Installation Guide for Symantec™ Endpoint Protection and Symantec Network Access Control

Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control

Documentation version 11.00.06.00.00

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 Maintenance Programs, you can visit our Web site at the following URL:

www.symantec.com/business/support/

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

- Product release level
- Hardware information
- Available memory, disk space, and NIC information

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

Additional enterprise services

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

Enterprise services that are available include the following:

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

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

www.symantec.com/business/services/

Select your country or language from the site index.

Contents

Section 1

Introduction, requirements, and planning

Chapter 1

Introducing Symantec Endpoint Protection and Symantec Network Access Control

This chapter includes the following topics:

About Symantec Endpoint Protection

Symantec Endpoint Protection combines virus protection with advanced threat protection to proactively secure your computers against known and unknown threats.

Symantec Endpoint Protection protects against malware such as viruses, worms, Trojan horses, spyware, and adware. It provides protection against even the most sophisticated attacks that evade traditional security measures such as rootkits,

zero-day attacks, and spyware that mutates. Symantec Endpoint Protection also lets you maintain fine-grained application and device control. Symantec Endpoint Protection provides multiple layers of protection for your endpoint computing devices.

Your Symantec software may include Symantec Network Access Control. Symantec Network Access Control also uses Symantec Endpoint Protection Manager to install and manage Symantec Endpoint Protection clients and Symantec Network Access Control clients. Symantec Network Access Control ensures that clients are compliant with your organization's security policies before they are allowed access to your network. Symantec Endpoint Protection and Symantec Network Access Control work together but are purchased separately.

See "About Symantec Network Access Control" on page 18.

See "Components of Symantec Endpoint Protection and Symantec Network Access Control" on page 19.

About Symantec Network Access Control

Symantec Network Access Control ensures that a company's client computers are compliant with the company's security policies before the computers are allowed to access the network. Symantec Network Access Control uses a Host Integrity Policy and an optional Symantec Enforcer to discover and evaluate which computers are compliant. The clients that are not compliant are directed to a remediation server. The remediation server downloads the necessary software, patches, virus definitions updates, and so on, to make the client computer compliant. Symantec Network Access Control also continually monitors endpoints for changes in the compliance status.

Symantec Network Access Control is a companion product to Symantec Endpoint Protection. Both products include Symantec Endpoint Protection Manager, which provides the infrastructure to install and manage the Symantec Endpoint Protection and Symantec Network Access Control clients. The Symantec Endpoint Protection client protects your endpoints from both known threats and those threats that have not been seen before.

See "About Symantec Endpoint Protection" on page 17.

See "Components of Symantec Endpoint Protection and Symantec Network Access Control" on page 19.

For more information about the Enforcer appliance, see the *Implementation Guide for Symantec Network Access Control Enforcement*.

About Symantec Protection Center

Symantec Protection Center is a Web-based console that lets you integrate management of your Symantec security products into a single environment. Protection Center includes a centralized Dashboard that reports on the overall security of your network based on the products that you integrate.

You integrate supported products in Protection Center in a registration process. After you register your products, you log on to Protection Center to manage them all.

The products must be installed and configured separately before you can register them. Registered, or integrated, products still function independently of Protection Center. You can manage the products together, in Protection Center, or separately, in the individual product consoles.

Integrated products are purchased separately or as part of a suite. Only Symantec Endpoint Protection includes Symantec Protection Center.

The following products can be integrated into Protection Center:

- Symantec Endpoint Protection
- Symantec Critical System Protection
- Symantec Web Gateway
- Symantec Brightmail Gateway
- Symantec Data Loss Prevention
- Symantec IT Analytics

The products and product versions that are supported by Symantec Protection Center may change over time. For the latest information about supported products, see the Symantec Support Web site.

See "System requirements for Symantec Protection Center and Symantec Endpoint Protection Manager Web console" on page 34.

Components of Symantec Endpoint Protection and Symantec Network Access Control

Table 1-1 lists the product's components and describes their functions.

