item	Description
Know your IP address and related network settings for the Symantec Web Gateway appliance.	Determine if you intend to use a single IP address or two IP addresses. With one IP address, you can use a static address or you can rely on DHCP. Symantec recommends that you use a static IP address. The two IP address configuration is recommended if you plan to connect Symantec Web Gateway in the inline network configuration. Symantec Web Gateway requires two IP addresses if you intend to install Symantec Web Gateway in a proxy configuration. The IP addresses must be static and in different subnets. In the two IP address configuration, Symantec Web Gateway uses one IP address for communication with the Web GUI through the management port. Symantec Web Gateway uses the other IP address for communication with the user. For example, Symantec Web Gateway uses this IP address to send the end user blocking pages and authentication requests. The two IP addresses must be on different networks. 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. You need the following network settings for a static IP address: ■ IP address ■ Subnet mask ■ Default gateway ■ Primary DNS ■ Secondary DNS (optional) ■ DNS suffix (optional)

Table 2-1 Preinstallation checklist *(continued)*

Item	Description
Know your external proxy information. (Optional)	An external proxy is not required for Symantec Web Gateway to function. However, if Symantec Web Gateway uses an external proxy or users access the Internet through an external proxy, you must specify the following information: ■ Proxy IP address and port for Symantec Web Gateway to use for Internet access The external proxy must permit access to the Internet without the need for authentication. ■ HTTP proxy ports that users use to access the Internet
Know your DNS IP address and suffix. (Optional)	If you intend to use DNS, you must provide a DNS address. Optionally, you can provide a second DNS address and a DNS suffix.
Have a list of your internal subnets.	You must specify your internal subnets in Symantec Web Gateway after you run the setup wizard. See "Post-installation tasks" on page 52.
Have up to five normal and two crossover Ethernet cables.	You need up to four normal and up to two crossover Ethernet cables. The number of cables that you need depends on your network configuration 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. See "Port connections for typical network configurations" on page 27. See "Diagrams of typical network configurations" on page 30.

After you complete the preinstallation checklist, you can proceed with the installation.

See "Installing Symantec Web Gateway" on page 46.

System requirements

Table 2-2 lists the supported system requirements.

Table 2-2 Symantec Web Gateway system requirements

Requirement	Description
Appliance	You can run this release of Symantec Web Gateway on any of the following appliance models: ■ Symantec Web Gateway model 8490 ■ Symantec Web Gateway model 8450 ■ Symantec Web Gateway 84V (virtual edition)

Web browser	The following are the Web browser requirements:
	■ Computer that you use to access the Symantec Web Gateway Web GUI:
	  ■ Microsoft Internet Explorer 9/8/7/6
	  ■ Mozilla Firefox 14/13/12
	■ Client computers:
	  ■ Microsoft Internet Explorer 9/8/7/6
	  ■ Mozilla Firefox 14/13/12
	In most cases, Symantec Web Gateway does not require changes to any user software including the Web browser. However, if you configure Active Directory integration to use NTLM 401 authentication (only used in inline or tap network configurations), you may have to change the Web browser configuration on user computers. This change prevents an authentication pop-up window. You may also have to change the Web browser configuration on user computers if you use the Symantec Web Gateway proxy.
	See "Web browser changes needed for NTLM" on page 205.
	See "Required Web browser settings for the Symantec Web Gateway proxy" on page 80.

See "System requirements for Symantec Web Gateway Virtual Edition" on page 72.

About Symantec Web Gateway network configurations

Symantec Web Gateway offers a variety of ways that you can set up the product in your network. After you determine the network configuration that you want to use, you can determine the operating mode that best suits your needs.

See "About the Symantec Web Gateway operating modes" on page 26.

Table 2-3 describes the ways to connect Symantec Web Gateway to your network.

Table 2-3 Symantec Web Gateway network configurations

Network configuration	Description
Port span/tap	Blocks Web sites and phone-home attempts but cannot block file transfers. The port span/tap configuration may be easier to set up because it only requires one connection to your LAN. This configuration is useful as an initial test of Symantec Web Gateway. See Figure 2-7 on page 37. See "Download behavior in user Web browsers" on page 95.
Inline	Blocks file transfers, Web sites, and phone-home attempts. Inline configuration requires more network connections than port span/tap. See Figure 2-1 on page 31.
Proxy	Only analyzes the proxy traffic that is explicitly proxied to Symantec Web Gateway proxy. This means that Symantec Web Gateway can only analyze HTTP, HTTPS, FTP, and SOCKS Internet traffic. This configuration requires changes in your network to ensure that users' browsers use the Symantec Web Gateway proxy to access the Internet. See Figure 2-4 on page 34. See "Required Web browser settings for the Symantec Web Gateway proxy" on page 80.
Inline + proxy	A combination of both the inline network configuration and the proxy network configuration. Symantec Web Gateway can explicitly analyze both the proxy traffic and native traffic that pass through the WAN/LAN ports. See Figure 2-1 on page 31. See "Required Web browser settings for the Symantec Web Gateway proxy" on page 80.

Table 2-3 Symantec Web Gateway network configurations *(continued)*

Network configuration	Description
Inline and inline + proxy dual homing	Works the same as the inline configuration and the inline + proxy configuration but this configuration contains a second set of LAN and WAN ports. In an inline configuration, Symantec Web Gateway supports both of the LAN ports and WAN ports. In an inline + proxy configuration, Symantec Web Gateway only supports proxy function on LAN1 and WAN1 ports. Symantec Web Gateway only supports dual homing on the 8490 appliance. See Figure 2-3 on page 33.

See "Port connections for typical network configurations" on page 27.

About the Symantec Web Gateway operating modes

The mode that you choose defines Symantec Web Gateway's default behavior. You can override the default settings when you configure policies.

Table 2-4 describes the modes that are available for Symantec Web Gateway.

Table 2-4 Symantec Web Gateway operating modes

Mode	Description
Blocking	Based 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 the same reports on user activity as it does in monitoring mode. You must install Symantec Web Gateway in the inline network configuration to block file transfers. See "About Symantec Web Gateway network configurations" on page 24.
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.

See "Download behavior in user Web browsers" on page 95.

Port connections for typical network configurations

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

See "Diagrams of typical network configurations" on page 30.

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 "About ensuring Internet connectivity if Symantec Web Gateway is disabled" on page 56.

Table 2-5 Port connections for typical network configurations

Network configuration	Description	Connect Management to	Connect Monitor to	Connect LAN to	Connect WAN to
Port span/tap	Simple port span/tap network configuration. See Figure 2-1 on page 31.	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 (optional)	Not used
Proxy mode	Single leg proxy configuration. Symantec Web Gateway only inspects traffic directed to the Web Gateway proxy ports.	Port on a subnet separate from the LAN port subnet (required)	Not used	Port on your LAN switch (required)	Not used

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

Network configuration	Description	Connect Management to	Connect Monitor to	Connect LAN to	Connect WAN to
Inline + Proxy mode	Symantec Web Gateway is in transparent bridge operation and explicit proxy is enabled on the LAN and WAN ports. All traffic directed to the appliance is analyzed. Note that Dual Homing, available on some models, is not provided for proxy services. Proxy services are only provided over the LAN1/WAN1 ports, even if dual homing is enabled. Inline traffic is still inspected and forwarded over LAN2/WAN2 if Dual Homing is enabled.	Port on a subnet separate from the LAN port subnet (required)	Not used	Port on your LAN switch (required)	Internet firewall LAN port (required)
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. **Note:** When Symantec Web Gateway service is disabled, you can access the Symantec Web Gateway Web GUI from the Management port only. See Figure 2-1 on page 31.	Port on your LAN switch (required)	Not used	Port on your LAN switch (required)	Internet firewall LAN port (required)

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

Network configuration	Description	Connect Management to	Connect Monitor to	Connect LAN to	Connect WAN to
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. You can configure the firewalls in active/active failover or active-standby failover. You should configure the Symantec Web Gateway appliances identically except for the network settings. See Figure 2-2 on page 32.	Port on your LAN switch (required)	Not used	Port on your LAN switch (required)	Internet firewall LAN port (required)
Inline with one NIC external 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 36.	Port on your LAN switch (required)	Not used	Port on the proxy (required)	Port on your LAN switch (required)
Inline with two NIC external proxies that are connected 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 2-3 on page 33.	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 Management to	Connect Monitor to	Connect LAN to	Connect WAN to
Inline with two NIC external proxies that are connected to Symantec Web Gateway and to the firewall	The proxy server is connected to the firewall and Symantec Web Gateway. See Figure 2-5 on page 35.	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

Diagrams of typical network configurations

The following are diagrams of typical network configurations.

See "Port connections for typical network configurations" on page 27.

Figure 2-1 Simple inline or inline + proxy network configuration

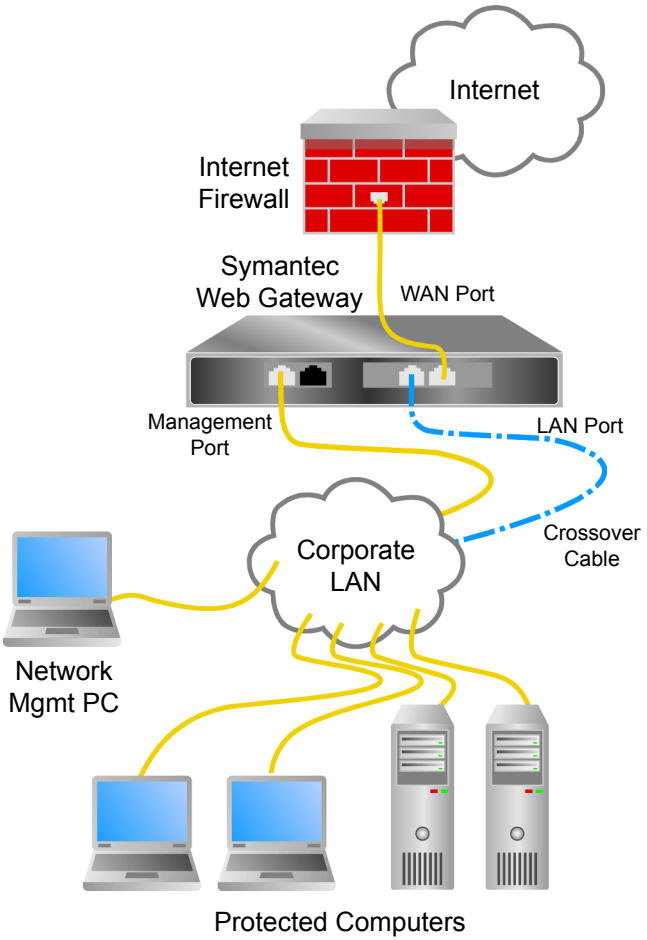


Figure 2-2 Inline with two firewalls, two external proxies, and two Symantec Web Gateway appliances

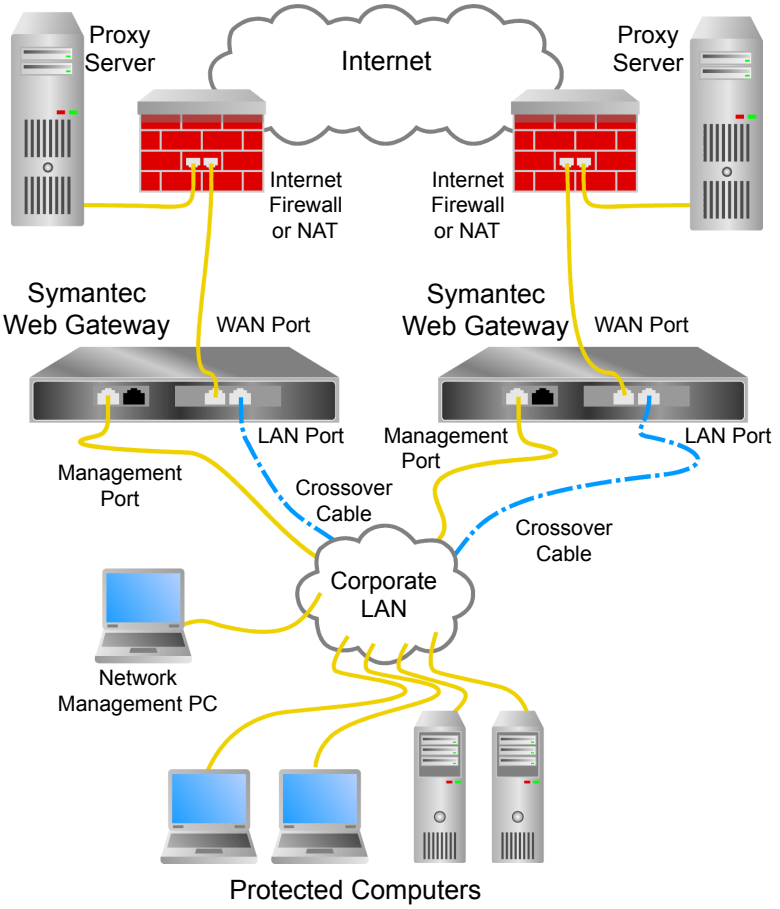


Figure 2-3 Inline with dual-homed Symantec Web Gateway inline

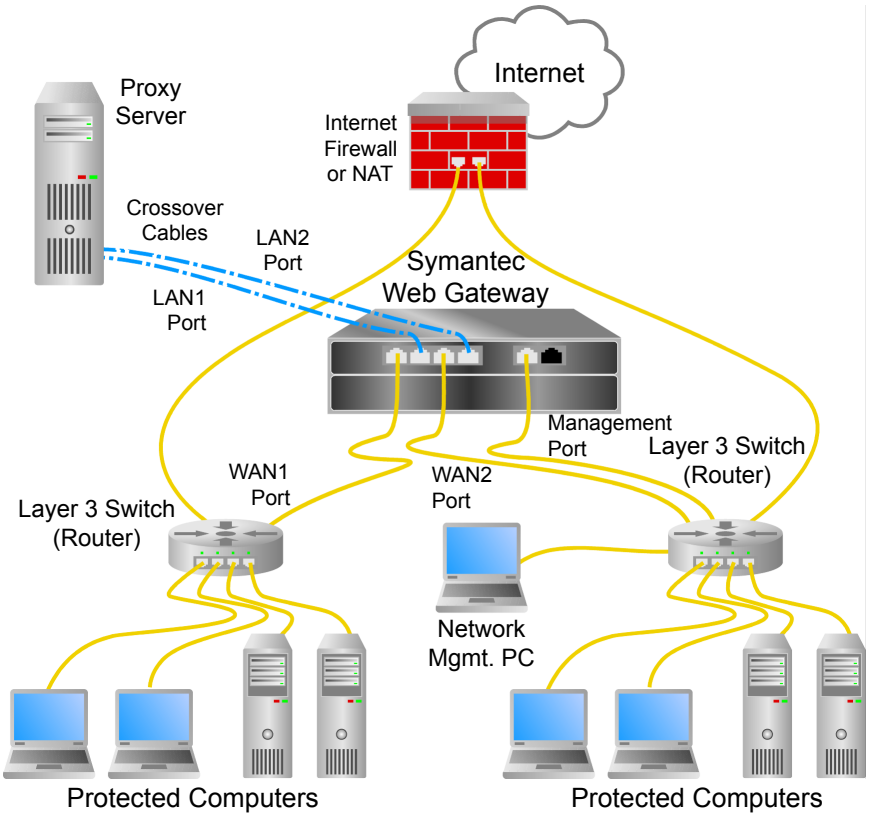


Figure 2-4 Symantec Web Gateway configured as a proxy

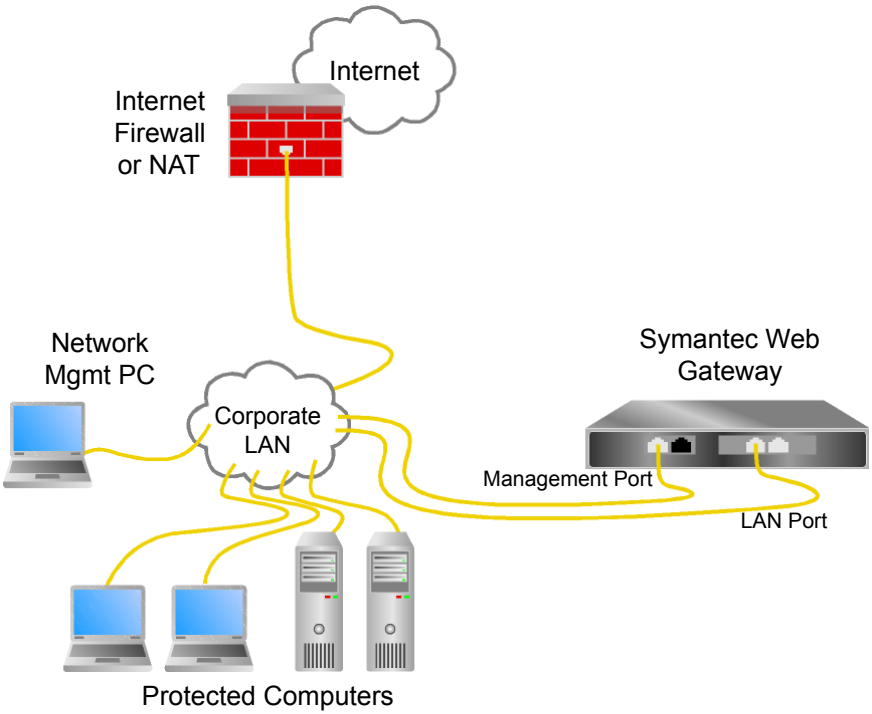


Figure 2-5 Inline Symantec Web Gateway with an external proxy server connected to firewall

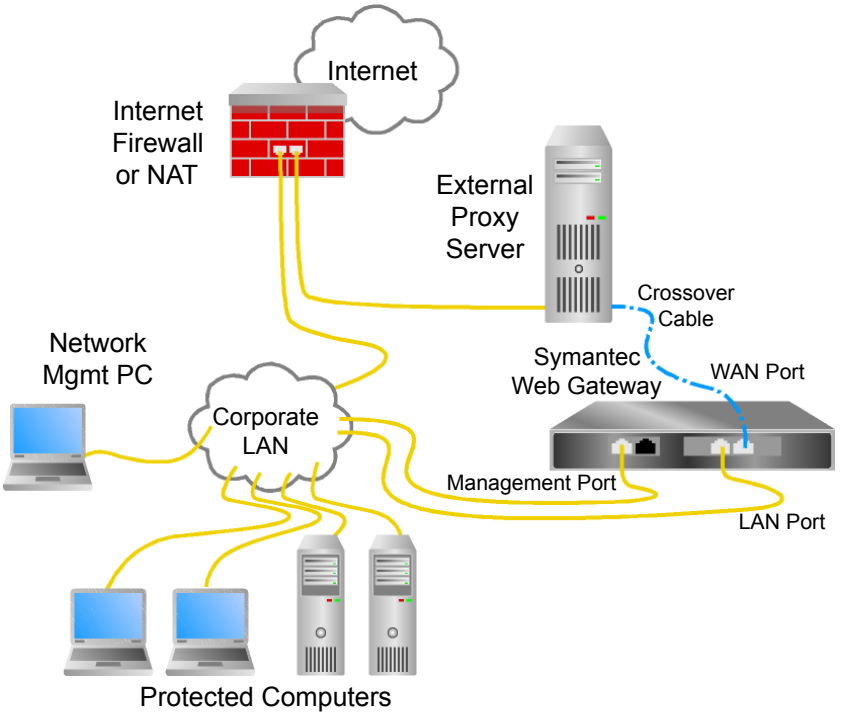


Figure 2-6 Inline with an external proxy server

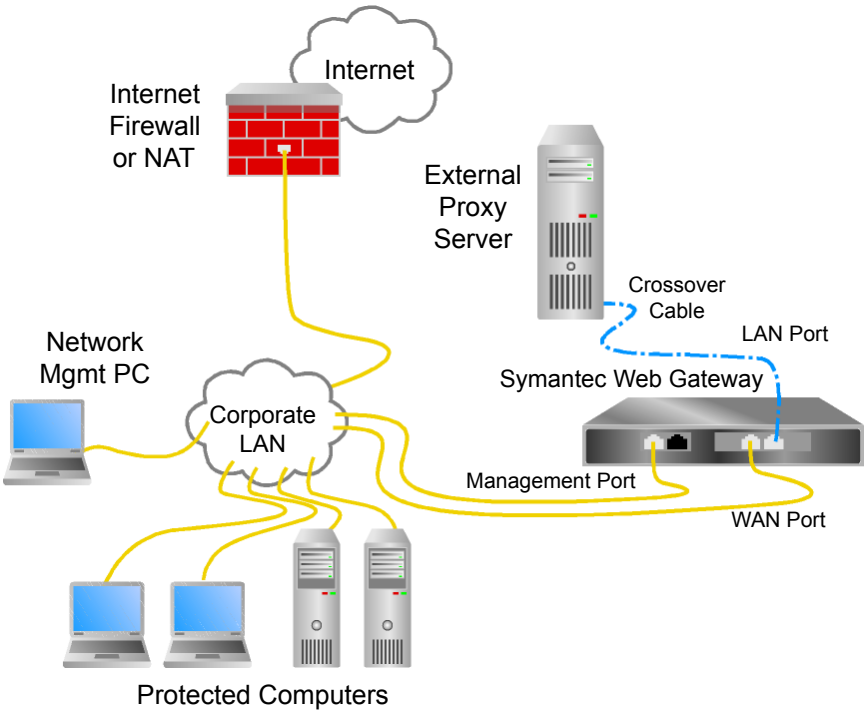
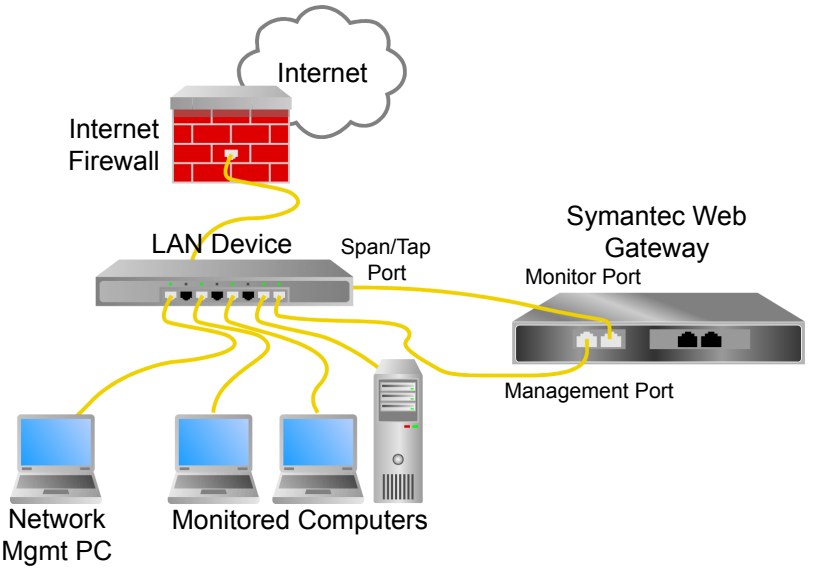


Figure 2-7 Simple port span/tap network configuration



Ports and settings that Symantec Web Gateway uses

Ports and URLs used for communications are useful in preparation of firewall for Symantec Web Gateway installation or troubleshooting communication problems.

Table 2-6 describes the ports that Symantec Web Gateway uses.

Table 2-6 Symantec Web Gateway ports and settings

URL	Port (Protocol)	From	To	Description
<hostname/IP>	TCP/25 (SMTP)	Symantec Web Gateway	User-defined SMTP mail servers	Delivers the SMTP notifications of alert conditions.
<hostname/IP>	UDP/53 (DNS)	Symantec Web Gateway	User-defined DNS servers	(Optional) Performs external DNS lookups, if configured.

Table 2-6 Symantec Web Gateway ports and settings *(continued)*

URL	Port (Protocol)	From	To	Description
liveupdate.symantec.com liveupdate.symantecliveupdate.com	TCP/80 (HTTP)	Symantec Web Gateway	Symantec LiveUpdate servers	Supplies the antivirus definitions downloads.
<hostname/IP> pool.ntp.org (default)	UDP/123 (NTP)	Symantec Web Gateway	User-defined NTP servers	Retrieves Network Time Protocol data from one or more Time servers.
<hostname/IP>	UDP/161 (SNMPv3)	Symantec Web Gateway	User-defined SNMP servers	(Optional) Provides the Simple Network Management Protocol (SNMP) trap and alerts, if configured.
<hostname/IP>	TCP/389 (domain controller) or TCP/3268 (Global Catalog)	Symantec Web Gateway	Active Directory servers	(Optional) Retrieves LDAP User information from Active Directory server, if configured.

Table 2-6 Symantec Web Gateway ports and settings *(continued)*

URL	Port (Protocol)	From	To	Description
threatcenter.symantec.com	TCP/443 (HTTP)	Symantec Web Gateway	Symantec Threat center servers	This port enables the following: ■ Symantec Web Gateway software update downloads, botnet signatures, and other updates. ■ Symantec Technical Support may use this port for remote system diagnosis.
mi5-shasta-rrs.symantec.com	TCP/443 (HTTP)	Symantec Web Gateway	Symantec Insight Reputation Server	This port receives the reputation content that is related to the Insight component and applies the relevant Insight-based policies.
<hostname/IP>	TCP/443 (Proprietary)	Central Intelligence Unit (CIU)	Symantec Web Gateway	(Optional) Polls Symantec Web Gateway for its status and data.

Table 2-6 Symantec Web Gateway ports and settings *(continued)*

URL	Port (Protocol)	From	To	Description
<hostname/IP>	TCP/443 (Proprietary)	Symantec Web Gateway	CIU	(Optional) Retrieves updates to configuration options from CIU.
<hostname/IP>	UDP/514 (Syslog)	Symantec Web Gateway	User-defined syslog servers	(Optional) Delivers malware alerts or system alerts to remote syslog, if configured.
<IP Address, as configured in dcinterface.txt>	TCP/60517 (Proprietary)	Symantec Web Gateway	dc interface	(Optional) Forwards audit success entries from the security log of the domain controller to Symantec Web Gateway, which permits Symantec Web Gateway to apply filtering policies based on LDAP.
<401 authentication port>	TCP/20200	Endpoint computer	Symantec Web Gateway	(Optional) Symantec Web Gateway to authenticate end user clients.
<Symantec Web Prevent communication channel>	ICAP/1344	Symantec Web Gateway	Symantec Web Prevent communication channel	(Optional) Used to communicate with the Symantec Web Prevent server.

Note: <hostname/IP> denotes the configuration that you provide based upon your local network architecture and your implementation plan for Symantec Web Gateway

Table 2-7 describes the proxy settings that Symantec Web Gateway uses.

Table 2-7 Symantec Web Gateway proxy settings

Settings	Port	From	To	Description
SOCKS Settings	1080	Web browser client	Symantec Web Gateway	You can enable Symantec Web Gateway proxy as SOCKS proxy for TCP and for UDP network traffic such as HTTP and FTP. Symantec Web Gateway supports the following SOCKS version 5. The default port is 1080, and you can modify as per your network configuration.
FTP Settings	8021	FTP client	Symantec Web Gateway	The proxy listens for FTP traffic at the port that you specify. The default port is 8021,and you can modify as per your network configuration.

Table 2-7 Symantec Web Gateway proxy settings *(continued)*

Settings	Port	From	To	Description
HTTP/S Proxy Settings	8080	Web browser client	Symantec Web Gateway	The proxy listens for HTTP/S traffic from the user Web browser at the specified ports. The default port is 8080, and you can modify as per your network configuration. These ports can only be used for the HTTP/S proxy.
SSL Deep Inspection Settings	8443	Web browser client	Symantec Web Gateway	The Symantec Web Gateway proxy listens for SSL traffic at the port that you specify. If you enable the internal HTTP/S proxy, the SSL port must be different than the HTTP/S ports. The default port is 8443, and you can modify as per your network configuration.

Connections, ports, and indicators on the Symantec Web Gateway appliance

The connections and ports on the back of the appliance that you need to configure Symantec Web Gateway are labeled. Connections that are not labeled are not functional or are not supported. Two solid (not blinking) LEDs indicate bypass mode is enabled.

Table 2-8 explains the connections and ports on Symantec Web Gateway appliances.

Table 2-8 Connections and ports on Symantec Web Gateway appliances

Connection or port	Description
USB ports	You can use this port to attach a keyboard to use for the command line interface. The Symantec Web Gateway appliance models that support a USB keyboard are listed below: ■ Symantec Web Gateway model 8450 Rev 1 or later You can view the revision of the Web Gateway model 8450 on the **System Status** page. ■ Symantec Web Gateway model 8490
Serial port	Connect the serial port to another computer to access the Serial Console character-based interface. See "Port connections for typical network configurations" on page 27.
LAN Ethernet port	Depending on how you deploy Symantec Web Gateway, you may connect the LAN port to your LAN switch.
WAN Ethernet port	Depending on how you deploy Symantec Web Gateway, you may connect the WAN port to your firewall.
Management (Mgmt) Ethernet port	Connect the management port to your LAN switch. The management port must have access to the following: ■ Domain Name Server (DNS) ■ Access to the required Internet services See "Ports and settings that Symantec Web Gateway uses" on page 37. ■ Domain controller (for authentication) See "Port connections for typical network configurations" on page 27.

Table 2-8 Connections and ports on Symantec Web Gateway appliances *(continued)*

Connection or port	Description
Monitor Ethernet port	If you deploy Symantec Web Gateway in a port span/tap network configuration, connect the monitor port to the network tap or a port on your LAN switch that is set to span mode. See "Port connections for typical network configurations" on page 27.
Keyboard	You can use this connection to attach a keyboard to use for the command line interface. The Symantec Web Gateway appliance models that support a USB keyboard are listed below: ■ Symantec Web Gateway model 8450 Rev 1 or later You can view the revision of the Web Gateway model 8450 on the **System Status** page. ■ Symantec Web Gateway model 8490
Mouse	This connection is not functional.
Power	This connection provides power to the appliance. Your appliance may have an extra, redundant power connection.

Chapter 3

Installing Symantec Web Gateway

This chapter includes the following topics:

- Installing Symantec Web Gateway
- Installing the Symantec Web Gateway appliance into a rack
- Configuring a computer to access Symantec Web Gateway for installation
- Running the setup wizard
- Post-installation tasks
- Accessing the Web GUI
- Connecting Symantec Web Gateway to your network
- About ensuring Internet connectivity if Symantec Web Gateway is disabled
- Testing the bypass mode
- Specifying internal networks
- Enabling URL filtering, Internet program monitoring, and other features
- Creating static routes for the inline network configuration
- Specifying a mail server for alerts and reports
- Specifying internal email and external proxy servers for report accuracy
- Testing Symantec Web Gateway for successful blocking or monitoring
- Testing Symantec Web Gateway Threat Center connectivity

- Running the setup wizard after initial installation

Installing Symantec Web Gateway

Before you install Symantec Web Gateway, ensure that you complete all of the items on the preinstallation checklist.

See "Preinstallation checklist" on page 19.

Table 3-1 describes the steps to install and initially configure Symantec Web Gateway.

Table 3-1 Steps to install Symantec Web Gateway

Step	Action	Description
Step 1	Mount the appliance.	Mount the Symantec Web Gateway appliance into a rack, but do not connect the Ethernet cables yet. See "Installing the Symantec Web Gateway appliance into a rack" on page 47.
Step 2	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 47.
Step 3	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" on page 48.

When you finish the installation, perform the post-installation tasks to ensure that you properly configure and test Symantec Web Gateway.

See "Post-installation tasks" on page 52.

Installing the Symantec Web Gateway appliance into a rack

You can mount the Symantec Web Gateway appliance into a 19-inch (483mm) rack. If you do not have a rack, the Symantec Web Gateway appliance can rest on a stable surface.

After you install the appliance into a rack, configure a computer to access the setup wizard next. But do not connect the Ethernet cables yet.

See "Configuring a computer to access Symantec Web Gateway for installation" on page 47.

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. If your appliance came with two power cords, connect the second power cord.

Configuring a computer to access Symantec Web Gateway for installation

You must connect a computer to the management port to initially set up Symantec Web Gateway. You must also configure the IP address and netmask of that computer.

After you install Symantec Web Gateway, you can access it from a browser on any computer in your network. You can also disconnect the computer from the management port and reconfigure the network settings as desired.

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)**.

For more information about how to configure your computer network settings, see your operating system documentation.

After you configure a computer to access Symantec Web Gateway for installation, run the setup wizard.

See "Running the setup wizard" on page 48.

To configure a computer to access Symantec Web Gateway for installation

1. Copy the license file 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 the following address:

   192.168.254.253
4. Set the subnet mask of the computer to the following address:

   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 management port on the back of the Symantec Web Gateway appliance.

Running the setup wizard

After you physically install Symantec Web Gateway and connect a computer to the management port, you can run the setup wizard. This procedure describes how to configure an appliance as a Web Gateway, not as a Central Intelligence Unit.

See "Installing a Central Intelligence Unit" on page 214.

When installation completes the Symantec Web Gateway services restart. The appliance does not restart.

To run the setup wizard

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

   The appliance takes several minutes to start.
2. On the computer that is connected to the management port, start a Web browser and go to the following URL:

   http://192.168.254.254

   The setup wizard automatically appears the first time that you install the product.
3. On the **Welcome** panel, click **Next**.
4. On the **License Agreement** panel, read the license agreement, check the box indicating that you accept the terms of the agreement, and then click **Accept**.
5. On the **Install License** panel, do the following tasks:

- In the **Company Name** box, type the name of your organization.
- Click **Browse** and locate your license file.
- Click **Next**.

If you do not install a license now, there is a two week grace period. During this time the product runs as if the Symantec Web Gateway license were installed.

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

You can only change the server type in the setup wizard. You cannot change it in the Web GUI after the setup wizard finishes.

See "Running the setup wizard after initial installation" on page 66.

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.
Reenter password	Type the password again to verify its accuracy.
Description (Optional)	Optionally, you can type a description for the current user account. This description appears on the **Edit User** page.
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:

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. It 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.

Mode

Select one of the following default operating mode 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. You can override these default operating modes with custom policies.
  Symantec recommends that you do not use Blocking mode, if you use the Inline configuration and you do not have static routes configured.

See "About the Symantec Web Gateway operating modes" on page 26.

Select one of the following network configurations:

- **Port span/tap**
- **Inline**
- **Proxy**
- **Inline + Proxy**

See "About Symantec Web Gateway network configurations" on page 24.

Network Settings	Do the following tasks: ■ To specify one IP address for the Web GUI and a separate IP address for the monitoring and blocking capabilities of Symantec Web Gateway, check **Enable separate management and inline networks**. ■ Specify if you want to use Automatic (DHCP) resolution or if you want to manually specify IP addresses. Symantec Web Gateway does not support DHCP when you enable separate management and inline networks. ■ If you did not check **Enable separate management and inline networks**, specify the **Management Network Settings**. Specify the IP address and related network settings for the Web GUI, monitoring capabilities, and blocking capabilities. ■ If you checked **Enable separate management and inline networks**, specify the following settings: ■ **Management Network Settings** Specify the IP address and related network settings for the Web GUI. The use of DHCP is disabled. ■ **Inline Network Settings** Specify the IP address and related network settings for the monitoring and blocking capabilities. ■ **DNS Settings** You can specify up to two IP addresses. You can optionally also specify a DNS suffix.
Proxy Settings (Optional, if you intend to use external proxies)	Specify the following external proxy settings: ■ Check **Use proxy for Web Gateway secure communications (SSL) with Symantec Threat Center** if you intend to have Symantec Web Gateway to use an external proxy to communicate with Symantec Threat Center. Also specify the proxy IP address and port. ■ Check **Analyze ports used by proxy** if you want Symantec Web Gateway to inspect the external proxy traffic from clients. Also specify the HTTP proxy port/port range and the FTP port.

Time Zone Setting	Click the drop-down list and select your time zone. The time zone settings do not apply if you use Symantec Web Gateway as a proxy.

10 Click **Finish**.

11 The Symantec Web Gateway service restarts.

See "Preinstallation checklist" on page 19.

See "Installing Symantec Web Gateway" on page 46.

Post-installation tasks

After you install the appliance and run the setup wizard, perform the following post-installation tasks to ensure that you properly configure and test Symantec Web Gateway.

Table 3-2 Post-installation tasks

Step	Task	Description
Step 1	Reconnect the Ethernet cable, if required.	If you selected the inline networking configuration., disconnect the Ethernet cable from the management port and connect it to the LAN port on Symantec Web Gateway. You do not need to switch to the LAN port if you use the two IP configuration. If Symantec Web Gateway is in bypass mode in this configuration, leave the Ethernet cable connected to the management port to access the Web GUI. With all other configurations, leave the Ethernet cable connected to the management port. In all configurations, keep the other end of the cable connected to your computer.

Table 3-2 Post-installation tasks *(continued)*

Step	Task	Description
Step 2	Configure Symantec Web Gateway to be able to access the Web GUI from a Web browser through your network.	On the computer that is connected to the management 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 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 47.
Step 3	Access the Web GUI.	Access the Web GUI to test Symantec Web Gateway and to perform post-installation configurations. See "Accessing the Web GUI" on page 54.
Step 4	Connecting Symantec Web Gateway to your network.	After you access the Web GUI, you can connect Symantec Web Gateway to your network. See "Connecting Symantec Web Gateway to your network" on page 55.
Step 5	Test bypass mode. (Inline configuration only)	If you configure Symantec Web Gateway for the inline configuration, test to ensure that the bypass mode operates properly. See "About ensuring Internet connectivity if Symantec Web Gateway is disabled" on page 56. See "Testing the bypass mode" on page 58.
Step 6	Specify your internal networks.	When you specify your internal networks, Symantec Web Gateway knows which networks are internal and which are external. See "Specifying internal networks" on page 59.

Table 3-2 Post-installation tasks *(continued)*

Step	Task	Description
Step 7	Enable key filtering and monitoring features.	Configure the following features: ■ Enable Insight reputation-based security See "Enabling Insight reputation-based security" on page 104. ■ Enable application control ■ Enable content filtering ■ Enable record browse view times See "Enabling URL filtering, Internet program monitoring, and other features" on page 60.
Step 8	Create static routes, if needed. (Inline configurations only)	If you plan to connect Symantec Web Gateway in the inline network configuration, specify static routes. See "Creating static routes for the inline network configuration" on page 62.
Step 9	Specify servers and proxies for reports and alerts.	You should specify your servers and external proxies so that they appear in your alerts and reports. See "Specifying a mail server for alerts and reports" on page 63. See "Specifying internal email and external proxy servers for report accuracy" on page 64.
Step 10	Test Symantec Web Gateway.	Test Symantec Web Gateway to ensure that it blocks and monitors Web traffic as you intend it. Also test the connection to the Threat Center. See "Testing Symantec Web Gateway for successful blocking or monitoring" on page 64. See "Testing Symantec Web Gateway Threat Center connectivity" on page 65.

Accessing the Web GUI

You can use the Web GUI to configure Symantec Web Gateway. Access the Web GUI from a Web browser on any computer in the LAN that is connected to Symantec Web Gateway.

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 the following:

   `http://`***IP address***

   Where *IP address* is the 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 per session.

Connecting Symantec Web Gateway to your network

After you complete the setup wizard, connect Symantec Web Gateway to your network based on the network configuration and operating mode that you configured during installation. Symantec recommends that you make the connections while the Symantec Web Gateway service is disabled. This way you can test that the bypass mode works while the service is disabled. Symantec Web Gateway only supports bypass mode for inline configurations.

To connect Symantec Web Gateway to your network

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

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

   See "About ensuring Internet connectivity if Symantec Web Gateway is disabled" on page 56.

   You can check the Symantec Web Gateway service status at **Administration > Configuration > Operating Mode**.
2. Disconnect your computer from the management 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.

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

See "Port connections for typical network configurations" on page 27.

4 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, ports, and indicators on the Symantec Web Gateway appliance" on page 43.

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

See "Post-installation tasks" on page 52.

About 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, Symantec Web Gateway routes Internet traffic through the LAN port and the WAN port, but no monitoring or blocking occurs.

Note: In the bypass mode, the Ethernet cables on the LAN port and the WAN port are interconnected. You must ensure that the total length of the interconnected cables does not exceed the maximum Ethernet cable length. The Ethernet cable length, per ANSI/TIA/EIA cabling standards, is 100m for Cat5e and Cat6.

For more information on the Ethernet cable length, refer the ANSI/TIA/EIA cabling standards.

Symantec Web Gateway Virtual Edition does not have a bypass mode. For Symantec Web Gateway Virtual Edition with inline configurations, network traffic is halted when the service is disabled or the physical host computer is turned off.

Table 3-3 explains the differences between the hardware bypass mode and software bypass mode.

Table 3-3 Symantec Web Gateway bypass modes

Hardware bypass mode	Software bypass mode
If the Symantec Web Gateway appliance is turned off, it is called Hardware bypass.	If the Symantec Web Gateway appliance is turned on and the Symantec Web Gateway service is disabled, it is called Software bypass.
Hardware bypass does not generate any reports for scanning, monitoring, and blocking.	Software bypass does not generates reports for scanning, monitoring, and blocking.
The WAN, LAN, management port, and monitoring ports are disabled. But traffic still flows through the LAN port and WAN port unimpeded.	The WAN port and LAN port are disabled. Traffic still flows through the LAN port and WAN port unimpeded.

For bypass mode to function properly, ensure that you use the proper type of Ethernet cables to connect to the LAN. Two solid LEDs on the back of the Symantec Web Gateway appliances indicate bypass mode is on.

See "Connections, ports, and indicators on the Symantec Web Gateway appliance" on page 43.

Note: If you connect the wrong type of Ethernet cable from Symantec Web Gateway to the LAN, Internet connectivity is blocked when Symantec Web Gateway is disabled or off. In bypass mode, Symantec Web Gateway works the same as if you were using a crossover Ethernet cable.

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 3-4 describes the cable options for LAN port.

Table 3-4 Connecting the LAN cable in the inline network configuration

LAN auto sensing behavior	Cable options for Symantec Web Gateway LAN port
The LAN switch that is 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 following row. If the LAN switch is unintentionally turned off, auto sensing may not function.
The LAN switch that is 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 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 configure 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 never blocks 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 that is configured in span mode.

See "Testing the bypass mode" on page 58.

Testing the bypass mode

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 port and the WAN port, 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. LEDs on the back of the Symantec Web Gateway appliances indicate bypass mode if it is not turned off.

Note: In the bypass mode, the Ethernet cables on the LAN port and the WAN port are interconnected. You must ensure that the total length of the interconnected cables does not exceed the maximum Ethernet cable length. The Ethernet cable length, per ANSI/TIA/EIA cabling standards, is 100m for Cat5e and Cat6.

For more information on the Ethernet cable length, refer the ANSI/TIA/EIA cabling standards.

To test the bypass mode

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

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

   See "About ensuring Internet connectivity if Symantec Web Gateway is disabled" on page 56.

2. 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 but not blinking.

   See "Connections, ports, and indicators on the Symantec Web Gateway appliance" on page 43.

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

4. Test Symantec Web Gateway to ensure that it functions properly.

   See "Testing Symantec Web Gateway for successful blocking or monitoring" on page 64.

Specifying internal networks

When you define 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. Check **Apply Static Routes to Internal Networks** if the following conditions apply, and then click **Save** and ignore the rest of this procedure:

   - You have configured static routes.

- Your internal networks are the same as or more than the static routes.

See "Creating static routes for the inline network configuration" on page 62.

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

Normally, do not check **Define internal network as addresses not in the following list**. That setting is for special cases of when you install Symantec Web Gateway in front of an external 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.

Symantec Web Gateway supports the wide subnets also known as supernets. If portions of your network are in a contiguous wide range, it is not necessary to have multiple separate internal network entries for each range. A single wide range is sufficient.

6 Optionally, in **Description**, type a description of the internal network.

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

You must enable some features of Symantec Web Gateway for them to function. Alternatively, you can disable the features that you do not use to improve Symantec Web Gateway performance.

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

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

2 Check the appropriate box to enable the following features:

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 Symantec Web Gateway license. See "Configuring policies for Internet applications" on page 111.
Enable Content Filter	If you have the URL filtering license, you can enable URL filtering. Configure URL filtering policies on the **Edit Policy** page. See "Configuring URL filtering policies for Web sites" on page 118.
Detect Embedded URLs	Symantec Web Gateway detects embedded URLs. See "Configuring embedded URL detection" on page 139.
Bypass Whitelist for Content Filter	If you check **Bypass Whitelist for Content Filter**, you disable the internal whitelist and your custom whitelist. The Web pages in those whitelists that Symantec Web Gateway normally ignores are subject to monitoring and blocking. This feature requires the URL filtering license. The internal whitelist contains the domain names for definition updates and software updates of antivirus vendors and software vendors. Due to security concerns, Symantec cannot publish the contents of the internal whitelist. Symantec recommends that you not bypass the whitelist for content filter.

Record browse time	Symantec Web Gateway records the approximate amount of time that each user views Web sites. This feature requires the URL filtering 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 Symantec Web Gateway detects no Web browsing activity after this time has elapsed, it stops tabulating the browse time. Symantec Web Gateway ignores or records the browse time depending on the **Threshold** value. The default is 3 minutes. See "Monitoring user browse time" on page 187.
Insight	Symantec Web Gateway can block, monitor, ignore, or allow access to files and other sources of malware based on reputation-based security. Insight is a Symantec technology that can flag probable malware not previously known to Symantec. See "Enabling Insight reputation-based security" on page 104.

3 Click **Save**.

Creating static routes for the inline network configuration

You must use static routes 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, users on that subnet may see the following error message: "Page not found."

Note: You do not have to configure static routes in the Web GUI if you deploy Symantec Web Gateway in the port span/tap network configuration. Symantec Web Gateway only requires static routes for the inline network configurations.

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 another subnet, 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 network 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 subnet.

   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 a mail server for alerts and reports

You can provide settings for an alternate mail server in case your default mail server fails to send reports and alerts to administrators.

To specify a mail server for alerts and reports

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

   The mail server that you specify must support the SMTP email protocol.
3. Uncheck **Requires Authorization** if the server does not require authentication.

   This server does not require authentication.
4. Click **Save**.

Specifying internal email and external proxy servers for report accuracy

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

To specify internal email and external 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**.

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.
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 configure 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 configure 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 reports. 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.

See "About the Symantec Web Gateway operating modes" on page 26.

Testing Symantec Web Gateway Threat Center connectivity

You can check the connection from Symantec Web Gateway to the Threat Center in the Web GUI. If Symantec Web Gateway can connect to the Threat Center, then it can also download database updates and software updates.

See "About database and software updates" on page 161.