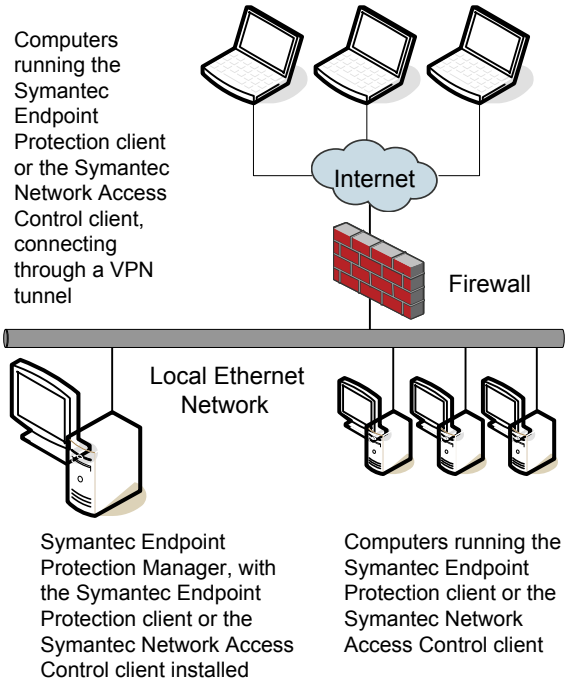
Table 1-1 Product components

Component	Description
Symantec Endpoint Protection Manager	Symantec Endpoint Protection Manager is a management server that manages the client computers that connect to your company's network. Symantec Endpoint Protection Manager includes the following software: ■ The console software coordinates and manages security policies and client computers. ■ The server software provides secure communication to and from the client computers and the console.
Database	The database that stores security policies and events. The database is installed on the computer that hosts Symantec Endpoint Protection Manager.
Symantec Endpoint Protection client	The Symantec Endpoint Protection client protects the computers with antivirus and antispyware scans, a firewall, an intrusion prevention system, and other protection technologies. It runs on the servers, desktops, and portable computers that you want to protect. For more information, see the *Client Guide for Symantec Endpoint Protection and Symantec Network Access Control*. The Symantec Endpoint Protection Mac client protects the computers with antivirus and antispyware scans.
Symantec Network Access Control client	The Symantec Network Access Control client enforces security policy compliance on the client computers by using Host Integrity checks and self-enforcement capabilities. The client reports its Host Integrity compliance status to a Symantec Enforcer. For more information, see the *Implementation Guide for Symantec Network Access Control Enforcement*. For more information, see the *Client Guide for Symantec Endpoint Protection and Symantec Network Access Control*.
Symantec Protection Center	Symantec Protection Center is installed when you install Symantec Endpoint Protection Manager. Protection Center lets you integrate management consoles from multiple supported Symantec security products into a single management environment. See "About Symantec Protection Center" on page 19.

Table 1-1 Product components *(continued)*

Component	Description
Symantec Enforcer (optional)	An Enforcer ensures that the clients that try to connect to the network comply with configured security policies. You can restrict non-compliant computers to specific network segments for remediation and you can completely prohibit access to non-compliant computers. Symantec Network Access Control includes the following types of Enforcers: ■ The Enforcer appliance, which is a hardware appliance on which you install one of several Symantec Enforcer appliance images. ■ The Integrated Enforcers, which are the software components that interact with a Microsoft DHCP Server and a Microsoft Windows Network Policy Server. For more information, see the *Implementation Guide for Symantec Network Access Control Enforcement*.
Symantec Network Access Control On-Demand clients for Windows and Macintosh (optional)	On-Demand clients are the temporary clients that you provide to users when they are unauthorized to access your network because they do not have the software that is compliant with your security policy.
LiveUpdate Server (optional)	The LiveUpdate Server downloads definitions, signatures, and product updates from a Symantec LiveUpdate server and distributes the updates to client computers. For more information, see the *Symantec LiveUpdate Administrator User's Guide*.
Central Quarantine (optional)	The Central Quarantine receives suspicious files and unrepaired infected items from the Symantec Endpoint Protection clients. Central Quarantine forwards a sample to Symantec Security Response, which analyzes the sample. If a threat is new, Symantec Security Response produces security updates. For more information, see the *Symantec Central Quarantine Implementation Guide*.

Figure 1-1 The product components in a network



See "About Symantec Endpoint Protection" on page 17.

See "About Symantec Network Access Control" on page 18.

See "Key features of Symantec Endpoint Protection and Symantec Network Access Control" on page 23.

Key features of Symantec Endpoint Protection and Symantec Network Access Control

Table 1-2 Product key features

Feature	Description
Enterprise-level protection	The product provides the following features: ■ Client computer scans for viruses and security threats. ■ Detection and repair of the effects of known viruses, worms, Trojan horses, spyware, adware, and rootkits. ■ Analysis of processes for behavior anomalies to detect known and unknown viruses and security risks. ■ Prevention of unauthorized users from accessing the computers and networks that connect to the Internet. ■ Cleaning, deleting, and quarantining infected files. ■ Automatic detection and blocking of network attacks.
Management	The following features are included: ■ Out-of-the-box configuration for any size business. ■ Symantec Protection Center console optionally lets you integrate more than one Symantec product management console into a single environment. See "About Symantec Protection Center" on page 19. ■ Single Symantec Endpoint Protection Manager console provides a view of the entire client deployment. ■ Symantec Endpoint Protection Manager coordinates console and client communication and event logging. ■ Administrator accounts that provide access to the console. ■ LiveUpdate downloads of the latest virus definitions and product updates.
Migration	The following features are included: ■ Group and policy settings from Symantec legacy software. ■ Client computer upgrades using the Client Installation Wizard.
Client enforcement	The following features are included: ■ Ensures that a client computer is properly protected and compliant before it is allowed to connect to the corporate network. ■ Remediates the non-compliant client computers.