To test Symantec Web Gateway Threat Center in the Web GUI

1. In the Symantec Web Gateway Web GUI, click **Administration > Configuration > Network**.
2. Beside **Test Connection to Symantec Threat Center**, click **Test**. The following message appears when the test connection is successful:

   Connection to Symantec Threat Center from Appliance Serial No. (Appliance ID) is successful.

Running the setup wizard after initial installation

You might want to run the setup wizard again to address the following issues:

- 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 175.
- 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 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 through the Serial Console. Symantec Web Gateway retains your initial configuration choices when you run the setup wizard again.

To run the setup wizard after initial installation

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

   See "Serial Console access to Symantec Web Gateway" on page 176.
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 appear. Complete the setup wizard.

   See "Running the setup wizard" on page 48.

Chapter 4

Installing Symantec Web Gateway Virtual Edition

This chapter includes the following topics:

- About Symantec Web Gateway Virtual Edition
- Installing Symantec Web Gateway Virtual Edition
- System requirements for Symantec Web Gateway Virtual Edition
- About adding the VMware LAN Network virtual switches
- About configuring the VMware virtual switch

About Symantec Web Gateway Virtual Edition

Symantec Web Gateway Virtual Edition runs as a virtual machine on VMware so that you can run Symantec Web Gateway on the hardware and operating system of your choice.

Table 4-1 describes some considerations about Symantec Web GatewayVirtual Edition.

Table 4-1 Symantec Web Gateway Virtual Edition usage notes

Consideration	Details
All network configurations are supported.	You can install Symantec Web Gateway Virtual Edition in any of the following network configurations: ■ Inline This configuration is supported but not recommended. ■ Proxy ■ Inline + proxy ■ Port span/tap ■ Central Intelligence Unit See "About Symantec Web Gateway network configurations" on page 24. See "About centralized management using a Central Intelligence Unit" on page 213.
The bypass mode is unsupported.	Symantec Web Gateway Virtual Edition does not have a bypass mode like the Symantec Web Gateway appliances. For Symantec Web Gateway Virtual Edition, in an inline network configuration, network traffic is halted when the service is disabled or the physical host computer is turned off. See "About Symantec Web Gateway network configurations" on page 24. See "About ensuring Internet connectivity if Symantec Web Gateway is disabled" on page 56.
Connecting management computers to the Management network.	You must connect the computers that you want to access the Web GUI to the Ethernet port that is assigned to the Management network.
The VMware snapshot is unsupported.	Symantec does not support restoring from a VMware snapshot. Use the instructions in this guide to install Symantec Web Gateway Virtual Edition.

See "Installing Symantec Web Gateway Virtual Edition" on page 68.

Installing Symantec Web Gateway Virtual Edition

Table 4-2 describes the steps to install Symantec Web Gateway Virtual Edition.

Table 4-2 Steps to install Symantec Web Gateway Virtual Edition

Step	Action	Description
Step 1	Review system requirements.	Ensure that you have a supported version of VMware and that the virtual machine is provisioned appropriately. See "System requirements for Symantec Web Gateway Virtual Edition" on page 72.
Step 2	Download the Virtual image files.	If you purchase a license for Symantec Web Gateway, you can download the Virtual image files from the Symantec File Connect site. To access Symantec File connect, on the Internet, go to the following URL: https://fileconnect.symantec.com/ If you have not yet purchased a license, you can download the Virtual image files from our product Trialware site. To access the Symantec Web Gateway Trialware site, on the Internet, go to the following URL: http://www.symantec.com/business/products/trialware.jsp?pcid=pcat_security&pvid=web_gateway_1 Ensure that you put all of the virtual image files in the same directory.
Step 3	Prepare your host.	Do the following tasks to prepare your virtual machine: ■ Add the VMware LAN network virtual switches and configure their port properties. Each Symantec Web Gateway port that you use (management, WAN, LAN, and monitor) requires one unique virtual switch. See "About adding the VMware LAN Network virtual switches" on page 73. ■ Configure the default VMware virtual switch. See "About configuring the VMware virtual switch" on page 75.

Table 4-2 Steps to install Symantec Web Gateway Virtual Edition *(continued)*

Step	Action	Description
Step 4	Deploy the OVF template.	Deploy the OVF template that you downloaded in Step 2 on a VMware ESX/ESXi Server. If you use ESX version 4.1, when you download the template, you may be asked to choose thin disk provisioning or thick disk provisioning. Symantec Web Gateway recommends that you use thick disk provisioning. An OVF template is a virtual machine that includes the software that you plan to run on the computer. You can deploy the OVF template with a vSphere client on a different computer than the computer that hosts your ESX/ESXi Server. Symantec Web Gateway only supports the deployment of an unaltered OVF template file. Symantec Web Gateway does not support the creation of an OVF template from the Symantec Web Gateway template. The OVF deployment takes about 10 minutes. When it completes, the new computer appears in your inventory. You may want to configure your guest computer to restart when the host computer restarts.
Step 5	Reserve memory for the Symantec Web Gateway virtual appliance.	You can set the memory reservation in vSphere in the **Resources > Memory > Reservation** settings. See "System requirements for Symantec Web Gateway Virtual Edition" on page 72.

Table 4-2 Steps to install Symantec Web Gateway Virtual Edition *(continued)*

Step	Action	Description
Step 6	Configure virtual network adapters.	To configure the virtual network adapters, do all of the following tasks: ■ In the vSphere client, edit the following setting: **Symantec_Web_Gateway_VMimage_5.1.0.*xxx*_Linux_EN** where *x.x..x* is the Symantec Web Gateway version release number. ■ Configure the network adapters with the following names and network connections: ■ Adapter 1 Management - Management network ■ Adapter 2 WAN - WAN network ■ Adapter 3 LAN - LAN network ■ Adapter 4 Monitor - Span/tap network **Note:** Depending on your deployment, not all of these settings may apply. See "Port connections for typical network configurations" on page 27. After you configure your virtual network adapters, verify in vSphere that they are properly configured.
Step 7	Physically connect the network adapters as you would for a non-virtual deployment.	Physically connect the actual network adapters to the ESX/ESXi host computer. See "Connections, ports, and indicators on the Symantec Web Gateway appliance" on page 43. See "Port connections for typical network configurations" on page 27. See "Diagrams of typical network configurations" on page 30.
Step 8	Start the virtual computer.	In the vSphere client, turn on the following: **Symantec_Web_Gateway_VMimage_5.0.0.*xxx*_Linux_EN** where *x.x..x* is the Symantec Web Gateway version release number. You must connect the computer that you to access the Web GUI to the Ethernet port that is assigned to the Management network.
Step 9	Run the setup wizard.	Run the Symantec Web Gateway setup wizard as you would for a non-virtual installation. See "Running the setup wizard" on page 48.

For more information about how to perform the tasks or navigate to the settings that are described in Table 4-2, consult your vSphere documentation.

System requirements for Symantec Web Gateway Virtual Edition

Table 4-3 lists the system requirements for Symantec Web Gateway Virtual Edition.

Table 4-3 System requirements for Symantec Web Gateway Virtual Edition

Requirement	Minimum for production environment
Disk space	90 GB (thick provisioned format)
Memory	The memory requirement is based on your network configuration mode, as follows: ■ Port span/tap mode: 4 GB ■ Inline mode: 4 GB ■ Proxy mode: 8 GB ■ Inline + proxy mode: 8 GB ■ CIU mode: 4 GB
CPUs	2

Table 4-4 lists the system requires for the host.

Table 4-4 System requirements for the ESX/ESXi host

Requirement	Minimum for production environment
VMware ESX Server or VMware ESXi Server	ESX version 4.0 or 4.1 ESXi version 4.0, 4.1, or 5.0
CPU type	64-bit
CPUs (includes Hyper-Threading)	2
CPU speed	1.8 GHz
Hardware virtualization	Enabled
Disk space	120 GB

Table 4-4 System requirements for the ESX/ESXi host *(continued)*

Requirement	Minimum for production environment
Memory	The memory requirement is based on your network configuration mode, as follows: ■ Port span/tap mode: 4 GB ■ Inline mode: 4 GB ■ Proxy mode: 8 GB ■ Inline + proxy mode: 8 GB ■ CIU mode: 4 GB
Physical NICs	The NIC requirement is based on your network configuration mode, as follows: ■ Port span/tab mode: 2 ■ Inline mode: 3 ■ Proxy mode: 2 ■ Inline + proxy mode: 3 ■ CIU mode: 1

Refer to your VMware documentation for VMware system requirements.

About adding the VMware LAN Network virtual switches

You must create VMware LAN Network virtual switches for each Symantec Web Gateway network port that you intend to use based on your deployment option. After you create the switch, you can configure the certain properties. Create the LAN Network virtual switch on your ESX/ESXi system to connect to your network based on the Symantec Web Gateway network configuration guidelines.

See "Port connections for typical network configurations" on page 27.

If you want to build the LAN Network virtual switch to map to the Symantec Web Gateway interface, create a virtual switch and select the appropriate ESX/ESXi interface for your device.

Figure 4-1 Suggested Network virtual switch configuration

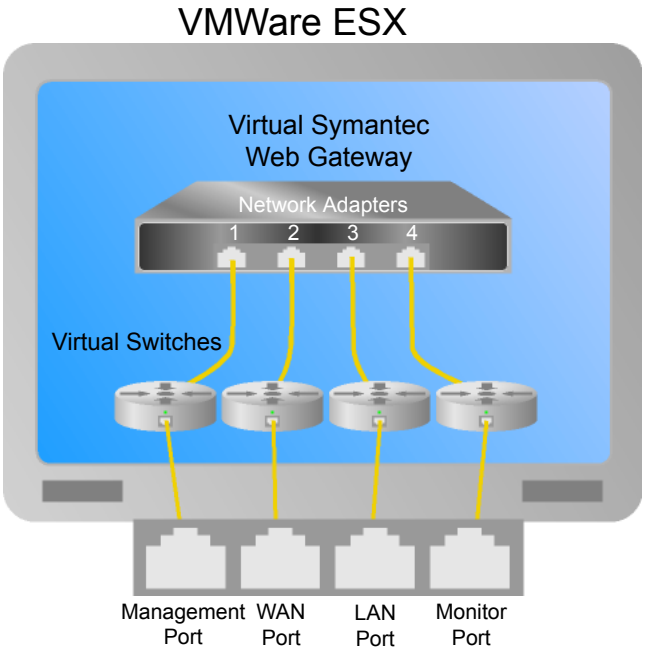


Table 4-5 describes the values that you should use in vSphere when you create a LAN Network virtual switch.

Table 4-5 VMware LAN Network virtual switch property values

Property	Value
Connection Type	**Virtual Machine**
VLAN ID	Leave as is
Promiscuous Mode	**Accept**
Failback	**No**
Notify Switches	**No**

For any property that Table 4-5, does not specify, use any value.

For more information about how to add a VMware LAN Network virtual switch and configure port property settings, refer to your vSphere documentation.

After you configure the VMware LAN virtual switch, map the virtual switches to your network the same as you would for a non-virtual installation.

See "Port connections for typical network configurations" on page 27.

About configuring the VMware virtual switch

ESX/ESXi installations automatically create a default virtual switch, which is called the VM Network. You must configure the VM Network virtual switch network properties for Symantec Web Gateway Virtual Edition to function properly.

Table 4-6 describes how you should configure the VM Network port properties in vSphere.

Table 4-6 VM Network virtual switch property values

Property	Value
Connection Type	**Virtual Machine**
VLAN ID	Leave as is
Promiscuous Mode	**Accept**
Failback	**No**
Notify Switches	**No**

For any property that Table 4-6 does not specify, use the default value.

For more information about how to configure port properties, refer to your vSphere documentation.

After you configure the VMware virtual switch, map the virtual switches to your network the same as you would for a non-virtual installation.

See "Port connections for typical network configurations" on page 27.

Chapter 5

Configuring the Symantec Web Gateway proxy

This chapter includes the following topics:

- About the Symantec Web Gateway proxy
- Available features when the Symantec Web Gateway proxy is enabled
- Required Web browser settings for the Symantec Web Gateway proxy
- Configuring the Symantec Web Gateway HTTP proxy and HTTPS proxy
- How SSL Deep Inspection differs from SSL Domain Level Inspection
- Configuring the Symantec Web Gateway proxy for SSL Deep Inspection
- Configuring the Symantec Web Gateway proxy for SSL Domain Level Inspection
- Specifying a Symantec Data Loss Prevention server
- Configuring the Symantec Web Gateway SOCKS proxy
- Configuring the Symantec Web Gateway FTP proxy

About the Symantec Web Gateway proxy

Symantec Web Gateway has an integrated proxy. The Symantec Web Gateway proxy can perform as a traditional FTP, HTTP, and SOCKS proxy. The Symantec Web Gateway proxy can also decrypt SSL-encrypted network traffic for URL content filtering, blacklisted-domain matching, and malware. The Symantec Web Gateway proxy lets you route network traffic through a Symantec Data Loss Prevention server. SSL-encrypted network traffic can also be routed to and

inspected by Symantec Data Loss Prevention. You must enable the Symantec Web Gateway proxy to use some features.

See "Available features when the Symantec Web Gateway proxy is enabled" on page 78.

Configure your firewall to allow the traffic to and from the Symantec Web Gateway proxy ports. Web browsers at your site must be configured to work with the Symantec Web Gateway proxy.

See "Required Web browser settings for the Symantec Web Gateway proxy" on page 80.

Symantec Web Gateway is designed to load balance your proxy traffic across multiple HTTP/S proxy ports within one proxy server. The default number of proxy ports is one. However, you can change the port configuration to the port(s) that you use.

See "Sample proxy auto-configuration (PAC) file" on page 211.

Symantec Web Gateway can also integrate with a separate software or hardware proxy on your network.

Available features when the Symantec Web Gateway proxy is enabled

Symantec Web Gateway can perform some tasks without the Symantec Web Gateway proxy. You can block and monitor Web sites, detect malware, and use whitelists and blacklists.

Table 5-1 describes some features that require you to enable the proxy.

Table 5-1 Features for which the Symantec Web Gateway proxy is required

Feature	Description
HTTP, HTTPS, SOCKS, or FTP proxy	To use the Symantec Web Gateway proxy as a proxy for HTTP, HTTPS, SOCKS, or FTP, you must enable it. See "Configuring the Symantec Web Gateway HTTP proxy and HTTPS proxy" on page 81. See "Configuring the Symantec Web Gateway SOCKS proxy" on page 89. See "Configuring the Symantec Web Gateway FTP proxy" on page 89.

Table 5-1 Features for which the Symantec Web Gateway proxy is required *(continued)*

Feature	Description
SSL Deep Inspection	You must enable SSL Deep Inspection to monitor the network traffic that is encrypted with SSL. See "Configuring the Symantec Web Gateway proxy for SSL Deep Inspection" on page 85. See "How SSL Deep Inspection differs from SSL Domain Level Inspection" on page 82.
SSL Domain Level Inspection	Use the proxy to monitor and block the Web sites that are encrypted with SSL by domain (for example, https://foo.com) or IP address (for example, https://192.168.1.10). But it cannot report or inspect full URLs. Nor can it report or inspect file transfers, malware, or any data in the stream, such as the keywords it forwards to Symantec Web Prevent. See "Configuring the Symantec Web Gateway proxy for SSL Domain Level Inspection" on page 87. See "How SSL Deep Inspection differs from SSL Domain Level Inspection" on page 82.
Integration with Symantec Data Loss Prevention	Symantec Web Gateway integrates with Symantec Data Loss Prevention Network Prevent for Web to monitor outgoing Web traffic. Symantec Data Loss Prevention Network Prevent is a component of Symantec Data Loss Prevention. This Symantec product discovers, monitors, and protects confidential data wherever it is stored or used. With Symantec Data Loss Prevention, you can create the policies that extend across endpoint, network, and storage systems. See "Specifying a Symantec Data Loss Prevention server" on page 87.

Table 5-1 Features for which the Symantec Web Gateway proxy is required *(continued)*

Feature	Description
Proxy authentication using 407 NTLM authentication	Some forms of NTLM authentication require the proxy. 407 NTLM authentication is only available when you enable the Symantec Web Gateway HTTP/HTTPS proxy. SSL and SOCKS do not support 407 NTLM. See "Web browser changes needed for NTLM" on page 205.

Required Web browser settings for the Symantec Web Gateway proxy

The Web browsers at your site must be configured to work with the Symantec Web Gateway proxy.

Table 5-2 provides an overview of the Web browser settings that are required.

Table 5-2 Web browser settings for the Symantec Web Gateway proxy

Component	Configuration requirement
Proxy settings in Web browsers	You must configure Web browsers to access the Internet through the Symantec Web Gateway proxy. You can configure each Web browser separately or use automation. Automation methods include the following: ■ WPAD and PAC In this method, Web browsers automatically detect the required proxy settings from a central PAC file. See "Sample proxy auto-configuration (PAC) file" on page 211. ■ Group policy in Active Directory If you use Active Directory, you can propagate proxy settings to Web browsers with group policies.

Table 5-2 Web browser settings for the Symantec Web Gateway proxy *(continued)*

Component	Configuration requirement
Certificate store in Web browsers (for SSL Deep Inspection only)	You must import either the Symantec Web Gateway certificate or your own certificate into every Web browser on your network. You can manually import the certificate into each Web browser separately or use automation. Automation methods include the following: ■ Group policy in Active Directory If you have Active Directory configured at your site, you can import the certificate into Web browsers using group policies. ■ Domain login script In Microsoft Windows environments, you can configure a login script to run after users log on.

Configuring the Symantec Web Gateway HTTP proxy and HTTPS proxy

Symantec Web Gateway has a proxy that you can enable for HTTP and HTTPS network traffic. The HTTP/HTTPS proxy supports HTTP version 1.0 and version 1.1.

For the HTTP cache, Symantec Web Gateway honors the cache-related code in downloaded HTTP files.

To configure the Symantec Web Gateway HTTP proxy and the HTTPS proxy

1. In the Web GUI, click **Administration > Configuration > Proxy**.
2. Under **HTTP Settings**, check **Enable HTTP/S Proxy**.
3. For **HTTP/S Proxy Port(s)**, type one or more ports.

   The proxy listens for HTTP traffic from user Web browsers at the ports that you specify. You can type individual ports or a range of ports. Separate a range of ports with a dash. Use commas to separate ports. You can configure a maximum of 16 ports.

   The default port is 8080.

4 Type a number for the **Keep Alive Timeout**.

The **Keep Alive Timeout** is how long the proxy keeps a network connection open after the last transmission. The maximum is 1800 seconds (30 minutes).

The default is 120 seconds.

5 Type a number for the **Maximum Cache Object Size**.

Files over the number that you specify are not retained in the cache on Symantec Web Gateway.

The default value and the maximum value are 256 KB.

6 Check or uncheck **Byte Range Support**.

The byte range support determines whether partial requests for data are served from the cache or fetched from the Internet.

Byte Range Support checked	HTTP and HTTPS requests under 14 KB are served from the cache. If the requested files are not already cached, the data is fetched, cached, and passed along. Requests that are over 14 KB in size bypass the cache and are served from the Internet.
Byte Range Support unchecked	Partial responses are fetched and passed along but not cached.

The default is checked. The 14 KB byte range cannot be changed.

7 If you want, click **Add a Cache Exception** to add a domain that you do not want cached.

Data is not cached for the domains that are listed under **Cache Exception Domain**. You may want to exclude the Web sites that mainly stream content. In some cases, you may want to exclude internal Web servers.

The maximum number of cache domain exceptions is 30.

8 Click **Save**.

How SSL Deep Inspection differs from SSL Domain Level Inspection

Table 5-3 describes how SSL Domain Level Inspection differs from SSL Deep Inspection.

Table 5-3 Differences between SSL Domain Level Inspection and SSL Deep Inspection

SSL Domain Level Inspection	SSL Deep Inspection
Symantec Web Gateway reports the access of and blocks Web sites by domain (for example, https://foo.com) or IP address. But it cannot report or inspect full URLs. Nor can it report or inspect file transfers, malware, or any data in the stream such as the content it forwards to Symantec Web Prevent (Symantec DLP server). SSL Domain Level Inspection occurs when you do either of the following: ■ Send HTTPS traffic to the Symantec Web Gateway HTTP/S proxy. ■ Send HTTPS traffic to the SSL Deep Inspection Proxy and have no policy that intercepts the HTTPS traffic. **Note:** The custom blacklist is not supported over HTTPS. See "Configuring the Symantec Web Gateway proxy for SSL Domain Level Inspection" on page 87.	Symantec Web Gateway reports the access of and blocks Web sites by domain, and it can inspect all of the traffic in the traffic stream. This inspection includes full URLs and file inspections. It also includes the content that it forwards to Symantec Web Prevent. Only the SSL Deep Inspection proxy can intercept HTTPS traffic and decrypt the traffic to read the contents. Symantec Web Gateway disables the ability to intercept HTTPS traffic by default. But you can enable it through the use of policies. See "Configuring the Symantec Web Gateway proxy for SSL Deep Inspection" on page 85. See "Configuring policies for SSL Deep Inspection" on page 107.

You can enable the HTTP/S proxy and the SSL Deep Inspection proxy at the same time. Based on your configuration, you can route HTTPS traffic from the network to either or both proxies. You can configure each individual computer on the corporate network to send HTTPS traffic to Symantec Web Gateway HTTP/S proxy or to the SSL Deep Inspection proxy. You can configure some computers to send traffic through one proxy while other computers send traffic to the other.

The following is a simple use case scenario:

IT administrator sets up the Symantec Web Gateway proxy to protect Group A and Group B. Group B requires a higher level of security. So the administrator wants to ensure that Symantec Web Gateway decrypts and inspects all of the contents of this traffic. But the administrator does not want to decrypt or inspect Group A's or Group B's financial transactions for privacy purposes and legal purposes. So the administrator creates an SSL policy that intercepts all HTTPS traffic except for the traffic that goes to financial institutions.

The administrator creates corporate policies with a PAC file or other configuration settings to ensure that:

- Group A and Group B HTTP traffic goes to the Symantec Web Gateway HTTP/S proxy.
- Group A HTTPS traffic goes to the Symantec Web Gateway HTTP/S proxy. In this scenario, SSL Domain Level Inspection occurs.
- Group B HTTPS traffic goes to the SSL Deep Inspection proxy. Per the policy, SSL Deep Inspection occurs except for the HTTPS traffic to financial institutions.

Table 5-4 describes what occurs when users in each group attempt to access certain Web sites.

Table 5-4 Use case scenarios

Scenario	Result
A user from Group A or Group B goes to http://blacklisted_domain.com	■ Symantec Web Gateway blocks this traffic. ■ Symantec Web Gateway reports that this user was blocked from going to http://blacklisted_domain.com.
A user from Group A or Group B goes to https://blacklisted_domain.com	■ Symantec Web Gateway blocks this traffic. ■ Symantec Web Gateway reports that this user was blocked from going to https://blacklisted_domain.com.
A user from Group A or Group B tries to download a virus from http://site_with_virus.com/virus_file.exe	■ Symantec Web Gateway inspects the file and blocks the virus download. ■ Symantec Web Gateway reports that the virus was blocked from being downloaded from http://site_with_virus.com/virus_file.exe.
A user from Group A tries to download a virus from https://site_with_virus.com/virus_file.exe	■ Symantec Web Gateway does not block the virus. ■ Symantec Web Gateway reports that the user went to https://site_with_virus.com/.
A user from Group B tries to download a virus from https://site_with_virus.com/virus_file.exe	■ Symantec Web Gateway inspects and downloads the file. ■ However, Symantec Web Gateway corrupts the contents of the file to disable the virus.

Table 5-4 Use case scenarios *(continued)*

Scenario	Result
A user from Group A tries to download a financial statement text file from https://my_bank.com/monthly_statement.txt	■ Symantec Web Gateway reports that the user went to https://my_bank.com/. ■ Symantec Web Gateway does not inspect the file.
A user from Group B tries to download a financial statement text file from https://my_bank.com/monthly_statement.txt	■ Symantec Web Gateway reports that the user went to https://my_bank.com. ■ Symantec Web Gateway does not inspect the file.

Configuring the Symantec Web Gateway proxy for SSL Deep Inspection

Symantec Web Gateway has a proxy that you can enable to inspect the contents of SSL-encrypted network traffic. Symantec Web Gateway can check SSL-encrypted network traffic for URL content filtering, blacklisted-domain matching, and malware. Symantec Web Gateway can also route SSL-encrypted network traffic to Symantec Data Loss Prevention for inspection.

See "How SSL Deep Inspection differs from SSL Domain Level Inspection" on page 82.

SSL Deep Inspection for computers in your network is not automatically enabled after you configure the proxy. To use SSL Deep Inspection, you must create one or more policies that employ SSL Deep Inspection.

Note: SSL Deep Inspection does not support custom blacklists.

See "Configuring policies for SSL Deep Inspection" on page 107.

To configure the proxy for SSL deep inspection

1. In the Web GUI, click **Administration > Configuration > Proxy**.
2. Under **SSL Deep Inspection Settings**, check **Enable SSL Deep Inspection**.
3. For **SSL Port**, type a port.

   The Symantec Web Gateway proxy listens for SSL traffic at the port that you specify. If you have enabled the internal HTTP/S proxy, the SSL port must be different than the HTTP/S ports and cannot be 8080-8083. The default port is 8443.

4 Type a number for **Maximum SSL Connections**.

If the number of SSL connections that Symantec Web Gateway monitors exceeds this number, new connections are blocked until existing connections are closed.

The default is 10240 connections.

5 Select a certificate type beside **SSL Certificate**.

Use Default Certificate	Use the default certificate that is included in Symantec Web Gateway.
Use Imported Certificate	Use your own certificate. You must specify the certificate and key. The certificate and key must be in DER format or PEM format containing US-ASCII or UTF characters only. The way that you import SSL certificates in Internet Explorer 9 differs from Internet Explorer 8/7. For Internet Explorer 9, select the option to **Place all certificates in the following store** to import the certificate into Trusted Root Certification Authorities. For Internet Explorer 8/7, select the option **Automatically select the certificate store based on the type of certificate** to import the certificate to the intermediate Certification Authorities. For more information, see your Internet Explorer documentation.

6 Click **Export SSL Certificate** and save the default certificate.

You must import this exported certificate into user Web browsers if you choose the option **Use Default Certificate**.

See "Required Web browser settings for the Symantec Web Gateway proxy" on page 80.

7 Click **Save**.

Configuring the Symantec Web Gateway proxy for SSL Domain Level Inspection

Symantec Web Gateway reports and blocks Web sites by domain (for example, https://foo.com) or IP address (for example, https://192.168.1.10). But it cannot report or inspect full URLs. Nor can it report or inspect file transfers, malware, or any data in the stream, such as the content it forwards to Symantec Web Prevent.

See "How SSL Deep Inspection differs from SSL Domain Level Inspection" on page 82.

To configure the Symantec Web Gateway proxy for SSL Domain Level Inspection

- Do either of the following tasks:
  - Send HTTPS traffic to the Symantec Web Gateway HTTP/S proxy.
    See "Configuring the Symantec Web Gateway HTTP proxy and HTTPS proxy" on page 81.
  - Send HTTPS traffic to the SSL Deep Inspection Proxy and have no policy that intercepts the HTTPS traffic.
    See "Configuring the Symantec Web Gateway proxy for SSL Deep Inspection" on page 85.
    See "Configuring policies for SSL Deep Inspection" on page 107.

Specifying a Symantec Data Loss Prevention server

If you use the Symantec Web Gateway proxy, you can route outbound HTTP traffic and HTTPS traffic through a Symantec Data Loss Prevention (DLP) server. The Symantec DLP server discovers, monitors, and protects confidential data.

The connection to Symantec DLP is fail open. If there is a communication problem between Symantec Web Gateway and Symantec DLP, network traffic bypasses Symantec DLP without inspection.

Note: When you configure the Symantec DLP server, carefully consider the value that you specify on the **Configure Server** page under **Request Filtering** for the option **Ignore Requests Smaller Than**. If you set the value too high, Symantec Web Gateway may ignore potentially important files. Symantec Web Gateway still sends the request, but the DLP server does not inspect it.

For more information, see your Symantec Data Loss Prevention server documentation.

You must check **Enable HTTP/S Proxy** or **SSL Deep Inspection** for the **Enable DLP** option to appear.

See "Configuring the Symantec Web Gateway proxy for SSL Deep Inspection" on page 85.

See "Configuring the Symantec Web Gateway proxy for SSL Domain Level Inspection" on page 87.

To specify a Symantec Data Loss Prevention server

1. Configure the HTTP settings of the Symantec Web Gateway proxy.

   See "Configuring the Symantec Web Gateway HTTP proxy and HTTPS proxy" on page 81.

2. In the Web GUI, on the **Administration > Configuration > Proxy** tab, under **Symantec DLP Network Prevent Settings**, click **Enable DLP**.
3. In the **DLP Session Timeout** box, type the number of seconds that the Symantec DLP server session remains idle. After this timeout period, Symantec Web Gateway disconnects the session. Symantec Web Gateway re-establishes the connection when another request is made.

   You may need a shorter timeout if Internet traffic at your site is high. You may need a longer timeout if Internet traffic at your site is low. Please test changes before you deploy them in a production environment.
4. Click **Add a DLP Server** to add a Symantec DLP server.
5. In the **DLP Server IP Address** box, type the address of the Symantec DLP server.
6. In the **DLP Port** box, type the port number of the Symantec DLP server.

   The Symantec DLP server communicates with the Symantec Web Gateway proxy over the ICAP protocol. The default value of ICAP protocol port is 1344, but you can change this value.
7. Repeat 4 through 6 to add additional Symantec DLP servers.

   The maximum number of Symantec DLP servers that you can use is as follows:

If you enable SSL Deep Inspection	16
If you enable SSL Domain Level Inspection	4

8. Click **Save**.

Configuring the Symantec Web Gateway SOCKS proxy

Symantec Web Gateway has a proxy that you can enable as a SOCKS proxy for TCP and UDP network traffic such as HTTP and FTP. Symantec Web Gateway supports SOCKS version 5.

To configure the Symantec Web Gateway SOCKS proxy

1. In the Web GUI, click **Administration > Configuration > Proxy**.
2. Under **SOCKS Settings**, check **Enable SOCKS Proxy**.
3. For **SOCKS Port**, type the port number.

   The Symantec Web Gateway proxy listens for network traffic at the port that you specify.

   The default port is 1080.
4. Type a number for the **SOCKS Session Timeout**.

   The **SOCKS Session Timeout** is how long the Symantec Web Gateway proxy keeps a network connection open after the last transmission. You may need a shorter timeout if Internet traffic at your site is high. You may need a longer timeout if Internet traffic at your site is low. Test changes before you deploy them in a production environment.

   The default is 120 seconds.
5. Click **Save**.

Configuring the Symantec Web Gateway FTP proxy

Symantec Web Gateway has a proxy that you can enable for FTP network traffic.

To configure the Symantec Web Gateway FTP proxy

1. In the Web GUI, click **Administration > Configuration > Proxy**.
2. Under **FTP Settings**, check **Enable FTP Proxy**.
3. For **FTP Proxy Port**, type a port.

   The proxy listens for FTP traffic at the port that you specify.

   The default port is 8021.
4. Check or uncheck **Allow PASV Mode to FTP Server**.

   In PASV mode, the FTP server negotiates a communication session using an alternate port after it establishes a session on the default port.

   The default is checked.

5 Type a number for the **FTP Session Timeout**.

The **FTP Session Timeout** is how long the proxy keeps an FTP network connection open after the last transmission. You may need a shorter timeout if Internet traffic at your site is high. You may need a longer timeout if Internet traffic at your site is low. Please test changes before deploying them in a production environment.

The default is 300 seconds.

6 Click **Save**.

Chapter 6

Configuring policies

This chapter includes the following topics:

- About policies
- Configuring the policy precedence order
- Download behavior in user Web browsers
- Internet applications, malware, and URL filtering blocking behavior
- Specifying computers or users for policies
- About Insight reputation-based security
- Configuring policies for SSL Deep Inspection
- Configuring policies for malware
- Configuring policies for Internet applications
- Malware categories for policies
- Configuring URL filtering policies for Web sites
- Configuring embedded URL detection
- Allowing after hours access to Web sites
- Quarantining infected computers
- Configuring NTLM user authentication behavior
- Blocking or monitoring Web sites using the blacklist
- Blocking or monitoring file transfers using the blacklist
- Allowing Web site access using the whitelist

- About the Blocking Feedback report
- About end user pages

About policies

You can create policies to control the content that flows in and out of your Web gateway. 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 were expected. Also, you should test that the desired action occurs by accessing the Symantec Web Gateway test page from a computer in each policy workgroup.

See "Testing Symantec Web Gateway for successful blocking or monitoring" on page 64.

Note: You must install Symantec Web Gateway in the inline, proxy, or inline plus proxy network configuration to block file transfers. 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 Symantec Web Gateway network configurations" on page 24.

Table 6-1 describes the types of actions that you can configure a policy.

Table 6-1 Policy actions

Action	Description
Decrypt SSL-encrypted network traffic.	Check SSL-encrypted network traffic for malware detection and URL filtering. SSL-encrypted network traffic can also be routed to and inspected by Symantec Data Loss Prevention. See "Configuring policies for SSL Deep Inspection" on page 107.

Table 6-1 Policy actions *(continued)*

Action	Description
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, subnets, and services because Active Directory information is not available before authentication. See "Configuring NTLM user authentication behavior" on page 142.
Quarantine infected computers.	Prevent malware-infected computers from accessing the Internet. See "Quarantining infected computers" on page 141.
Block, monitor, or ignore malware by category, severity, or detection type.	Block, monitor, or ignore certain categories of malware. Generally you should block all malware for all users. If necessary, you can configure exceptions for certain categories of malware for certain computers. See "Configuring policies for malware" on page 108.
Allow, block, monitor, or ignore downloads based on Insight reputation-based security.	Allow, block, monitor, or ignore downloads using Insight, a Symantec technology that can flag probable malware not previously known to Symantec. See "Configuring policies for Insight reputation-based security" on page 106.
Block or allow select Internet applications and spyware.	Block, monitor, or allow access to individual Internet applications or categories of Internet applications. See "Configuring policies for Internet applications" on page 111.

Table 6-1 Policy actions *(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 140.
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. Both features also require that the content filter module is licensed and enabled. See "Configuring URL filtering policies for Web sites" on page 118.
Block specific Web sites or downloads.	Use the blacklist to block access to specific Web sites or downloads. See "Blocking or monitoring Web sites using the blacklist" on page 143. See "Blocking or monitoring file transfers using the blacklist" on page 145.
Allow specific Web sites or downloads.	Use the whitelist to allow access to a specific Web site or download. See "Allowing Web site access using the whitelist" on page 146.
Enforce application control.	Symantec Web Gateway can allow, block, or monitor Internet access for applications with the application control policy settings. See "Configuring policies for Internet applications" on page 111.

Configuring the policy precedence order

Policies are evaluated in the order that they appear on the **Policies > Configuration** page. Symantec Web Gateway evaluates the policy at the top of the page 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 workgroups of different network types. If you consistently use subnet, IP range, or VLAN ID to define all of your workgroups , new policies are inserted in the correct order. If you use workgroups of different network types in your policies, ensure that the policies are ordered as you want. Precedence is also necessary in the case of conflicting or overlapping policies of the same network type.

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 up the policy or move down a policy.
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** option is not available for the port span/tap network configuration.

See "About Symantec Web Gateway network configurations" on page 24.

For both the **Block** or **Monitor** actions, if the download might take 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 that is used on this page and the image that appears.

Note: You may experience unexpected behavior on non-supported Web browsers.

See "End user pages for blocked Web sites, file transfers, and infections" on page 149.

Table 6-2 describes the download behavior for each action.

Table 6-2 Download behavior in user Web browsers

Action	Inline, proxy, or inline and proxy 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 149.
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.
Use default action for Insight	Available	Not available	The action that is set for the default Insight policy is available on the **Administration > Configuration > Insight** page.

See "About Insight reputation-based security" on page 103.

Internet applications, malware, and URL filtering blocking behavior

You can configure blocking in the following types of policies:

Application control policy	Allow, block, or monitor Internet access for applications with the application control policy settings. See "Configuring policies for Internet applications" on page 111.
Malware policy	Block malware, which includes spyware, viruses, worms, Trojan horses, botnets, keyloggers, and so on. See "Configuring policies for malware" on page 108.
URL filtering policy	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 118. See "Preinstallation checklist" on page 19.
Blacklist	Block file downloads by file extension using the blacklist. See "Blocking or monitoring file transfers using the blacklist" on page 145.

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

Table 6-3 describes these blocking methods.

Table 6-3 Blocking methods

Blocking method	Description	Examples
End user blocking page	For downloads and the 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 also enters text into the binary to identify it blocked the file. The default text is as follows: Malware has been detected by Symantec Web Gateway.	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 Symantec Web Gateway network configurations" on page 24.

Table 6-4 describes the blocking behavior for each type of policy.

Table 6-4 Blocking behavior for policies

Policy	Application	Application action	Browser patience page	Blocking method	Supported network configurations
Antivirus scan from malware policy	Web browsers	Download .exe, .zip, .rar, .dll, and .cab files that are over 50,000 bytes	Yes	End user blocking page	Inline, proxy, and inline plus proxy
Antivirus scan from malware policy	Web browsers	Download file	No	End user blocking page	Inline, proxy, and inline plus proxy
Blacklist block by file extension	Web browsers	Download file	No	Interrupt connection only for port span/tap	Inline, proxy, inline plus proxy, and port span/tap
Antivirus scan from malware policy	Web browsers	Upload file	No	Corrupts the file	Inline, proxy, and inline plus proxy
Blacklist block by file extension	Web browsers	Upload file	No	Interrupt connection	Inline, proxy, inline plus proxy, and port span/tap
Malware or URL filtering	Web browsers	Browse to URL	No	End user blocking page	Inline, proxy, inline plus proxy, and port span/tap
Antivirus scan from malware policy	FTP	Upload file or download file	No	Corrupts the file FTP command line (inline mode only) error message: 226 Spyware Blkd	Inline, proxy, and inline plus proxy
Malware	Malware phone home	Any network activity	No	Interrupts connection	Inline, proxy, inline plus proxy, and port span/tap

Table 6-4 Blocking behavior for policies *(continued)*

Policy	Application	Application action	Browser patience page	Blocking method	Supported network configurations
Application control	Applications available for application control	Any network activity	No	Interrupts connection	Inline, proxy, inline plus proxy, and port span/tap Some limitations for port span/tap as noted in Web GUI
Application control	IM applications	Upload file or download file	No	Interrupts connection	Inline and port span/tap Some limitations for port span/tap as noted in Web GUI
Antivirus scan from malware policy	IM applications	Upload file or download file	No	Corrupts the file	Inline, proxy, and inline plus proxy
Antivirus scan from malware policy	Applications that access the Internet, such as for software updates	Download file	No	Corrupts the file	Inline, proxy, and inline plus proxy
Antivirus scan from malware policy	Unknown Web browser applications	Download file	No	Corrupts the file	Inline, proxy, and inline plus proxy
Antivirus scan from malware through SSL Deep Inspection	Web browsers	Download .exe,.zip, .rar, .dll, and .cab files that are over 50,000 bytes	No	Corrupts the file	Inline + Proxy, Proxy

See "About policies" on page 92.

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, and so on.

If you attempt to configure a policy that includes an Active Directory user or workgroup, Symantec Web Gateway may display an error. This error occurs if the user or workgroup does not exist in your Active Directory. The problem is most likely a typo in the policy. The name or workgroup does not match the user name or workgroup in Active Directory.

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 (Optional)	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 149.

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 189.

The options that you can configure are as follows:

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. A drop-down list appears if there are 100 or fewer discovered entities. For example, if a large enterprise has over 100 departments, a text box appears, and the administrator must type the department name.
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 92.

About Insight reputation-based security

Symantec Web Gateway can block, monitor, ignore, or allow access to files and other sources of malware based on file's reputation. Insight is a Symantec technology that can flag probable malware not previously known to Symantec. Symantec gathers anonymous computer usage behavior from participating Symantec customers and malware based on file reputation. Symantec combines the aggregate usage behavior with other attributes, such as the file publisher and file uniqueness, to make a reputation score for a file. You can configure the policies that allow only content with a reputation score of safe. Or you can also block content with a reputation score of unsafe. You can also monitor Internet traffic and view the content reputation for monitored files in a report.

To employ Insight, you must enable it. Symantec Web Gateway processes Insight reputation-based security after antivirus scanning.

Insight only supports Microsoft Portable Executable (PE) files. PE files include, but are not limited to: .exe, .dll, .sys, .cpl, .ocx, .scr, .drv, and .tlb.

See "Enabling Insight reputation-based security" on page 104.

See "Configuring policies for Insight reputation-based security" on page 106.

Enabling Insight reputation-based security

To employ Insight reputation-based security, you must first enable it. After you enable it, you can configure a policy that uses it.

See "About Insight reputation-based security" on page 103.

See "Configuring policies for Insight reputation-based security" on page 106.

To enable Insight reputation-based security

1. In the Web GUI, click **Administration > Configuration > Insight**.
2. Click **Enable Insight Policies**.
3. Click the **Safe Content Confidence Setting** drop-down list and select an option.

   The **Safe Content Confidence Setting** is the level of confidence that Symantec has that a file is safe. You can create a policy to allow users to only download files considered safe.

   The options that you can select are as follows:

Norton Trusted	Norton believes that these files are trustworthy. This is the highest level of trust.
Good (Recommended)	There are indications that these files are trustworthy. This is the recommended setting for most environments.

4 Click the **Unsafe Content Confidence Setting** drop-down list and select an option.

The **Unsafe Content Confidence Setting** is the level of confidence that Symantec has that a file is unsafe. You can create a policy to block users from downloading files considered unsafe.

The options that you can select are as follows:

Poor (Recommended)	There are some indications that these files are not trustworthy. This is the recommended setting.
Not Trusted	There are many indications that these files are not trustworthy. This is the lowest level of trust.

5 Click the **Default Insight Policy** drop-down list and select a default policy.

The policy that you select appears as the default action on the **Policies > Configuration** page under **Action** and beside **Insight**. You can still change the action as you create policies. By default, the action is **Block unsafe files**, which is the recommended setting. When you select a default policy on this page, Symantec Web Gateway uses this policy for PE file downloads. You can set Insight policies by specifying a policy action for Insight in the custom policy.

See "Configuring policies for Insight reputation-based security" on page 106.

If you do not create a specific policy, the Symantec Web Gateway default policy is based on the setting on this page. The **Use Default** action in policies inherits its setting from here.

This option is not available for the port span/tap network configuration.

6 Optionally, to add a file exception, do all of the following tasks:

- Click **Add a File Exception**.
- Under **Filename**, either type the file name or click **Browse** to locate the file.
  Symantec Web Gateway does not support compressed files for reputation-based filtering file exceptions. It only supports Microsoft PE executable files.
  The maximum file size that you can upload is 16 MB.

- Click the **File Action** drop-down list to specify the action that you want Symantec Web Gateway to take for the exception file.

7 Click **Save**.

Configuring policies for Insight reputation-based security

To employ Insight, you must enable it. After you enable it, you can configure a policy that uses it.

See "About Insight reputation-based security" on page 103.

See "Enabling Insight reputation-based security" on page 104.

Note: Insight is not enabled for all computers by default. To enable Insight for all computers, configure a policy for all computers and set the **Insight** action to **Use Default**, **Allow Only Safe Content**, **Block Unsafe Content**, **Monitor All Content**, or **Ignore Reputation**.

Note: You must install Symantec Web Gateway in your network in the inline, proxy, and inline + proxy network configuration to block file transfers. If you configure Symantec Web Gateway in the port span/tap network configuration, the block action (**Allow Only Safe Content** and **Block Unsafe Content**) is not available in the Web GUI.

See "About Symantec Web Gateway network configurations" on page 24.

To configure policies for Insight reputation-based security

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

See "Specifying computers or users for policies" on page 101.

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

3 Under **Action**, select one of the following options:

Allow Only Safe Content	Allow content based on the **Safe Content Confidence Setting** on the **Reputation** configuration page. Any content that is not considered safe is blocked.
Block Unsafe Content	Block content based on the **Unsafe Content Confidence Setting** on the **Reputation** configuration page. Any content that is not considered unsafe is allowed.
Monitor All Content	Do not block anything based on Insight. Instead, record the activity that is related to reputation for reports.
Ignore Insight	Disable Insight for the current policy and do not record the activity that is related to reputation.
Use Default	Allows the policy to use the default action that is specified in **Administration > Configuration > Insight**. See "Enabling Insight reputation-based security" on page 104.

4 Configure other policy settings as desired.

5 Click **Save**.

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

Configuring policies for SSL Deep Inspection

To employ SSL Deep Inspection, you must enable it and you must be running an SSL proxy. After you enable SSL Deep Inspection, configure a policy that specifies the range of computers and URL categories to which SSL Deep Inspection applies. You must enable the content filter module to enable SSL Deep Inspection by URL category.

See "Configuring the Symantec Web Gateway proxy for SSL Deep Inspection" on page 85.

See "Enabling URL filtering, Internet program monitoring, and other features" on page 60.

To configure policies for SSL Deep Inspection

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

   See "Specifying computers or users for policies" on page 101.

2. Continuing on the **Policies > Configuration** page, locate **SSL Deep Inspection**.
3. Click **SSL Deep Inspection policy**.
4. If the content filter module is enabled, configure the **Content Filter Categories**.

Intercept	For the computers in this category, inspect SSL-encrypted network traffic for the URL category.
Ignore	For the computers in this category, ignore SSL-encrypted network traffic for the URL category. Do not record the activity that is related to SSL Deep Inspection for reports.

   If the content filter module is not enabled, the **Content Filter Categories** and **SSL Intercept Exceptions** are not displayed. Choose a default action for SSL encrypted traffic.

5. Under **SSL Intercept Exceptions** you can optionally add domain names or IP addresses for which you want to intercept or ignore SSL traffic.
6. Click **Save**.
7. On the **Policies > Configuration** main page, click **Save and Activate Changes**.

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 "Internet applications, malware, and URL filtering blocking behavior" on page 97.

Note: If the operating mode is set to block, malware is blocked by default. Otherwise, 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 or proxy 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 Symantec Web Gateway network configurations" on page 24.

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 101.

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 95.

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 a computer on your network or to send a malicious network element such as a network worm.
Malware URL	A user has attempted to access a known malware Web site.

8 Configure other policy settings as desired.

See "Malware categories for policies" on page 113.

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.

All application control settings are available for inline and inline plus proxy mode. However, there are some limitations for proxy only and port tap/span operating modes.

See "About policies" on page 92.

See "Internet applications, malware, and URL filtering blocking behavior" on page 97.

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 60.

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 101.

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** beside the category.

5 Configure other policy settings as desired.

6 Click **Save**.

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

Malware categories for policies

Symantec Web Gateway can block malware and spyware categories as per the configuration settings in the policies.

Table 6-5 describes the malware or spyware categories.

Table 6-5 Malware or spyware categories

Malware or spyware categories	Description
Ad-supported Program	An ad-supported program is any software package that automatically displays or downloads advertisements to a computer. These advertisements can be in the form of a pop-up and the main objective is to generate revenue.
Adware	An adware is a software package that facilitates the delivery of advertising content to the user.
Adware Bundler	Software bundling is a common type of spyware that installs several pieces of software at the same time. An adware bundler installs adware (or several pieces of adware) as part of the installation of another, desired program, and often requires the adware to run for the desired program to function. Many peer-to-peer (P2P) programs are adware bundlers.
Adware Installer	An adware installer runs stealthily on a computer, connects to external servers, downloads adware, installs adware, and updates installed adware programs.
Attack	An attack is an unauthorized attempt by one computer to remotely access another computer. A remote system or an internal system attacks a computer located within the Protected Networks defined within the Symantec Web Gateway user interface.
Backdoor	A backdoor bypasses normal security mechanisms to provide access to a computer (or other illegitimate use). Computer attackers often use backdoors as part of an exploit or Trojan horse to gain access to a user's computer.

Table 6-5 Malware or spyware categories *(continued)*

Malware or spyware categories	Description
Botnet	Symantec Web Gateway detected a host on the network that displays network patterns that are indicative of a botnet infection.
Browser hijacker	A browser hijacker is a malicious program that changes your Web browser settings by usually altering the default start and search pages. A browser hijacker can also modify any aspect of a Web browser such as adding bookmarks, redirecting search traffic to alternative sites.
Browser plug-in	Software that is installed in your Web browser which is designed to enhance the browser's capabilities and expand its functions. Plug-ins can come in the form of toolbars, buttons, or background processes that handle special file formats. Plug-ins may be harmful because they have complete access to your Web browser and can modify, spy and redirect search, and other browsing tasks.
Critical Spyware Web site	A Web site containing malicious files or drive-by infections which directly lead to a critical infection.
Custom Restricted Lists 1, 2, and 3	The recommended use for the custom restricted lists is for you to store related blacklisted Web sites.
Destroyer	The programs crash the computer, either directly by shutting it down, or by destroying essential files.
Dialer	A dialer is a software that dials a phone number using the computer's modem. Most dialers connect to toll numbers without your awareness or permission to incur phone charges. It also includes the Web sites that distribute dialers.
Downloader	A program that is stealthily installed in your computer. After installation, it connects to a remote server and downloads additional programs and files, such as spyware. Spyware is installed in your computer without your knowledge.

Table 6-5 Malware or spyware categories *(continued)*

Malware or spyware categories	Description
Exploit	An exploit is a file that uses the design flaws (vulnerabilities) in software and controls your system. The exploit is used to perform a number of actions such as downloading worms and Trojan horses. Once installed, the exploit malware accesses confidential data or crashes the software, depending on the nature and severity of the vulnerability. An exploits Web site is a Web site that distributes many types of spyware through various exploits in the operating systems and browsers.
Hack tool	Hacking tools are used to gain information or access hosts surreptitiously by using the methods that bypass security mechanisms. The target computer may or may not be disabled. Hacking tools may also facilitate attacks on third-party computers as part of a direct or a distributed denial-of-service attempt.
Joke program	Programs that alter or interrupt the normal behavior of your computer, creating a general distraction or nuisance.
Keylogger	A program that runs in the background and records the user's keystrokes. The logged keystrokes are hidden in the computer for later retrieval or transmitted secretly to the attacker by email or by Internet. Some keyloggers are available for commercial use.
Major Spyware Website	A Web site that contains malicious files or drive-by the infections that may directly lead to a major infection.
Malicious behavior	Malicious behavior describes executable files that display characteristics or behaviors found exclusively within malware. These files are blocked to prevent intrusion, disruption, or damage to computer systems.
Minor Spyware Website	A Web site that contains files and drive-by the infections that directly lead to a minor infection.
Misleading Application	Programs that report false or significantly misleading information on the presence of a security risk, threat, or system issue on the computer being scanned.

Table 6-5 Malware or spyware categories *(continued)*

Malware or spyware categories	Description
P2P	P2P software is an Internet file-sharing application that causes security issues.
Parental control	Parental control programs monitor or restrict Internet access.
Password Hijacker	A password hijacker steals passwords from a user's computer. For example, the hijacker can steal logon IDs and passwords for the installed programs. The hijacker can then send the passwords remotely to the attacker.
Phishing	Phishing is a form of social engineering that is characterized by attempts to fraudulently acquire sensitive information, such as passwords and credit card details. Phishing often takes the form of an email or IM from what appears to be a legitimate business.
Potentially Unwanted Software	Any software which is not determined to belong to any other specific category. It includes software with objectionable distribution, installation, uninstallation procedures, potential privacy risks, and other questionable behaviors that lack proper consent from the user.
RAT	A Remote Administration/Access Tool (RAT) gives an attacker the ability to remotely control a user's computer over the Internet. The victim's computer usually listens on the Internet for the attacker's commands, which can control most functions on the computer. Some RATs are commercially available for legitimate use.
Remote access	Remote access tools provide a means to access PCs and their file systems remotely. The category includes programs such as pcAnywhere, VNC, Cool Remote Control , Telnet, SSH, TN3270, and more.
Rogue Security Program	A program that pretends to be a useful security tool, such as a spyware removal tool. Such security program acts as spyware or fakes security alerts to lure the user to purchase it.
Rootkit	A rootkit is a set of software tools that is designed to be invisible and placed on a computer by a third party. A rootkit is used to conceal running processes, files, or system data.

Table 6-5 Malware or spyware categories *(continued)*

Malware or spyware categories	Description
Security Assessment Tool	Programs intended for legitimate use by administrators to assess network security, but which may be used maliciously to determine weaknesses.
Security risk	A potentially malicious program that does not fit into other categories.
Spammer	A program that can take part in an email flooding campaign.
Spyware	Spyware is any software package that tracks and sends personally identifiable information or confidential information to third parties.
Spyware Marketing and Tools	A Web site that either markets tools to develop a spyware, or attempts to recruit marketing affiliates for spyware.
Stealth Notifier	Also known as a Trojan horse Notifier or a call-home Trojan horse. A stealth notifier connects to a remote server by a stealth connection and notifies the server that the Trojan horse is installed.
Surveillance	Any software that is designed to use a webcam, microphone, screen capture, or other approaches to monitor and capture information. Such software transmits the captured information to a remote source.
System Monitor	Software that monitors system information or provides security tools. Software may be legitimate; however, it is potentially dangerous if used by unauthorized parties.
Tracking Software	Software that monitors user behavior, or gathers information about the user, sometimes including personal information. Most often, the information is sent out to be used for targeted advertising.
Trackware	Trackware is any software package that tracks system activity, gathers system information, or tracks user habits and relays this information to third-party organization.
Trojan	A malicious program that is disguised as legitimate software. Unlike a virus or a worm, Trojan horses do not replicate.
Trojan FTP	An FTP (or telnet) server that is installed on the user's computer by stealth means. An attacker can connect to this server to download files from the user's computer.

Table 6-5 Malware or spyware categories *(continued)*

Malware or spyware categories	Description
Unclassified Critical Spyware	A program that is considered from trusted sources to be a security risk, but it is not fully analyzed to determine its precise effects.
Unclassified Spyware	Software that is suspected from trusted sources as spyware, but whose specific effects were not yet determined.
Worm	A computer worm is a self-replicating program that spreads through email or other file transmission capabilities. Worms harm the network and consume bandwidth, whereas viruses infect or corrupt files on a targeted computer.

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.

Symantec Web Gateway applies content filter policies to embedded URLs including domain exceptions that you specify in content filter policies. However, user configured whitelisted domains are not applied to embedded URLs. An embedded URL is when a URL contains another URL within it. The embedded URL in the following example is badurl.com:

http://symantecexample.com/index.html/?badurl.com/home.js

See "Preinstallation checklist" on page 19.

See "URL filtering categories" on page 122.

See "Configuring embedded URL detection" on page 139.

Symantec Web Gateway does not support the ability to redirect URLs or block URLs if you use the port span/tap configuration and any of the following conditions exist:

- Your organization uses a corporate switch that implements Access Control Lists (ACL)
- Your network has a feature that prevents session hijacking

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 60.

When a user attempts to access a Web site in a blocked category, a message appears 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 149.

Note: If you use the SSL proxy, users cannot see your custom end user page when they attempt to access a domain in which no intercept policy exists. This situation can occur if you do not have an SSL intercept policy for a certain category, but you do have a content filtering blocking policy for that category. The message that they see depends on the Web browser that they use. For example, Internet Explorer displays a forbidden error message. Firefox displays a message that the proxy server refuses the connection. This issue occurs for HTTP/HTTPS or deep inspection ports.

See "Internet applications, malware, and URL filtering blocking behavior" on page 97.

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. The blacklist and whitelist in Symantec Web Gateway provide more global behavior.

Note: Symantec Web Gateway does not map the domain name and IP address of a Web site that you add as an exception.

If a website is accessed using an IP address and a policy that you created blocks/monitors/allows the category of the IP address, you can add the IP address as an exception to the policy with a different action.

If a website is accessed using a URL and a policy that you created blocks/monitors/allows the category of URL, you can add the domain name as an exception to the policy with a different action.

See "Blocking or monitoring Web sites using the blacklist" on page 143.

See "Allowing Web site access using the whitelist" on page 146.

To configure URL filtering 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 101.

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 140.

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, 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, 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 appear 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 appear 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 in reports.

See "URL filtering categories" on page 122.

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

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

Specify a domain name or an 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**.

URL filtering categories

Symantec Web Gateway uses Symantec's RuleSpace Web Categorization Solution (Symantec RuleSpace) to classify URL filtering categories. Symantec RuleSpace has several new URL categories and classes and makes URL filtering more effective than the previous URL filtering database.

Table 6-6 through Table 6-29 describe the URL filtering categories available in Symantec Web Gateway. Use these categories when you create URL filtering policies.

You can report any misclassified URLs to Symantec.

See "Reporting misclassified URLs " on page 139.

Table 6-6 URL filtering class: Criminal Activities

Category	Description
Criminal Skills	Web sites which provide instruction for threatening or violating the security of property or the privacy of people; also how to avoid complying with legally mandated duties and obligations.
Hacking	Web sites which promote or provide the means to practice illegal or unauthorized acts of computer crime using technology or computer-programming skills.
Hate	Web sites which advocate hostility or aggression toward an individuals or groups on the basis of race, religion, gender, nationality, ethnic origin, or other involuntary characteristics; Web sites which denigrate others on the basis of those characteristics or justifies inequality on the basis of those characteristics; Web sites which purport to use scientific or other commonly accredited methods to justify said aggression, hostility or denigration.

Table 6-7 URL filtering class: Drugs

Category	Description
Alcohol	Web sites which promote or sell alcoholic beverages; supply recipes or paraphernalia to make alcoholic beverages; glorify, tout, or otherwise encourage alcohol consumption or intoxication.
Drugs	Web sites which promote, offer, sell, supply, encourage or otherwise advocate the recreational or illegal use, cultivation, manufacture, or distribution of drugs, pharmaceuticals, intoxicating plants or chemicals and their related paraphernalia.
Tobacco	Web sites which encourage, promote, offer for sale or otherwise encourage the consumption of tobacco.

Table 6-8 URL filtering class: Dymanic Content

Category	Description
Dynamic	Web sites which have been found to contain both appropriate and inappropriate user-generated content like social networking or blogging Web sites. Also, Web sites in which the page content changes based how the user is interacting with it (e.g. an internet search). Web sites that return a Dynamic category will also normally have a standard category.

Table 6-9 URL filtering class: Entertainment

Category	Description
Art & Museums	Web sites which include art galleries, artists, and museums. All types of visual arts such as performing arts, theater, painting, drawing, sculpture, and photography are included as well as natural history, science and children's museums.
Entertainment	Web sites which relate to personal entertainment as well as the entertainment industry.
Mobile Entertainment	Web sites which offer a range of add-ons for handheld devices like ringtones, wallpapers, games, videos.
Music	Web sites related to Radio, Band/artist pages, Music fan, Music reviews, Music studios, venues, record labels, promotional Web sites, Lyrics, tablature, and sheet music.

Table 6-9 URL filtering class: Entertainment *(continued)*

Category	Description
Streaming Media	Web sites which host streaming media like television, movies, video, radio, or other media.

Table 6-10 URL filtering class: Extreme

Category	Description
Child Abuse Images and Content	Web sites hosting illegal child abuse images and content anywhere in the world.
Gore	Web sites which display graphic violence and/or the infliction of pain or injuries. Gross violence towards humans or animals such as scenes of dismemberment, torture, massive blood and gore, sadism and other types of excessive violence.
Self Harm	Web sites which describe or discuss ways in which to self harm including eating disorders and self-injury.
Suicide	Web sites which describe or promote suicide.
Violence	Web sites which advocate or provide instructions for causing physical harm to people or property through use of weapons, explosives, pranks, or other types of violence.

Table 6-11 URL filtering class: Finance

Category	Description
Finance & Investing	Web sites which provide the opportunity to establish, plan, research, or manage personal finances and investments.

Table 6-12 URL filtering class: Games

Category	Description
Cash Gambling	Web sites which specifically involve the wagering and exchange of money online, e.g. placing bets or participating in betting pools (including lotteries).
Gambling	Web sites which allow users to place bets or participate in a betting pool (including lotteries) online; obtain information, assistance or recommendations for placing bets; receive instructions, assistance, or training on participating in games of chance.

Table 6-12 URL filtering class: Games *(continued)*

Category	Description
Gaming	Web sites which are related to computer or video games, game downloads, and online game Web sites.

Table 6-13 URL filtering class: General Business

Category	Description
Business	Web sites which are sponsored by or devoted to individual businesses not covered by any other categories.
Energy	Web sites which represent companies involved with the production and distribution of energy. These include companies related to oil, power, gas, and other alternative sources of energy.
Law	Web sites which offer legal content and services.
Real Estate	Web sites which are commercial in nature and involved in the real estate business.
Wedding	Web sites related to the traditions, customs, planning, and products involved in a marriage or commitment ceremony as well as in civil unions.

Table 6-14 URL filtering class: Illegal Activities

Category	Description
Plagiarism	Web sites which are primarily designed to allow students to cheat at school by taking the work or ideas of someone else and pass it off as their own. Includes Web sites that offer free or paid-for written essays, tests and/or term-papers as well as paid-for services for custom written papers.

Table 6-15 URL filtering class: Information

Category	Description
Chat	Web sites which offer users the ability to chat online (by broadcasting messages to people on the same Web site in real time).

Table 6-15 URL filtering class: Information *(continued)*

Category	Description
Enterprise Webmail	Web sites which provide online email services. These include the following:software for providing webmail services, ISP email access via web mail interface. Web mail provided as part of paid or premium hosting servicesBusiness, school, or institutional mail accessed via a web mail interface.
Forums & Message Boards	Web sites which provide a web application enabling users to participate in the discussion of numerous topics, often in conjunction with online communities.
News	Web sites which primarily report, inform, or comment, on current events or contemporary issues of the day. Includes sports, weather, editorials, and human interest news.
Portal	Web sites which offer a broad array of resources and services, such as email, forums, search engines, and on-line shopping malls. Portals typically publish their own content or collate multiple sources of information for many areas such as news, entertainment, sports, technology, and finance.
Reference	Web sites which are commercial in nature and involved in the real estate business.
Search	Web sites which support searching the Internet, news groups, or indices and directories.
Webmail	Web sites which provide free, web-based email services, accessible through any Internet browser. For example, Hotmail, Gmail, Yahoo Mail, and so on.

Table 6-16 URL filtering class: IT

Category	Description
Anonymizer	Web sites which offer anonymous access to Web sites through a PHP or CGI proxy, allowing users to gain access to Web sites blocked by corporate and school proxies as well as parental control filtering solutions.
Automated Web Application	Web sites which allow a computer to automatically open an http connection for various reasons including checking for operating system or application updates.

Table 6-16 URL filtering class: IT *(continued)*

Category	Description
Content Delivery Network	Web sites which are content delivery/distribution networks (CDN) designed to accelerate the delivery of content rich internet pages or large files to end users. This is typically done by deploying geographically dispersed datacenters, each containing copies of the data.
File Sharing	Web sites which make files available for other users to download over the Internet or private networks.
Freeware & Shareware	Web sites which offer the download of software online.
Hosting	Web sites which provide individuals or organizations with online systems for storing images, video, or any content accessible via the Web.
Internet Telephony	Web sites which enable users to make telephone calls via the Internet or obtain information or software for this purpose. These services include PC to PC, PC to phone, and phone-to-phone services connecting via TCP/IP networks.
Online Backup and File Storage	Web sites which provide the ability to backup or upload data files to the internet providing long term storage, access from other computers or locations, or the ability to share data files with other users. This category specifically excludes dedicated photo/video sharing Web sites.
Remote Access	
Technology & Telecommunications	Web sites which provide information pertaining to computers, the Internet as well as telecommunication

Table 6-17 URL filtering class: Job Search

Category	Description
Job Search	Web sites which provide assistance or tools to help to find employment.

Table 6-18 URL filtering class: Lifestyle

Category	Description
Food & Restaurants	Web sites which provide information about food, recipes, specialty food shops, catering, and food delivery as well as Web sites which include information about restaurants. Also included are restaurant guides and reviews.
Glamour	Web sites which emphasize, promote, or provide information on how to achieve physical attractiveness, allure, charm, beauty or style with respect to personal appearance.
Hobbies	Web sites which provide information on private pastimes. For example, genealogy, collectibles, crafts, outdoor hobbies, new age activities (astrology/horoscope), non-online gaming, and so on.
Lifestyles	Web sites which contain general material relevant to sexual orientation. This will include pages dedicated to the groups themselves, discussions, issues, clubs, personal home pages that address or support sexual orientation lifestyle choices. These are Web sites mainly by target group members for target group members. Discussions and issues that are of an explicitly mature nature are not part of this category. The specific TARGET groups in question are gay, lesbian, bisexual and transgender and are subsequently referred to as “GLBT”.
Personal Ads & Dating	Web sites which promote or provide opportunity for establishing or continuing romantic relationships.
Pets	Web sites and forums related to the care, maintenance, purchase, rescue or breeding of any animal for companionship and enjoyment. The category excludes livestock or laboratory animals which are kept for economic or scientific reasons.
Photography	Web sites related to taking, sharing, printing, studying, or manipulating photos at all levels, whether casual, amateur or professional. Excludes galleries of photos on social networking Web sites.

Table 6-18 URL filtering class: Lifestyle *(continued)*

Category	Description
Sports	Web sites which promote or provide information about spectator sports. For example, professional sports teams, leagues, organizations, or association Web sites, player and fan Web sites.
Travel	Web sites which promote or provide opportunity for travel planning in a general sense, particularly finding and making travel reservations.

Table 6-19 URL filtering class: Malware

Category	Description
Adware/Spyware	Web sites of domains associated with vendors and distributors of spyware, adware, greyware, and other potentially unwanted advertising software. Some of these domains may run exploits to facilitate the installation of this unwanted software.
Malware Domain	Web sites where the domain was found to either contain malware or take advantage of other exploits to deliver adware, spyware or malware.
Malware Object	Web sites that contain direct links to malware file downloads: . exe, .dll, .ocx, and others. These URLs are generally highly malicious.
Malware Phishing	Web sites containing characteristics of phishing techniques: transposition, misspellings, common phishkit paths, and other phishing keywords. Also includes phishing Web sites reported to eBay and Paypal, as well as other 3rd-party phishing feeds.
Potential Malware Victim	Web sites that click fraud and adware components use when "phoning home" which could signal that a device is infected with spyware or adware. This category should be used only for reporting, not for blocking as the target URLs can be perfectly legitimate Web sites.

Table 6-20 URL filtering class: Mature Content

Category	Description
Art Nudes	Web sites which contain the non-pornographic, tasteful, and artful display of the naked body. The main purpose of these Web sites is not sexual arousal.
Bikini	Web sites which offer the sale of bikinis, mico-kinis, mono-kinis, and thongs which are marketed as beachwear rather than swimwear. Also Web sites which feature galleries and/or videos of models in bikinis.
Lingerie	Web sites offering the sale of lingerie.
Mature Content	Web sites which contain sexually explicit information that is not of a medical or scientific nature.
Sexual Advice	Web sites which contain discussions or descriptions of sexual techniques or exercises, sexual relationship counseling, explicit discussions of sex and sexuality and products to improve one's sex life.
Sexual Education	Web sites which provide educational information on reproduction and sexual development, sexually transmitted disease, contraception, safe sexual practices, sexuality, and sexual orientation.
Sexual Orientation	Web sites which contain discussions of Sexual orientation issues.

Table 6-21 URL filtering class: Medicine

Category	Description
Abortion	Web sites which provide information or arguments in favor of or against abortion; describe abortion procedures; offer help in obtaining or avoiding abortion; provide testimonials on the physical, social, mental, moral, or emotional effects of abortion.
Health	Web sites which provide information or advice on personal health or medical services, health insurance, procedures, or devices; Web sites which include information on diets, nutrition, therapies and counseling services.

Table 6-22 URL filtering class: Ordering

Category	Description
Advertising	Web sites which provide Internet advertising services.
Placeholder	Web sites which are typically owned by domain name registrars, domain brokers or Internet advertising publishers. They usually display dynamically generated content with the intent to monetize on traffic through linked advertising listings.
Shopping	Web sites which offer a broad array of resources and services, such as email, forums, search engines, and on-line shopping malls. Portals typically publish their own content or collate multiple sources of information for many areas such as news, entertainment, sports, technology, and finance.

Table 6-23 URL filtering class: Personal Web sites

Category	Description
Blog	Web sites which contain 'blogs' (an abridgment of the term 'web logs'). Blogs are usually maintained by an individual with regular entries of commentary, descriptions of events, or other material such as graphics or video. Entries are commonly displayed in reverse chronological order.

Table 6-24 URL filtering class: Pornography

Category	Description
Nudism	Web sites which are related to Nudism or Naturism. These Web sites may contain pictures or videos or nude bodies but do not contain sexually explicit material.
Pornography	Web sites which contain sexually explicit material for the purpose of arousing a sexual or prurient interest.

Table 6-25 URL filtering class: Social Networking

Category	Description
Virtual Community/Social Networking	Web sites which offer a variety of tools and mechanisms to enable a group of people to communicate and interact via the Internet.

Table 6-26 URL filtering class: Society

Category	Description
Cults	Web sites which feature well-known, organized new religious movements and sects that are regarded as exploitative or unorthodox. Characteristics include: gross deviation from mainstream doctrine; single charismatic leader; abusive, manipulative control over followers' lives; second-coming/doomsday prophecies.
Education	Web sites which represent schools or other educational facilities, faculty or alumni groups.
Government	Web sites which are sponsored by government branches or agencies.
Kids	Web sites which provide a safe and interesting Internet experience for children under 12 years of age.
Non-profit	Web sites which are owned by non-profit organizations. A non-profit organization (abbreviated "NPO", also "not-for-profit") is a legally constituted organization whose primary objective is to support or to actively engage in activities of public or private interest without any commercial or monetary profit purposes. NPOs are active in a wide range of areas, including the environment, humanitarian aid, animal protection, education, the arts, social issues, charities, health care, politics, religion, research, sports or other endeavors.
Occult	Web sites which promote or offer methods, means of instruction, or other resources to affect or influence real events through the use of spells, curses, magic powers or supernatural beings.
Politics	Web sites which relate to politicians, election campaigns, political organizations and publications. Includes official homepages of politicians and political parties as well as personal Web sites about politics and grass-root movements.
Religion	Web sites which are about religion as any set of beliefs and practices that have the function of addressing the fundamental questions of human identity, ethics, death, and the existence of the Divine.

Table 6-26 URL filtering class: Society *(continued)*

Category	Description
Science	Web sites which provide research materials in the natural and life sciences.

Table 6-27 URL filtering class: Vehicles

Category	Description
Automotive	Web sites which relate to motor vehicles, dealers, sales and clubs.

Table 6-28 URL filtering class: Weapons

Category	Description
Military	Web sites which are sponsored by military branches or agencies as well as official and personal Web sites related to military history, ideology, or specific branches of the military.
Weapons	Web sites which describe or offer for sale weapons including guns, ammunition, firearm accessories, knives and martial arts.

Table 6-29 URL filtering class: Unclassified

Category	Description
Unclassified	Web sites that do not fall into any of the above mentioned categories.

Upgrade considerations for Symantec Web Gateway version 5.1

Symantec RuleSpace has several new URL categories and classes and makes URL filtering more effective than the previous URL filtering database.

See "URL filtering categories" on page 122.

As a result of improved categorization, after you upgrade to Symantec Web Gateway version 5.1, several Web sites are categorized differently from the categorization in version 5.0.x. This results in some Web sites being mapped into the categories that have a different policy action assigned to them. For example, in version 5.0.x, the Web site http://twitter.com is categorized as **Social Media** and **Social Networking**. The policy that you created has the following settings and actions for the categories:

Social Media	**Monitor**
Social Networking	**Monitor**
Uncategorized	**Block**
Multiple Categories	**Restrictive: Block takes precedence**

In version 5.1, the Web site http://twitter.com is categorized as **Blog** and **Unclassified**. For the above mentioned policy actions, after you upgrade to version 5.1, Symantec Web Gateway blocks http://twitter.com though it was monitored in version 5.0.x.

Additionally, many categories in the previous URL filtering database now have a different name. For example, version 5.0.x has a category named **Cinema** while version 5.1 has a category named **Entertainment**. If you configured a custom report to display all Web sites under **Cinema**, you must modify the custom report configuration to include **Entertainment**. This ensures that Symantec Web Gateway reports similar information after you upgrade to version 5.1.

You must note that upgrade process to version 5.1 cannot be reversed easily. Symantec recommends that you test the categorization changes in a lab setup before you upgrade to version 5.1. You thus ensure that your important Web site concerns are addressed in the manner you expect. Accordingly, you may apply any policy changes that are required to meet your business needs.

Symantec RuleSpace URL filtering categories mapping information

Symantec RuleSpace has several new URL categories and classes and makes URL filtering more effective than the previous URL filtering database.

Before you refer Symantec RuleSpace URL filtering categories mapping information you must know several upgrade considerations.

See "Upgrade considerations for Symantec Web Gateway version 5.1" on page 133.

Table 6-30 lists the mapping information of the previous URL filtering database to Symantec RuleSpace URL filtering database and the default action for each of the categories.

Note: Each category of the previous URL filtering database may be mapped into more than one new category in the Symantec RuleSpace URL filtering database. For example, **Illegal Activities** is mapped into the three new categories, namely, **Criminal Skills**, **Plagiarism**, and **Child Abuse Images and Content**.

When you upgrade to version 5.1, Symantec Web Gateway modifies your existing policies based on the Symantec RuleSpace URL filtering categories mapping information. For example, a policy that you created allows all Web sites that are categorized as **Gambling** in the previous URL filtering database. When you upgrade to version 5.1, the modified policy allows all Web sites that are categorized as **Cash Gambling** and **Gambling** in the Symantec RuleSpace URL filtering database.

You can report any misclassified URLs to Symantec.

See "Reporting misclassified URLs " on page 139.

Table 6-30 Symantec RuleSpace URL filtering categories mapping information

Previous URL filtering category	Symantec RuleSpace URL filtering category	Default action
Abortion	Abortion	Allow
Alcohol	Alcohol	Allow
Anonymous Proxies	Anonymizer	Block
Art	Art & Museums	Allow
Banner Advertisements	Advertising	Allow
Banner Advertisements	Placeholder	Allow
Blogs	Blog	Allow
Blogs	Forums & Message Boards	Allow
Chat	Chat	Block
Cinema	Entertainment	Allow
Communication Services	Technology & Telecommunications	Allow
Communication Services	Remote Access	Allow
Computer Crime	Hacking	Block
Computer Games	Gaming	Block
Dating	Lifestyles	Block
Dating	Personal Ads & Dating	Block
Dating	Sexual Orientation	Block
Education	Education	Allow

Table 6-30 Symantec RuleSpace URL filtering categories mapping information *(continued)*

Previous URL filtering category	Symantec RuleSpace URL filtering category	Default action
Education	Kids	Allow
Education	Reference	Allow
Education	Science	Allow
Environment	Pets	Allow
Erotic	Mature Content	Block
Erotic	Sexual Advice	Block
Fashion	Glamour	Allow
Financial Services	Finance & Investing	Allow
Gambling	Cash Gambling	Block
Gambling	Gambling	Block
General Business	Business	Monitor
General Business	Content Delivery Network	Monitor
General Business	Energy	Monitor
General Business	Law	Monitor
General Business	Photography	Monitor
General Business	Real Estate	Monitor
General Business	Wedding	Monitor
Governmental Organizations	Government	Allow
Health	Health	Allow
Illegal Activities	Criminal Skills	Block
Illegal Activities	Plagiarism	Block
Illegal Activities	Child Abuse Images and Content	Block
Illegal Drugs	Drugs	Block
Job Search	Job Search	Allow

Table 6-30 Symantec RuleSpace URL filtering categories mapping information *(continued)*

Previous URL filtering category	Symantec RuleSpace URL filtering category	Default action
Malware	Malware Domain	Block
Malware	Malware Object	Block
Malware	Adware/Spyware	Block
Malware	Potential Malware Victim	Block
Malware	Malware Phishing	Block
Mobile Telephony	Internet Telephony	Allow
Music	Mobile Entertainment	Allow
Music	Music	Allow
News	News	Allow
Non-Governmental Organizations	Non-profit	Allow
Political Extreme	Hate	Block
Political Parties	Politics	Allow
Pornography	Pornography	Block
Recreational Facilities	Hobbies	Allow
Religion	Religion	Allow
Restaurants	Food & Restaurants	Allow
Search Engines	Portal	Allow
Search Engines	Search	Allow
Sects	Cults	Allow
Sects	Occult	Allow
Shopping	Shopping	Monitor
Social Media	Streaming Media	Monitor
Social Networking	Virtual Community/Social Networking	Monitor

Table 6-30 Symantec RuleSpace URL filtering categories mapping information *(continued)*

Previous URL filtering category	Symantec RuleSpace URL filtering category	Default action
Software-Hardware	Automated Web Application	Allow
Software-Hardware	Freeware & Shareware	Allow
Sports	Sports	Monitor
Swimwear	Art Nudes	Monitor
Swimwear	Bikini	Monitor
Swimwear	Lingerie	Monitor
Swimwear	Nudism	Monitor
Swimwear	Sexual Education	Monitor
Tobacco	Tobacco	Allow
Travel	Travel	Allow
Unclassified	Unknown	Allow
Unclassified	Dynamic	Allow
Vehicles	Automotive	Allow
Violence	Gore	Block
Violence	Self Harm	Block
Violence	Suicide	Block
Violence	Violence	Block
Weapons	Military	Block
Weapons	Weapons	Block
Web Storage	File Sharing	Monitor
Web Storage	Hosting	Monitor
Web Storage	Online Backup and File Storage	Monitor
Webmail	Enterprise Webmail	Allow
Webmail	Webmail	Allow

Reporting misclassified URLs

When you identify a URL that is wrongly classified or that belongs to an inappropriate URL category, you can report the misclassified URL to Symantec.

See "URL filtering categories" on page 122.

To report a misclassified URL

1. In the Web GUI, click **Administration > Policies > Blocking Feedback**.
2. Click **Request changes to Content Filter classification**.
3. On the **Symantec Web Gateway URL Lookup and Review Submission** Web page, enter the misclassified URL in the **Enter URL to check** text box .
4. Enter the appropriate validation input and then click **Categorize URL**.
5. Under **URL database lookup results**, click **Submit**.

Configuring embedded URL detection

An embedded URL is a URL that contains another URL within it. An embedded URL lets the user evade URL filtering rules and access an inappropriate or a blocked Web site. For example, a policy that you created blocks the Web site `www.symantecs.org`. The embedded URL `www.symantecexample.com/path/www.symantecs.org` lets the user access `www.symantecs.org` though you blocked it.

Symantec Web Gateway by default detects embedded URLs. However, you can disable embedded URL detection when you do not want to monitor embedded URLs.

Note: Symantec recommends that you enable embedded URL detection.

Symantec Web Gateway logs the detection of embedded URLs in the **Custom Reports** page. The detected embedded URLs are listed under **Requested URL or file** in the following format: `EURL:(<embedded url>)<url of the website user visited>`.

For example, `EURL:(youtube.com)google.com/#hl=en&q=youtube.com&pf=p&.....`

To configure embedded URL detection

1. In the Web GUI, click **Administration > Configuration > Modules**.
2. Under **Content Filter Configuration**, do one of the following:

Uncheck **Detect Embedded URLs**	To disable embedded URL detection.
Check **Detect Embedded URLs**	To enable embedded URL detection.

3. Click **Save**.

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 118.

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 101.
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 beside **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 beside **Non-Working Days**.
6. For **After Hours End**, click the hour and minute before which after hours exceptions apply on working days.

7 Under **After Hours Exception**, specify the after hours behavior for **Content Filter Categories**.

See "Configuring URL filtering policies for Web sites" on page 118.

To copy the working hour settings to the **After Hours Exception**, click **Copy from 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 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. Based on your policy, the blocking page for quarantined computers can include malware cleanup information and contact information for your site's IT help desk.

You must first enable **Client Scan and Cleaning**. Then you can assign infected computers to the quarantine.

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 149.

See "About end user pages" on page 148.

You can configure a policy to quarantine infected computers in either of the following ways:

- With the **Client Remediation** option
  See "To enable Client Scan and Cleaning" on page 141.
- By assigning infected computers to the quarantine
  See "To assign infected computers to the quarantine" on page 142.

To enable Client Scan and Cleaning

- In the Web GUI, click **Administration > Configuration > Client Remediation**.

  You can set the default action for all computers to Quarantine, or optionally create Infected Client Cleanup policies for specific workgroups.

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 101.

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. Beside **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**.

Configuring NTLM user authentication behavior

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

See "About Active Directory integration" on page 189.

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 workgroups but not using any of the LDAP **Network Types**.

   See "Specifying computers or users for policies" on page 101.

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 and servers running without a user.

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 appears in the Web browser.
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 all of 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. The default setting in the monitoring mode is to monitor. 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 with blacklists.

Symantec Web Gateway supports custom blacklist policies over HTTP and HTTPS. However, blacklist with keyword or by file extension policies are not supported over HTTPS.

See "Configuring URL filtering policies for Web sites" on page 118.

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. You assign the same **Category** and **Severity** for all domain names and IP addresses in the file.

   List one domain name or IP address per line in the file. You can optionally add one or more keywords to the file. Separate keywords from the domain name with a comma. You should separate multiple keywords with spaces.
3. Type a **Name** for the blacklist entry.

   The name appears 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`. Omit the `http://` part of a URL. Omit 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**. Omit slashes in the **Keyword**.
7. For **Description**, type a description.

   The **Description** appears on the blacklist page and in reports.
8. Click a **Severity**.

   The blacklist **Severity** relates to the policy **Spyware Severity**. The action that you 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 that you 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.

Symantec Web Gateway supports custom blacklist policies over HTTP. However, for SSL Deep Inspection Symantec Web Gateway does not support custom blacklist policies for file extensions.

To block or monitor file transfers 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 appears on the blacklist page and in reports.

4 For **Block Type**, click **Block by File Extension**.

5 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 click 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**. Omit periods when typing a file extension.

7 Optionally, for **Keyword** you can 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 Under **File Direction**, click one of the following options:

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 In the **Description** box, type a description.

This **Description** appears on the blacklist page and in reports.

10 Click a **Severity**.

The blacklist **Severity** relates to the policy **Spyware Severity**. The action that you 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 that you 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**.

Allowing 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 is allowed to a Web site or network on the whitelist 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.

Symantec Web Gateway applies content filter policies to embedded URLs. However, whitelisted domains and domain exceptions that you specify in content filter policies are not applied to embedded URLs. An embedded URL is when a URL contains another URL within it. The embedded URL in the following example is badurl.com:

http://symantecexample.com/index.html/?badurl.com/home.js

The Symantec Web Gateway proxy does not support IP-based or Ignore Authentication whitelist configuration. However, domain-based whitelisting is supported in proxy mode.

For proxy configuration, if you want to whitelist a server, you must use a proxy auto-configuration (PAC) file. If you want to whitelist a client's computer, do not configure the client browser to use the Symantec Web Gateway proxy service.

See "Sample proxy auto-configuration (PAC) file" on page 211.

See "Configuring URL filtering policies for Web sites" on page 118.

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 189.

   See "Sample proxy auto-configuration (PAC) file" on page 211.

6 Optionally, under **Comment** type a comment.

This comment appears 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 on your network think are 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. When they click the link, Symantec Web Gateway adds the Web site or file that is blocked in error to the Blocking Feedback report. You can then review the report to determine whether the Web site or file should be unblocked.

You can block user feedback by disabling the link that is available on the blocking page.

See "About end user pages" on page 148.

See "About policies" on page 92.

The Blocking Feedback report is located on the **Policies > Blocking Feedback** page. You can add a Web site or file to the whitelist after you review the report. You can also submit Web sites to Symantec's Web site categorization service for review.

See "Allowing Web site access using the whitelist" on page 146.

After you determine that a Web site or file in the report should remain blocked, you can delete those items from the report. It then becomes easier for you to focus on the other items in the report.

About end user pages

A message appears in the user's Web browser indicating a blocked Web site, blocked file upload or download, or a malware infection. The page that appears 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 149.

To block file transfers, you must install Symantec Web Gateway in the inline network configuration or proxy network configuration, not the port span/tap network configuration.

When no Quarantine Policy is configured, Symantec Web Gateway sends an end user page to its Quarantined end user clients. As the end user page displays an URL with host name, instead of displaying an URL with Symantec Web Gateway IP address. You cannot access the quarantined end user page, because the URL contains a host name. Symantec recommends that you add the host name of the Management Interface to your local DNS server.

See "Quarantining infected computers" on page 141.

See "About policies" on page 92.

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

End user pages provide your users with information about blocked Web sites, blocked file uploads and downloads, and possible infections. You can customize many of these settings for end user pages.

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 that is used on this page and the image that appears. The **Language** and **New Image** settings that are described in Table 6-31 apply to the patience page.

See "Download behavior in user Web browsers" on page 95.

Note: If you use the SSL proxy, users cannot see your custom end user page when they attempt to access a domain in which no intercept policy exists. This situation can occur if you do not have an SSL intercept policy for a certain category, but you do have a content filtering blocking policy for that category. The message that they see depends on the Web browser that they use. For example, Internet Explorer displays a forbidden error message. Firefox displays a message that the proxy server refuses the connection. This issue occurs for HTTP/HTTPS or deep inspection ports.

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 152.

See "About end user pages" on page 148.

Table 6-31 and Table 6-32 describe the settings for the messages that Symantec Web Gateway displays to end users.

Table 6-31 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 101.
Language	**English**	Display the default text in the selected language. In the Web page that appears to the user, supporting text, such as the text for user feedback, appears in the selected language.
Header Image	Symantec Web Gateway logo	The default image that is located at the top of the Web page that appears to the user.
New Image	No default	Import a different image than the Symantec Web Gateway logo for the top of the Web page that appears to the user.
URL Block text	`This URL, %domain%, is a known %category% location and violates company policy.`	Text that appears when the user attempts to access a blocked Web site.
Download Block Text	`The file, %filename%, contains %category% and violates company policy.`	Text that appears when the user attempts to upload or download a blocked file.

Table 6-31 Blocked URL or File Message Configuration *(continued)*

Item	Default	Description
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 appears 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**.

In Table 6-32, the detected pages and scheduled cleaning pages only apply if you enable Client Remediation. If you use version 5.0 or later, you must provide your own remediation URL. Also note that these are the pages that appear to quarantined users.

Table 6-32 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 appears 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 appears in normal font when spyware has been detected on a computer. In the default text, the detected spyware is listed.

Table 6-32 Spyware Detected Page & Scheduled Cleaning Configuration *(continued)*

Item	Default	Description
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 appears to the user when spyware has been detected on a computer.

Variables for end user pages

Symantec Web Gateway lets you use variables for end user page messages. 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 149.

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 6-33 describes variables available for the messages in end user pages.

Table 6-33 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
%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

Table 6-33 Variables for end user pages *(continued)*

Variable	Encoded version	Description	Blocked URL	Blocked file	Detected page	Scheduled cleaning page
`%url%`		The URL that was blocked.	Yes	No	No	No

Chapter 7

Administering Symantec Web Gateway

This chapter includes the following topics:

- About system users
- About database and software updates
- About alerts
- About backing up and restoring the Symantec Web Gateway configuration
- Enabling and disabling remote assistance
- Uploading diagnostic files
- Resetting Symantec Web Gateway to factory settings
- Restarting and turning off the Symantec Web Gateway appliance
- Configuring incident history
- Testing ports connectivity
- Testing NTP server connectivity
- Testing mail server settings
- Resetting the Web GUI password for the primary system user
- Serial Console access to Symantec Web Gateway
- About traffic capture

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 159.

See "Creating roles for system users" on page 157.

See "Monitoring system user activity" on page 160.

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 156.

Table 7-1 Permissions for system users

Permission type	Read-only Web GUI areas	Editable Web GUI areas
Read Only	■ **Administration > System Status** ■ **Administration > Updates** ■ **Administration > End User Pages** ■ **Administration > System Users** ■ **Administration > Configuration**	■ **Reports**
Read & Write	■ **Administration > System Status** ■ **Administration > Updates** ■ **Administration > End User Pages** ■ **Administration > System Users** ■ **Administration > Configuration**	■ **Reports** ■ **Policies**
Administration	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 189.

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 7-2 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 189.
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 that is permitted to system users.

See "Permissions for system users" on page 156.

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 156.

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.
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 any of the 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, the report data that matches either filter appears 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 159.

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 156.

See "Creating roles for system users" on page 157.

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. The default option is **N/A**. Use this option if there is no role for system user. See "About roles for system users" on page 156.
Description (Optional)	The **Description** appears 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 156.

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 7-3 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 7-3 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 MB	Automatically check for updates hourly	No	Definitions of known malware
Database	Multiple times daily	About 5-10MB	Automatically check for updates hourly	No	Antivirus and content filter
Software	■ Minor releases (w.x.y.z) ■ Major releases (x.y and x.y.z)	About 70 MB	Manual update	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. 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 Gatewayappliance. Examples of alerts are as follows: ■ By the hardware bypass being activated or deactivated ■ When disk space is running low ■ When the system starts up ■ When the CPU temperature is high ■ When a power supply fails ■ When a hard drive is corrupt (models with RAID arrays only) ■ When the network is not configured properly (Redundant power and RAID are not available on all models)
CIU alerts	Alerts for when CIU's managed appliance has system problem and when it loses connection for a specific period of time

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 in CSV format or HTML format.

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 163.

See “About monitoring Symantec Web Gateway using SNMP” on page 163.

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 162.

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 162.

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 and 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 213.

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 you need to reinstall Symantec Web Gateway on the same appliance, you can restore the configuration. You can also restore the configuration to a different, compatible appliance. For example, when you upgrade to a new Symantec Web Gateway appliance, you can back up the old model and restore the configuration to the new model. As a best practice, you should include backing up Symantec Web Gateway as part of your network backup scheme.

You can make a backup from one type of Symantec Web Gateway model and restore it on the same model or on a different but compatible model.

See "Cross-model backup and restore compatibility" on page 164.

See "Creating a manual backup" on page 166.

See "Creating a scheduled backup" on page 167.

See "Restoring backups" on page 168.

Cross-model backup and restore compatibility

Table 7-4 describes the cross-model backup and restore compatibility of various Symantec Web Gateway models. **Yes** means that the backup capabilities and restore capabilities are supported between the source model and destination model. **No** indicates that they are not supported. The rows in this table indicate the model of the backup. The columns indicate the models onto which you can restore the backup. For example, you can restore backups from an 8450 model to an 8450 model, but you cannot restore backups from an 8490 model to an 8450 model.

Similarly, you can backup from a Central Intelligence Unit and restore it on the same Central Intelligence Unit. Or you can restore it on a different Central Intelligence Unit different but compatible Central Intelligence Unit.

Note: You cannot restore a backup from a managed appliance to a Central Intelligence Unit. Similarly, you cannot restore a backup from a Central Intelligence Unit to a managed appliance.

Table 7-4 Cross-model backup and restore compatibility

Backup from model	Restore to model 8450	Restore to model 8490	Restore to Virtual
8450	Yes	Yes	Yes
8490	No	Yes	No
Virtual	Yes	Yes	Yes

Backup file contents

When you use the Web GUI to create a backup, the backup data is stored in a file on your local computer. To store a file on a remote computer, schedule a backup.

See "About backing up and restoring the Symantec Web Gateway configuration" on page 164.

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

`backup_day_month_year_hour_minute_second_DeviceName.des3`

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

`backup_17_10_2009_11_10_15_WEBGATE2.des3`

The hour in the backup name follows the 24-hour format.

You can rename the backup file. Renaming the backup file does not affect the restore process. Do not attempt to edit the backup file.

Table 7-5 lists the configuration information that is and is not included in the backup file.

Table 7-5 Backup file contents

Included configuration information	Omitted configuration information
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 ■ SNMP settings ■ Policy Configuration ■ Web Gateway updates ■ Operating mode ■ Central Management Configuration ■ Servers ■ Email settings ■ Syslog settings ■ Proxy settings ■ Time zone and NTP server settings ■ Module settings ■ Insight settings ■ Dispatched scan and cleaning configuration ■ Appliance security settings ■ Report settings ■ End user Pages settings	The following configuration information is not saved when you back up Symantec Web Gateway: ■ Report data ■ System Maintenance ■ All Events ■ Blocking Feedback ■ System Status page

Creating a manual backup

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 164.

See "Backup file contents" on page 165.

As a best practice, every time you back up Symantec Web Gateway, save the backup files in the same location.

To create a manual backup

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

Creating a scheduled backup

In addition to creating a manual backup from the Web GUI page, you can set up a scheduled backup to occur at regular intervals. For example, you can schedule a backup to occur once, weekly, or monthly. Symantec Web Gateway saves the scheduled backup file to the FTP directory that you specify.

See "About backing up and restoring the Symantec Web Gateway configuration" on page 164.

See "Backup file contents" on page 165.

To create a scheduled backup

1. In the Web GUI, click **Administration > Configuration > Maintenance**.
2. Beside **Scheduled Backup Current Settings to File**, click **Scheduled Backup.**

   If there is no scheduled backup, the following message appears:

   You have no backups scheduled.
3. To create a scheduled backup, click **New Schedule.**

   The **Save and Schedule Backup** page appears.
4. On the **Save and Schedule Backup** page, specify the following information.

Backup Frequency	Beside **Backup Frequency**, select one of the following options: ■ **Save Only** Select this option if you want to save the current backup settings for future use. ■ **Once** Select this option if you want to back up the configuration once at a time. ■ **Daily, Weekly, Monthly** Select the backup frequency and set the date and time that the backup should occur.
Enable Email	Check **Enable email** to send a report of the backup status to the email addresses that you specify. The email report does not include the backup data.
Email Address(es)	Type the recipient email address. Separate multiple email address with commas.
File Transfer Protocol	Transmit the backup by FTP, SFTP, or FTPS. Specify a file path on the remote computer, computer address, and account information.
FTP server IP or Hostname	Type the FTP server IP address or host name.
FTP Username	Type the FTP user name.
FTP Password	Type the FTP password.
FTP Directory	Type the FTP directory to store the backup files. The FTP directory refers the directory relative to the base directory of the FTP user.

5 Click **Save** to create a new schedule.

Restoring backups

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 can restore a backup file of the same version or an older version than the

version that runs on the appliance. For example, if an appliance runs version 5.1, you can restore a backup of version 5.0 or 5.1. However, on an appliance that runs version 5.0, you cannot restore a backup of version 5.1.You can restore from a manual backup file or scheduled backup file.

See "Cross-model backup and restore compatibility" on page 164.

The IP address may optionally be restored. For example, if the backup file was created on a different appliance, you do not want to have both appliances use the same IP address.

See "Backup file contents" on page 165.

See "About backing up and restoring the Symantec Web Gateway configuration" on page 164.

When you upload a custom certificate, it is encrypted with an appliance identification and a secret key that is specific to that appliance. When you backup Symantec Web Gateway, the backup file contains this encrypted data. If you restore the backup on a different appliance, Symantec Web Gateway is not able to read the encrypted data because the appliance identification is different. Therefore, you must upload the custom certificate on the new appliance after you restore the backup.

To restore backups

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 after initial installation" on page 66.

   See "Running the setup wizard" on page 48.

2. Next to **Restore Settings From File**, click **Browse**.
3. In the dialog box, browse to the backup file and click **Open**.
4. Click **Restore**.
5. Click one or more of the following options on the **Restore Option** page:

Network, Operating mode, Proxy	Check **Network, operating mode and proxy configuration** to restore from the backup file. Uncheck **Network, operating mode and proxy configuration** not to restore from the backup file and retain the original configuration.

Central Management	Check **Central Management** to restore the Central Management configuration tab from the backup file. Uncheck **Central Management** not to restore from the backup file and include the original configuration.
No options selected	If none of the options are selected, the following configuration settings are restored: ■ Alerts ■ Appliance Name ■ Servers ■ Email ■ Syslog ■ SNMP ■ Authentication LDAP ■ Time Zone ■ Modules ■ Reputation ■ Client Remediation ■ Security ■ Reports Configuration ■ Blacklist ■ End User Page ■ Policy and Service ■ Whitelist ■ Update ■ Authentication NTLM ■ Authentication Radius ■ Saved Report ■ Scheduled Backup

6 Click **Restore** to start the restore process. A restore warning message appears.

7 Click **OK** to continue the restore process or click **Cancel** to cancel the restore.

The restore process message appears at the bottom of **Restore Option** page. The appliance restarts after the restoration process successfully completes.

8 In case of a configuration mismatch or any incompatible setting, select one of the following options in the dialog box that Symantec Web Gateway displays:

OK	Saves the restored setting with accepted errors.
Cancel	Reverts back to the original settings. Reverts back to the original settings if Symantec Web Gateway detects an error during the restoration process. When Symantec Web Gateway detects an error, a confirmation dialog lists all of the detected errors. You can determine whether to accept the errors and complete the restoration or revert to the original settings.

9 After the restore is complete, check the settings throughout the Web GUI to ensure that they are appropriate.

Enabling and disabling remote assistance

Technical Support needs remote access to Symantec Web Gateway to troubleshoot several issues on the Symantec Web Gateway. When you contact Technical Support, you may be requested to enable remote assistance. You can configure the duration for which you want remote assistance to be enabled.

Note: Symantec recommends that you disable Remote Assistance unless Technical Support requests you to enable the option.

To enable remote assistance

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

2 Next to **Remote Assistance**, click **Click here** to enable remote assistance.

When you enable remote assistance, the case number is displayed on the Web GUI.

3 Check **Automatically close session after hours** to configure the duration after which you want to disable remote assistance.

To disable remote assistance

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

2 Next to **Remote Assistance**, click **Click here** to disable remote assistance.

Uploading diagnostic files

Symantec Web Gateway lets you upload diagnostic files to Symantec Threat Center. Technical support uses these files to analyze any issue that you encounter with Symantec Web Gateway. You can upload diagnostics files when you do not want to Technical Support to remotely access Symantec Web Gateway.

To upload diagnostic files

1. In the Web GUI, click **Administration > Configuration > Maintenance**.
2. Under **Remote Assistance**, click **Upload Diagnostic Files**.

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 have to run the setup wizard again.

If you create a backup for an appliance, you can restore on the same appliance or different appliance depends upon the matrix from backup file. Restore the appliance from backup file after running the setup wizard.

See "About backing up and restoring the Symantec Web Gateway configuration" on page 164.

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" on page 48.

   See "Running the setup wizard for initial installation of a Central Intelligence Unit" on page 216.

Restarting and turning off the Symantec Web Gateway appliance

Before you turn off or restart the Symantec Web Gateway appliance, there are several services that must stop. You can use the **Reboot** and **Shutdown** options to ensure that these services are stopped and the appliance is shut down gracefully.

To restart the Symantec Web Gateway appliance

1. In the Web GUI, click **Administration > Configuration > Maintenance**.
2. Next to **Reboot Appliance**, click **Reboot**.

To turn off the Symantec Web Gateway appliance

1. In the Web GUI, click **Administration > Configuration > Maintenance**.
2. Next to **Shut Down Appliance**, click **Shut Down**.

Configuring incident history

Symantec Web Gateway generates events for several activities that happen on the Web Gateway. The events and incidents history is stored on the database. When you view any report, Symantec Web Gateway uses these events to generate the data. However, when the number of events on the database is high, the performance of the appliance may degrade. For example, the time that is taken to generate reports is high.

You can configure the number of days for which Symantec Web Gateway retains the incident history on the database. You can also specify the maximum number of events that Symantec Web Gateway stores on the database.

To configure the number of days for which Symantec Web Gateway retains the incident history

1. In the Web GUI, click **Administration > Configuration > Maintenance**.
2. Next to **Incident History**, in the **Keep incident history for days** text box enter the number of days.

   Note that when you enter zero, Symantec Web Gateway retains all history.
3. Click **Change**.

To configure the number of events that Symantec Web Gateway stores on the database

1. In the Web GUI, click **Administration > Configuration > Maintenance**.
2. Under **Incident History**, in the **Keep a maximum of events** text box enter the maximum number of events.

   Note that when you enter zero, Symantec Web Gateway does not delete any event.
3. Click **Change**.

To delete incidents generated before a specific date

1. In the Web GUI, click **Administration > Configuration > Maintenance**.
2. Under **Incident History**, in the **Delete all incidents detected on and before** text box enter the date.
3. Click **Delete**.

Testing ports connectivity

You can test connectivity the of the LAN, WAN, and Management ports from the Web GUI.

To test the Management port

1. In the Web GUI, click **Administration > Configuration > Maintenance**.
2. Next to **Test Ping**, enter the IP address of any computer on the same network as that of the Management port.
3. Click **Test Management Port**.

To test LAN or WAN port

1. In the Web GUI, click **Administration > Configuration > Maintenance**.
2. Next to **Test Ping**, enter the IP address of any computer on the same network as that of the LAN or WAN port.
3. Click **Test LAN/WAN Port**.

Testing NTP server connectivity

You can check the connection from Symantec Web Gateway to the NTP server from the Web GUI.

Note: Ensure that you specify a valid NTP server in the **Administration > Configuration > Time** page.

To test NTP server connectivity

1. In the Web GUI, click **Administration > Configuration > Maintenance**.
2. Next to **Test Time Server**, click **Test**.

Testing mail server settings

You can generate a test email to ensure that you receive any alerts or reports that Symantec Web Gateway generates.

To test mail server connectivity

1. In the Web GUI, click **Administration > Configuration > Maintenance**.
2. In the **Test Email** text box, enter the email address.
3. Click **Test**.

   Symantec Web Gateway generates a test email that contains the results of the email test.

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 after initial installation" on page 66.

To reset the Web GUI password

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

   Symantec Web Gateway emails the Web GUI password 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, menu-driven interface. Many of the Web GUI settings are available in the Serial Console.

Table 7-6 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, ports, and indicators on the Symantec Web Gateway appliance" on page 43.
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 logon name and password	By default, the logon name and password for console access is as follows: ■ Logon name: `admin` ■ Password: `admin1!`

If you connect the cable and properly configure the terminal emulation software, Symantec Web Gateway displays a logon 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.

About traffic capture

Symantec Web Gateway lets you capture traffic on your network. The information that is captured helps you troubleshoot any issues that are related to network traffic. Also, this information is useful when you contact technical support in case of a critical problem with the Symantec Web Gateway software or appliance. You can capture network traffic by using the Traffic Capture option under the **Maintenance** tab on the **Administration > Configuration** page.

Note: Traffic Capture is available on Symantec Web Gateway 8450, 8490, and 84V (virtual edition) appliance models only. The device must not be a Central Intelligence Unit.

Warning: Enabling the Traffic Capture option may affect the performance of Symantec Web Gateway.

See "Enabling and disabling network traffic capture" on page 178.

When you enable Traffic Capture, Symantec Web Gateway captures the network packets and stores them in files on your disk. Based on the port from which network packets are captured, Symantec Web Gateway creates separate files for each type of port that are called capture files. For example, the traffic that is captured from the LAN port is available in the capture file named lan.pcap00.

See "Viewing the network traffic capture files" on page 178.

By default, when the number of capture files exceeds the maximum number, the network traffic capture process stops. To ensure that the traffic capture process does not stop, you can configure Symantec Web Gateway to reuse the same files to capture network traffic.

See "Configuring the usage of network capture files" on page 179.

Note: The network capture terminates during a system restart or a software update. You must manually restart the traffic capture process after system restart or a software update.

When you enable Traffic Capture, Symantec Web Gateway captures traffic from all the IP addresses on your network. However, you can configure Symantec Web Gateway to capture network traffic from specific IP addresses. For example, if

there are 20 IP addresses on your network, you can capture network traffic from 10 of them. You can also configure Symantec Web Gateway to capture traffic from any one of the 20 IP addresses.

See "Filtering network traffic capture" on page 180.

Enabling and disabling network traffic capture

Symantec Web Gateway lets you capture traffic on your network. To capture network traffic, you must enable the traffic capture process. When you no longer want Symantec Web Gateway to capture network traffic, you can disable the traffic capture process.

See "About traffic capture" on page 177.

Note: Traffic Capture is available on Symantec Web Gateway 8450 and 8490, and 84V (virtual edition) appliance models only. The device must not be a Central Intelligence Unit.

Warning: When you enable the Traffic Capture, performance of the Web Gateway may be affected.

To enable network traffic capture

1. In the Web GUI, click **Administration > Configuration > Maintenance**.
2. Under **Traffic Capture**, click **Start Capture**.

To disable network traffic capture

1. In the Web GUI, click **Administration > Configuration > Maintenance**.
2. Under **Traffic Capture**, click **Stop Capture**.

Viewing the network traffic capture files

When you enable traffic capture, Symantec Web Gateway captures the network packets and stores them in files on your disk. Based on the port from which network packets are captured, Symantec Web Gateway creates separate files for each type of port that are called capture files. For example, the traffic that is captured from the LAN port is available in the capture file named lan.pcap00.

See "Configuring the usage of network capture files" on page 179.

Note: You must disable the network capture process before you download and view the capture files.

See "Enabling and disabling network traffic capture" on page 178.

Table 7-7 lists the information that is related to the names of the capture files, capture file size, and the number of capture files for different ports.

Table 7-7 Capture file information

Port	Maximum number of capture files	Name of the capture file	Maximum size of the capture file
Management	20	mgmt.pcap00 to mgmt.pcap19	2 MB
Monitoring	20	mon.pcap00 to mon.pcap19	20 MB
LAN	20	lan.pcap00 to lan.pcap19	20 MB
WAN	20	wan.pcap00 to wan.pcap19	20 MB
LAN2	20	lan2.pcap00 to lan2.pcap19	20 MB
WAN2	20	wan2.pcap00 to wan2.pcap19	20 MB

To view the network capture files

1. In the Web GUI, click **Administration > Configuration > Maintenance**.
2. Under **Traffic Capture**, click **Stop Capture** if the network capture process is enabled.
3. Click **Download Capture Files**.
4. Click **Save** to save the .ZIP file on your disk.

Configuring the usage of network capture files

When you enable Traffic Capture, Symantec Web Gateway captures the network packets and stores them in files on your disk. Based on the port from which network packets are captured, Symantec Web Gateway creates separate files for each type of port that are called capture files. For each port, the maximum number of capture files that Web Gateway creates is 20. When the number of capture files exceeds the maximum number, the network traffic capture process stops. To ensure that the traffic capture process does not stop, you can configure Symantec Web Gateway to reuse the same files to capture network traffic.

See "Viewing the network traffic capture files" on page 178.

To configure the usage of network capture files

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

2 Under **Traffic Capture**, check **Rotate Capture Files**.

You can view the **Rotate Capture Files** check box only when the traffic capture process is disabled. If the traffic capture process is already enabled, click **Stop Capture** to disable the process.

Filtering network traffic capture

Symantec Web Gateway by default captures traffic from all the IP addresses on your network. However, you can configure Symantec Web Gateway to capture network traffic from specific IP addresses. The **Filter Traffic Capture** option lets you specify the IP addresses from which you want to capture network traffic.

See "Enabling and disabling network traffic capture" on page 178.

Note: The filter options that you specify do not apply to the Management port.

To filter network traffic capture

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

2 Under **Traffic Capture**, check **Filter Traffic Capture**.

You can view the **Filter Traffic Capture** check box only when the traffic capture process is disabled. If the traffic capture process is already enabled, click **Stop Capture** to disable the process.

3 In the **Select Operator** row, select one of the following:

AND	To capture network traffic from any two IP addresses that you specify
OR	To capture network traffic from any of the IP address that you specify The maximum number of IP adresses that you can specify is 10.

4 In the **Filter IP Address(es)** text box, specify the IP addresses separated by commas.

5 Click **Start Capture**.

Chapter 8

Reports

This chapter includes the following topics:

- About reports
- Exporting a report to a .csv file
- Scheduling automatic reports
- Monitoring user browse time

About reports

Symantec Web Gateway lets you generate reports to monitor the following:

- 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, and so on.

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 or IP address instead.

See "About Active Directory integration" on page 189.

Table 8-1 Overview of reports

Reports	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.
Enterprise Summary	Lists the summary of activities that Symantec Web Gateway detects based on hostname. If you configured Microsoft Active Directory, the report lists the summary based on LDAP username.
Enterprise Summary (Browse Time)	Lists the time that users spend Web browsing. Located on the **Enterprise Summary** report. You must enable the browse time recording to activate this report. See "Enabling URL filtering, Internet program monitoring, and other features" on page 60.
Custom Reports	Lets you create your own reports based on the time period and various event statistics. You can run full queries of report log data.
Infected Clients	Lists all the computers that malware has infected.
Infections by Spyware Name	Lists all the 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.

Table 8-1 Overview of reports *(continued)*

Reports	Description
Potential Attacks	Lists all potential attacks. The following potential attack reports are available: ■ **Spyware** The **Spyware** report lists the attempts by remote systems to access an infected computer or send a malicious network element such as a worm. ■ **IP Scanning** The **IP Scanning** report lists the IP addresses that attempted to scan IP address at your site. ■ **Spamming** The **Spamming** report lists the IP address that attempted to send spam within your site.
Infection Sources	Lists all the monitored or blocked URLs, spyware Web sites, and spyware file downloads attempted by users at your site. It 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 the network transmissions of these applications were detected.
Web Destinations	Lists all attempts to contact the monitored or blocked Web sites by users at your site. This report also lists the number of computers and the number of times that users attempted to access the Web destinations.
Botnets	Lists the detected activity that may indicate a botnet.

Table 8-1 Overview of reports *(continued)*

Reports	Description
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.
Alerts	Lists the alerts that Symantec Web Gateway generates when it detects infections or when certain system events occur. Alerts are triggered based on the infection count, severity, or based on the IP address or host name of the infected PC.
Search by Hostname	Lists the reports by specifying the Host name of the computers available in the Active Directory network.
Search by User Name	Displays the report statistics by Active Directory user name.
Search by Department	Lets you search reports by department as configured in the Active Directory. You can also verify that your department is configured in the Organization directory or not.
Search by IP Location	Lets you search reports by IP address, and it lists the geographical location or country of origination of the host computer in the network.

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 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 appears, 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 on 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 the report that is emailed or saved to the remote computer. **Report Name** and **Report Description** appear 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. The most recent entries appear.
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. If you select this option, specify the following information: ■ **Email Address(es)** Type a valid email address. You must separate multiple email addresses with a comma or a line break. ■ **Email Format** Check the format that you want to use. You can only select one option.

File Transfer

Delivers the report by FTP, SFTP, or FTPS.

For file transfers, you must also specify the following information:

- **FTP Filename**
  Type a file path on the remote computer.
  Symantec Web Gateway adds a timestamp suffix to the file path. Do not specify a computer address that starts with a URI such as: `ftp://`
- **FTP Server IP or Hostname**
  Type the server IP address or host name.
- **FTP Username**
  Check **Anonymous** if you want to use anonymous FTP.
- **FTP Password**
  Type the FTP password.
- **FTP Directory**
  Type the FTP directory.

7 Click **Save**.

Monitoring user browse time

Symantec Web Gateway can record the approximate amount of time that each computer or user spends in the Web browser. You must configure Active Directory integration to display the browse time by user. Otherwise, Symantec Web Gateway displays the browse time by computer.

See "About Active Directory integration" on page 189.

To ensure that your browse time report truly reflects meaningful user browse times, you can specify a minimum threshold and inactivity threshold. For example, you can set a threshold to omit from the report instances in which a user browses the Web less than 5 minutes. You can also omit from the report instances in which a user is inactive in the Web browser more than 3 minutes.

Table 8-2 describes how you can configure the threshold and sensitivity to determine how Symantec Web Gateway records browse time.

Table 8-2 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.	The total browse time that is recorded is 0 minutes. The 3-minute sensitivity that is 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.	The total browse time that is recorded is 6 minutes. Between 9:00 and 9:06 is counted as 6 minutes.

You can review user browse time reports on the **Reports > Enterprise Summary > Browse Time** page.

See "Exporting a report to a .csv file" on page 184.

Note: You require URL filtering license to monitor user browse time.

To monitor user browse time

1. In the Web GUI, click **Administration > Configuration > Modules**.
2. Under **Browse Time Report Configuration**, check **Record browse time**.
3. In the **Threshold** field, type the threshold.

   User browse times that are less than the threshold do not appear in the browse time report.

   The default value is 5 minutes
4. In the **Sensitivity** field, specify the sensitivity.

   When a user is inactive more than the minutes that you specify, Symantec Web Gateway omits this time from the browse time report.

   The default value is 3 minutes.

Chapter 9

Configuring Active Directory integration

This chapter includes the following topics:

- About Active Directory integration
- Active Directory compatibility with Symantec Web Gateway
- Comparison of Active Directory integration with a domain controller and NTLM
- Configuring Active Directory integration by using DCInterface
- Configuring Active Directory integration with NTLM
- Refreshing Active Directory user data in reports

About Active Directory integration

You can configure Symantec Web Gateway to integrate with Microsoft Active Directory through LDAP. Active Directory is a Microsoft product that stores user account information and provides authentication on Windows networks.

The integration with Active Directory provides the following benefits:

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

See "Active Directory compatibility with Symantec Web Gateway" on page 190.

You can use a Central Intelligence Unit to configure the Active Directory Integration on managed appliances. You can also configure each Symantec Web Gateway directly. You can configure Symantec Web Gateway to obtain user login

information through NTLM authentication or by installing Symantec's Domain Controller Interface software (DCInterface) on an Active Directory server.

See "Comparison of Active Directory integration with a domain controller and NTLM" on page 190.

See "Configuring Active Directory integration by using DCInterface" on page 193.

See "Configuring Active Directory integration with NTLM" on page 200.

See "Refreshing Active Directory user data in reports" on page 212.

Active Directory compatibility with Symantec Web Gateway

Table 9-1 lists the versions of Microsoft Windows with which Symantec Web Gateway can interface.

Table 9-1 Supported Active Directory versions

Windows version	Physical installation	Virtual installation
Windows 2003	Yes	Yes, VMware
Windows 2008	Yes	Yes, VMware

Global catalogs are supported for both methods of Active Directory integration available for Symantec Web Gateway:

- Symantec Domain Controller Interface
- NTLM
  The global catalog server is only required in a multi-domain forest deployment.

See "About Active Directory integration" on page 189.

Comparison of Active Directory integration with a domain controller and NTLM

You can configure Active Directory integration with Symantec's Domain Controller Interface software (DCInterface) or by using NTLM. The method appropriate for your environment depends on the number of users at your site and other considerations.

Note: Do not attempt to configure Active Directory integration with both DCInterface and NTLM. The policies do not work correctly if you configure both DCInterface and NTLM.

See "About Active Directory integration" on page 189.

Table 9-2 describes the differences between DCInterface and NTLM.

Table 9-2 Comparing Active Directory integration with a Symantec Domain Controller Interface and NTLM

Consideration	Domain Controller Interface	NTLM
User identification method	The Symantec Domain Controller Interface 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	There are no scalability issues.	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. If the setting is 0, then NTLM authenticates continuously.
Configuration changes required outside of Symantec Web Gateway	You must install Symantec Domain Controller Interface software on each domain Controller Interface 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 9-2 Comparing Active Directory integration with a Symantec Domain Controller Interface and NTLM *(continued)*

Consideration	Domain Controller Interface	NTLM
User experience	Transparent to users. No special logon for Symantec Web Gateway is required.	Usually transparent to users who run Internet Explorer on Microsoft Windows if you check the **Use Interface Name for NTLM Authentication** checkbox on the **Administration > Configuration > Authentication** tab. In some cases Outlook or the Web browser displays a dialog box that requires users to log on. Firefox displays the authentication window in all cases. For 407 authentication, the authentication window does not appear if the domain user logs in. See "Ensuring compatibility with NTLMv1 and NTLMv2" on page 206.
Speed of recognition for reporting purposes	Users are identified immediately upon logon.	For inline traffic, 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. For proxy traffic, users are identified immediately upon login.

Configuring Active Directory integration by using DCInterface

Table 9-3 describes the steps to configure Active Directory integration by using DCInterface.

Table 9-3 Steps to configure Active Directory integration by using DCInterface

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.
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 194.
Step 3	Install the Symantec Domain Controller Interface.	Download the Symantec Domain Controller Interface from the Symantec Web Gateway Web GUI and install it. See "Installing the Symantec Domain Controller Interface software" on page 196.
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 198.
Step 5 (Optional)	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 198.

Table 9-3 Steps to configure Active Directory integration by using DCInterface *(continued)*

Step	Action	Description
Step 6	Start the Symantec Domain Controller Interface service.	Start the Symantec Domain Controller Interface in Services. See "Starting the Symantec Domain Controller Interface" on page 199.
Step 7	Test the Active Directory integration.	If the Active Directory integration works correctly, user names display in the Symantec Web Gateway Web GUI reports when you create at least one policy of any type.

Configuring Active Directory integration

You specify your Active Directory configuration in the Symantec Web Gateway 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 Symantec Web Gateway 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. Check **Use LDAP to identify end users**.
3. 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 plain text.
- **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.

Sync Frequency	The number of hours that Symantec Web Gateway considers a user's Active Directory attributes (such as workgroup association, email address, phone number) valid. After this period, a user's Active Directory attributes are considered stale, and Symantec Web Gateway automatically refreshes them through an LDAP query to the Active Directory. The default is 168 hours (one week).

4 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 administration 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**

5 Click **Test** for the type of authentication that you want to perform (HTTP 401 or HTTP 407).

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

6 Click **Save**.

Installing the Symantec Domain Controller Interface software

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 must install Symantec Domain Controller Interface software on each domain Controller Interface that users log on to.

Note: The domain controller must run on Windows Server 2008/2003. Symantec Web Gateway supports 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 198.

Configuring the Symantec Domain Controller Interface

After installing the Symantec Domain Controller Interface, you must configure it.

See "Installing the Symantec Domain Controller Interface software" on page 196.

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 199.

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 198.

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.exe` 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**.

Configuring Active Directory integration with NTLM

When you configure Active Directory integration with NTLM, Symantec Web Gateway communicates with user browsers to perform the following tasks:

- Extracts an Active Directory name
- Correlates the user's Active Directory name with the user's IP address
- Reinforces user authentication to the domain controllers when the user's credentials expire

Table 9-4 describes the steps to configure Active Directory integration with NTLM.

Table 9-4 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 202.
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 202.
Step 3	Specify your NTLM settings.	Specify your Active Directory and NTLM settings in the Web GUI. See "Configuring Active Directory integration" on page 194. See "Configuring Symantec Web Gateway to integrate Active Directory with NTLM" on page 203.
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 205.
Step 5	If necessary, make Outlook, Windows Vista, and Windows 7 or other operating system changes.	You may need to make changes to Outlook, Windows Vista and Windows 7, or other operating systems to ensure compatibility with NTLM. See "Ensuring compatibility with NTLMv1 and NTLMv2" on page 206.

Table 9-4 Steps to configure Active Directory integration with NTLM *(continued)*

Step	Action	Description
Step 6	Test the Active Directory integration with NTLM.	If the Active Directory integration works correctly, user names appear in the Web GUI reports if you have an NTLM authentication policy and a user-based policy. See 5 on page 196.

Specifying the Management Interface Name in Symantec Web Gateway

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

See "DNS change needed for NTLM" on page 202.

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.

This task does not apply for proxy network configurations.

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 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 9-5 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 9-5 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 Symantec Web Gateway to integrate Active Directory with NTLM

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

See "Configuring Active Directory integration with NTLM" on page 200.

See "Web browser changes needed for NTLM" on page 205.

To configure Symantec Web Gateway to integrate 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.

A secondary domain controller is optional if you want a redundant server.

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 202.
- Uncheck the box if you do not want to modify DNS. You must modify user browsers.
  See "Web browser changes needed for NTLM" on page 205.

The default is unchecked but checked (with proper configuration) is recommended.

Authentication TTL

Type the time between authentication requests from Symantec Web Gateway to the domain controller. 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. If you use an enforce authentication policy, users see an error page. If you use 407 authentication, users see a proxy error page. 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 142.

Use LDAP Credentials for Domain Controller	If you select this option, specify the **Domain Controller User Name** and the **Domain Controller Password** in the corresponding boxes. Use the administrator password. If you use a proxy network configuration and 407 authentication, Symantec Web Gateway does not save these login credentials. Therefore, an error occurs if you uncheck this box and use different credentials from those that you specify for the **Primary and Secondary Domain Controller**.

3 Click **Test** beside the type of authentication that you want to perform (HTTP 401 or HTTP 407).

The results of the test appear 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.

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.

The Symantec Web Gateway proxy supports basic 401 authentication from Web sites. Web sites that require NTLM 401 authentication or a higher level of 401 authentication are unsupported.

Table 9-6 describes cases in which you must configure user Web browsers.

Table 9-6 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 users' browsers.
Web browsers other than Microsoft Internet Explorer (for example, 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 NTLMv1 and NTLMv2

Some operating systems require configuration changes to work with NTLMv1 or NTLMv2.

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 user lockout 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 205.

See "Configuring NTLM user authentication behavior" on page 142.

Table 9-7 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 NTLMv1 and NTLMv2 compatibility for Windows Vista and Windows 7" on page 207.
Operating systems that Microsoft does not sell, 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 NTLMv1 and NTLMv2 compatibility for Outlook 2003 and Windows XP SP2" on page 208.
Configuring NTLMv2 compatibility for Windows XP	You should configure NTLMv2 compatibility for Windows XP to use the NTLMv2 session security. See "Configuring NTLMv2 compatibility for Windows XP" on page 209.

Configuring NTLMv1 and NTLMv2 compatibility for Windows Vista and Windows 7

Windows Vista and Windows 7 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 NTLMv1 and NTLMv2" on page 206.

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 and Windows 7 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 and Windows 7

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 NTLMv1 and NTLMv2 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 hot fix 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 hot fix 895948 from Microsoft.
  - Install Windows XP SP3, which contains hot fix 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.

Configuring NTLMv2 compatibility for Windows XP

Configuring NTLMv2 compatibility for Windows XP allows your Windows clients to only use NTLMv2 authentication and refuse other security. If you change to this high level of security, it is not easy to connect to other Windows computers without equivalent security settings.

See "Ensuring compatibility with NTLMv1 and NTLMv2" on page 206.

To configure NTLMv2 compatibility for Windows XP

1 Click **Start > Settings > Control Panel**.

2 Click the **Performance and Maintenance** category.

3 Click **Administrative Tools**.

4 Click **Local Security Policy > Local Policies > Security Options > Network Security: LAN Manager authentication level**.

5 Click **Send LM& NTLM - use NTLMv2 session security if negotiated**.

6 Click **OK**.

7 Click **Yes** to confirm the change.

8 Restart your computer.

Setting up the ignore authentication in NTLM v2 client

Before you use NTLM v2 client to configure the ignore authentication, you should set up the following initial configuration in Symantec Web Gateway.

To set up the ignore authentication in NTLM v2 client

1 To enable the HTTPS proxy, perform the following tasks:

- In the Web GUI, click **Administration > Configuration > Proxy**.
- Check **Enable HTTP/S Proxy**.

- Click **Save**.

2 To enable LDAP and NTLM authentication, perform the following tasks:

- In the Web GUI, click **Administration > Configuration > Authentication**.
- Check **Use LDAP to identify end users**.
- Check **NTLM Authentication**.
- Click **Save**.

3 To enable user authentication, perform the following tasks:

- In the Web GUI, click **Policies > Configuration**.
- Click **Create a New Policy**.
- Type the policy name.
- Check the **User Authentication**.
- Select **Enforce Authentication** from the list.
- Click **Save**.

See "Ignoring authentication when you use the NTLM v2 client to configure the whitelist" on page 210.

Ignoring authentication when you use the NTLM v2 client to configure the whitelist

You can use NTLM v2 Web browser client to configure Symantec Web Gateway with the inline proxy network configuration or proxy network configuration to ignore authentication of the whitelisted exception Web sites. You should configure your Web browser to access Internet through Symantec Web Gateway proxy and the required proxy settings can be done from a PAC file. The PAC file contains the whitelisted exception Web sites and it can be accessed from your local computer or from your remote computer.

See "Sample proxy auto-configuration (PAC) file" on page 211.

To ignore authentication when you use the NTLM v2 client to configure the whitelist

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

2 Click **Add a Whitelist Entry**.

3 In the **Hostname/IP or IP/mask** field, type the host name.

4 Check **Whitelist** and **Ignore Authentication**.

5 Click **Save**.

6 Configure your Web browser that uses the PAC file and access the Internet through Symantec Web Gateway proxy.

For more information on how to configure proxy using Internet Explorer and Mozilla Firefox browser, refer the browser documentation.

The PAC file contains the following list of whitelisted exception Web sites:

- windowsupdate.microsoft.com
- update.microsoft.com
- c.microsoft.com
- download.windowsupdate.com
- www.update.microsoft.com
- download.microsoft.com
- crl.microsoft.com
- symantecliveupdate.com

7 From the Web browser client, access the whitelisted Web site.

The whitelisted exception Web site appears, and the NTLM authentication pop-up does not appear.

See "Setting up the ignore authentication in NTLM v2 client" on page 209.

Sample proxy auto-configuration (PAC) file

Use a proxy auto-configuration (PAC) file to selectively drive HTTP traffic through either the inline bridge or the HTTP/S proxy path of the Symantec Web Gateway.

When you configure Internet Explorer to use a PAC file, it caches the proxy server information for each host on a host-by-host basis regardless of whether you use HTTP or HTTPS. The result is that some Web sites may be temporarily inaccessible when you switch between HTTP and HTTPS.

To resolve this issue, disable automatic proxy caching in the registry file or group policy settings.

For more information, on the Internet, go to the following URL:

http://support.microsoft.com/kb/271361

The following is sample content for a PAC file:

```
function FindProxyForURL(url, host)
{
// variable strings to return
```

```
var proxy_yes = "PROXY 10.130.16.60:8082";
var proxy_no = "DIRECT";
if (shExpMatch(url, "http://finance.yahoo.com*")) { return proxy_no; }
if (shExpMatch(url, "http://news.yahoo.com*")) { return proxy_no; }
if (shExpMatch(url, "http://www.google.com*")) { return proxy_no; }
if (shExpMatch(url, "http://video.google.com*")) { return proxy_no; }
if (shExpMatch(url, "http://zh-cn.facebook.com*")) { return proxy_no; }
if (shExpMatch(url, "http://10.130.16.150/*")) { return proxy_no; }
// Proxy anything else
return proxy_yes;
```

See "Ignoring authentication when you use the NTLM v2 client to configure the whitelist" on page 210.

Refreshing Active Directory user data in reports

You can refresh individual user information from LDAP to display the latest information from LDAP in user reports. By default, the synchronization frequency between Symantec Web Gateway and LDAP is 168 hours. After every 168 hours, Symantec Web Gateway synchronizes with LDAP for the updated user information.

To refresh Active Directory user data in reports

1. In the Web GUI, click **Custom Reports**.
2. In the **Custom Reports**, check for the data availability and for valid LDAP user name.
3. In the **Login Name or Fullname** column, click the user.

   The report for the selected user name appears.
4. Click **Refresh**.

   The report for the selected user refreshes and displays the latest information.

See "About Active Directory integration" on page 189.

Chapter 10

Configuring a Central Intelligence Unit to manage multiple appliances

This chapter includes the following topics:

- About centralized management using a Central Intelligence Unit
- Installing a Central Intelligence Unit
- Running the setup wizard for initial installation of a Central Intelligence Unit
- Connecting a Central Intelligence Unit to the network
- Configuring appliances to accept management by a Central Intelligence Unit

About centralized management using a Central Intelligence Unit

You can configure any Symantec Web Gateway appliance 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.

Note: You can only deploy one Central Intelligence Unit to manage a group of appliances. You cannot configure a Central Intelligence Unit to act as a failover appliance to another Central Intelligence Unit.

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 any operating mode other than Central Intelligence Unit. When you configure an appliance as a Central Intelligence Unit, that appliance cannot function as a Symantec Web Gateway.

See "Installing a Central Intelligence Unit" on page 214.

Table 10-1 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. For example, Central Intelligence Unit helps you to create policies centrally and apply them to multiple Symantec Web Gateway appliances.
Centralized reporting	View consolidated reports from all managed appliances.

Table 10-2 describes the frequency of data exchange between a Central Intelligence Unit and managed appliances.

Table 10-2 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	By default, every five minutes when there is new data or modified data on the managed appliance See "Configuring appliances to accept management by a Central Intelligence Unit" on page 219.

Installing a Central Intelligence Unit

Table 10-3 describes the steps to install a Central Intelligence Unit.

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 172.

Table 10-3 Steps to install a Central Intelligence Unit

Step	Action	Description
Step 1	Install and configure appliances for the Central Intelligence Unit to manage.	Install and configure the appliances that you plan to have the Central Intelligence Unit manage. 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 "Installing Symantec Web Gateway" on page 46.
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 47.
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 47.
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 216.
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 219.
Step 6	Review the network ports that Symantec Web Gateway uses.	Open ports between Central Intelligence Unit and managed appliances. See "Ports and settings that Symantec Web Gateway uses" on page 37.

Table 10-3 Steps to install a Central Intelligence Unit *(continued)*

Step	Action	Description
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 219.

See "About centralized management using a Central Intelligence Unit" on page 213.

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 management port, you can run the setup wizard. This procedure describes how to configure an appliance as a Central Intelligence Unit.

See "Installing a Central Intelligence Unit" on page 214.

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 runs 5.0, then all managed appliances must run 5.0 also. You must also synchronize the time between Symantec Web Gateway and the Central Intelligence Unit.

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.
2. On the computer that is connected to the management 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, do the following tasks:
   - In the **Company Name** box, type the name of your organization.
   - Click **Browse** and locate your license file.

- Click **Next**.

If you do not install a license now, there is a two week grace period. During this time the product runs as if the Symantec Web Gateway license were 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.
Reenter password	Type the password again to verify its accuracy.
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:

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. It 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.

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 the Central Intelligence Unit is installed.

10 Click **Finish**.

11 The appliance restarts.

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

See "Post-installation tasks" on page 52.

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 management 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.

See "Connections, ports, and indicators on the Symantec Web Gateway appliance" on page 43.

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 "Installing a Central Intelligence Unit" on page 214.

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

See "Installing Symantec Web Gateway" on page 46.

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 version5.0, then all managed appliances must be running version 5.0 also. You must also synchronize the time between Symantec Web Gateway and the Central Intelligence Unit.

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 host name 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 the **Management Password** field, type the management password that you specified on the Central Intelligence Unit.
5. In the **Upload Frequency** field, 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

A

Active Directory 189
  See also domain controller
  See also NTLM
  compatibility with Symantec Web Gateway 190
  configuring for remote access 198
  configuring integration 194
  controlling authentication with NTLM 142
  creating policies with 92, 101, 189
  integrating with DCInterface 193
  integrating with domain controller 189–190, 194, 196, 198
  integrating with NTLM 189–190, 194, 200, 203, 208
  integrating, about 189
  refreshing 212
  report data 156, 181
  specifying the Management Interface name 202
administrative users. *See* system users
after hours, access 140
alerts 63, 162–163
antivirus 13
appliance
  configuring to use Central Intelligence Unit 219
  connections and ports 43
  mounting into a rack 47
  restoring to factory default 172
  supported models 23
application control
  blocking behavior 97
  controlling access 60
  creating policies 111

B

backup 164, 166, 172
blacklist 143, 145
blocking
  after hours 140
  uploads or downloads 145
  using blacklists 143
  using NTLM 142
blocking *(continued)*
  Web sites 118
blocking feedback report 148
blocking mode
  about 26
  creating policies
    Insight reputation-based security 106
    Internet applications 111
    malware 108
    SSL Deep Inspection 107
  installing 48
  testing 64
blocking page 97, 101, 141, 148–149, 152
browse time 60, 187
browser, Web. *See* Web browser
bypass mode
  about 56
  LED indicators 43
  testing 58

C

Central Intelligence Unit
  about 213
  configuring appliances to accept management 219
  connecting to a network 219
  creating roles for system users 157
  installing 48, 214, 216
  integrating with Active Directory 189
  port connections 27
  resetting an appliance 172
  specifying the Management Interface Name 202
centralized management and reporting. *See* Central Intelligence Unit
crossover cable 27, 56
CSV report file 184–185

D

data loss prevention
  availability withSymantec Web Gateway proxy 78

data loss prevention *(continued)*
routing traffic through 87
database updates. *See* updates: database
DCInterface. *See* Symantec Domain Controller Interface
DNS 202
documentation, product 17
domain controller 189–190, 194
See also Active Directory
See also Symantec Domain Controller Interface
Domain Name Server. *See* DNS
downloads
blocking 108, 145
controlling behavior 95
dual homing network configuration
about 24
diagram 30

E

email server 63–64
Embedded URL
about 139
detecting 139
embedded URL 118, 146
end user pages 97, 148–149, 152
ESX/ESXi. *See* virtualization
Ethernet cables 56
Ethernet ports 27
external proxy 19, 64

F

factory default settings, restoring to 172
file downloads. *See* downloads
filtering, URL. *See* URL filtering
FTP proxy
availability withSymantec Web Gateway proxy 78
configuring 89

G

Global Intelligence Network 13

H

help 17
HTTP proxy
availability withSymantec Web Gateway proxy 78
configuring 81
HTTP proxy *(continued)*
routing traffic through DLP server 87
HTTPS proxy
availability withSymantec Web Gateway proxy 78
configuring 81
routing traffic through DLP server 87

I

inline + proxy network configuration
about 24
diagram 30
installing 48
inline network configuration
about 24
blocking downloads 92
creating static routes 62
diagram 30
ensuring Internet connectivity 56
installing 48
port connections 27
Insight reputation-based security
about 103–104
creating policies for 106
installation
Central Intelligence Unit 214, 216
post-installation tasks 52
preinstallation checklist 19
running setup wizard 48
Symantec Web Gateway 46
Symantec Web Gateway Virtual Edition 68
internal networks 59
Internet applications
blocking behavior 97
controlling access 60
creating policies 111
IP addresses 53

L

LAN Ethernet port 27, 43
license 19
LiveUpdate 37

M

malware
categories 113
creating policies 108
quarantining infections 141

Management Interface Name 202
See also NTLM
management port 27, 43
mgmt port. *See* Management port
misclassified URLs
reporting 139
modes, operating. *See* operating modes
monitor port 27, 43
monitoring
uploads or downloads 145
using blacklists 143
Web sites 118
monitoring mode
about 26
creating policies
Insight reputation-based security 106
Internet applications 111
malware 108
SSL Deep Inspection 107
installing 48
testing 64

N

network configurations
about 24
diagrams 30
port connections 27
virtualization, supported 67
networks, internal 59
new features 14
NTLM
adding A records in DNS 202
authentication availability withSymantec Web Gateway proxy 78
compatibility 206–209
configuring ignore authentication 209–210
configuring Web browser 205
controlling authentication 142
integrating with Active Directory 189, 194, 200, 203
specifying the Management Interface name 202

O

operating modes 26
Outlook 2003 208
OVF template 68

P

PAC file 211
password 66, 159, 175
permissions. *See* system users: permissions
policies
about 92
blocking after hours 140
blocking methods 97
configuring download behavior 95
configuring for
Insight reputation-based security 106
Internet applications 111
malware 108
SSL Deep Inspection 107
URL filtering 118
configuring precedence 95
controlling authentication with NTLM 142
integrating with domain controller 190
integrating with NTLM 190
malware categories 113
quarantining infections 141
specifying computers 101
specifying users 101
using Active Directory 189–190
using blacklists 145
using whitelists 143, 146
port span/tap network configuration
about 24
blocking downloads 92
diagram 30
ensuring Internet connectivity 56
installing 48
port connections 27
ports
appliance 27, 43, 56
connecting the appliance 55
used by Symantec Web Gateway 37
post-installation tasks 52
precedence, policy order 95
preinstallation checklist 19
privileges. *See* system users: permissions
proxy. *See* Symantec Web Gateway proxy
proxy network configuration
about 24
installing 48

Q

quarantine 141

R

rack, mounting appliance 47
release notes 161
reports
  about 181
  blocking feedback 148
  exporting to .csv 184
  integrating with Active Directory 189
  refreshing Active Directory 212
  saving 185
  scheduling 185
  specifying mail server for 63
  specifying proxy servers 64
reputation-based security. *See* Insight reputation-based security
reset appliance 172
restore 164, 168, 172
roles. *See* system users: roles

S

Serial Console 176
serial port 43
setup wizard
  Central Intelligence Unit 216
  initial installation 48
  post-installation 66
SMTP 63
SNMP 163
SOCKS proxy
  availability withSymantec Web Gateway proxy 78
  configuring 89
software updates. *See* updates: software
span. *See* port span/tap
spyware. *See* malware
SSL Deep Inspection
  availability withSymantec Web Gateway proxy 78
  comparison to SSL Domain Level Inspection 82
  configuring Symantec Web Gateway proxy 85
  creating policies for 107
  URL and port 37
SSL Domain Level Inspection
  availability withSymantec Web Gateway proxy 78
  comparison to SSL Deep Inspection 82
  configuring Symantec Web Gateway proxy 87
static routes 59, 62
Symantec Data Loss Prevention Server. *See* data loss prevention
Symantec Domain Controller Interface 190
  See also domain controller
  about 189
  configuring 198
  configuring Active Directory integration 190
  installing 196
  moving the DCInterface.exe file 200
  starting 199
  URL and port 37
Symantec RuleSpace
  about 122
  mapping information 134
Symantec Threat Center
  testing connectivity 65
  URL and port 37
Symantec Web Gateway
  accessing the Web GUI 54
  configuring computer access to 47
  ports and URLs 37
  proxy settings 37
  testing
    blocking and monitoring 64
    bypass mode 58
    Threat Center connectivity 65
Symantec Web Gateway proxy
  about 77
  configuring for
    SSL Deep Inspection 85
    SSL Domain Level Inspection 87
  diagram 30
  features 78
  routing traffic through DLP server 87
  Web browser settings 80
Symantec Web Gateway Virtual Edition. *See* virtualization
syslog 163
system requirements 23
system users
  about 156
  creating 159
  creating roles 157
  monitoring activity 160
  permissions 156, 159
  resetting passwords 66, 175
  roles 156
  specifying 49

T

tap. *See* port span/tap
terminal emulation software 176
tests. *See* Symantec Web Gateway: testing
third-party proxy server. *See* external proxy
Threat Center
    testing connectivity 65
    URL and port 37
threats 13
traffic capture
    about 177
    disabling 178
    enabling 178
    filtering 180
    viewing capture files 178

U

updates
    database 161
    software 161
upgrade
    product 133
URL filtering
    about 92
    after hours 140
    categories 122
    creating policies 118
    enabling 60
    using blacklists 143
URL, embedded 118, 146
URLs, Symantec Web Gateway 37
USB ports 43
users, system. *See* system users

V

variables, end user pages 152
virtual edition. *See* virtualization
virtual network adapters 68
virtualization
    about 67
    adding LAN network virtual switches 73
    configuring the virtual switch 75
    installing 68
    network virtual switch configuration 73
    supported network configurations 67
    system requirements 72
virus. *See* antivirus
VMware
    adding LAN network virtual switches 73
    configuring the virtual switch 75
    snapshot 67
    system requirements 72
vSphere. *See* virtualization

W

WAN Ethernet port 27, 43
Web 2.0 13
Web browser
    blocking behavior 97
    compatibility with NTLM 206
    configuring for NTLM 205
    controlling downloads 95
    end user pages 148
    Symantec Web Gateway proxy settings 80
    system requirements 23
Web GUI 54, 175
Web sites
    accessing after hours 140
    accessing using whitelists 146
    blocking 143
    creating filtering policies 118
whitelist 60, 146, 210
Windows 7 207
Windows Vista 207
Windows XP 209
Windows XP SP2 208