See "About Symantec Endpoint Protection" on page 17.

See "About Symantec Network Access Control" on page 18.

Technical Support resources

Table 1-3 lists the Symantec Web sites where you can find more information.

Table 1-3 Symantec Web sites

Types of information	Web address
Symantec Endpoint Protection trialware	http://www.symantec.com/business/products/downloads/
Public Knowledge Base Releases Manuals and documentation updates Contact options Release Notes and additional post-release information	http://www.symantec.com/business/support/overview.jsp?pid=54619 http://www.symantec.com/business/support/overview.jsp?pid=52788
Virus and other threat information and updates	http://securityresponse.symantec.com
Product news and updates	http://enterprisesecurity.symantec.com
Symantec Endpoint Protection forums	http://www.symantec.com/connect/security/forums http://www.symantec.com/connect/security/forums/network-access-control
Free online technical training	http://www.symantec.com/education/endpointsecurity

Chapter 2

System and installation requirements

This chapter includes the following topics:

System requirements

Before you begin the installation of Symantec Endpoint Protection Manager you should review the system requirements and the installation requirements. You should confirm the computers you plan to use meet the requirements and are configured for communication between the management server and clients.

Symantec software requires specific protocols, operating systems and service packs, software, and hardware. All computers to which you install Symantec software should meet or exceed the recommended system and internationalization requirements for the operating system that is used.

Note: Installation to or from the directory names that contain double-byte characters is not supported.

See "System requirements for the Symantec Endpoint Protection Manager, console, and embedded database" on page 26.

See "System requirements for the Symantec Endpoint Protection Manager and console" on page 28.

See "System requirements for the Symantec Endpoint Protection Remote Console" on page 31.

See "System requirements for the Symantec Endpoint Protection client software" on page 34.

See "System requirements for the Symantec Network Access Control client software" on page 38.

See "System requirements for the Symantec AntiVirus client for Linux" on page 41.

See "System requirements for the Quarantine Console" on page 41.

See "System requirements for the Central Quarantine Server" on page 42.

System requirements for the Symantec Endpoint Protection Manager, console, and embedded database

The console is installed with the Symantec Endpoint Protection Manager.

Table 2-1 System requirements for the Symantec Endpoint Protection Manager and embedded database

Component	32-bit	64-bit
Processor	1 GHz Intel Pentium III for most systems	The following processor speeds are supported: ■ 2 GHz for Small Business Server 2008 Premium Edition ■ 2.5 GHz for Essential Business Server 2008 Premium Edition 1GHz on x64 works only with the following processors: ■ Intel Xeon with Intel EM64T support ■ Intel Pentium IV with EM64T support ■ AMD 64-Bit Opteron ■ AMD 64-Bit Athlon **Note:** Itanium is not supported.

Table 2-1 System requirements for the Symantec Endpoint Protection Manager and embedded database *(continued)*

Component	32-bit	64-bit
Operating system	The following operating systems are supported: ■ Windows 2000 Server/Advanced Server/Datacenter Server with Service Pack 3 or later ■ Windows XP Professional with Service Pack 1 or later **Note:** Windows XP supports a limited number of concurrent users if the clients are in "push" mode. Use "pull" mode on Windows XP servers for up to 100 clients. For more information, search for *Symantec Endpoint Protection Manager 11.x communication troubleshooting* on the Symantec Support Web site. ■ Windows Server 2003 Standard Edition/Enterprise Edition/Datacenter Edition/Storage Edition/Web Edition ■ Windows Small Business Server 2000/Windows Small Business Server 2003 ■ Windows Server 2008 Standard/Windows Server 2008 Enterprise/Windows Server 2008 Datacenter/Windows Web Server 2008 (all Service Packs supported)	The following operating systems are supported: ■ Windows XP Professional with Service Pack 1 or later **Note:** Windows XP supports a limited number of concurrent users if the clients are in "push" mode. Use "pull" mode on Windows XP servers for up to 100 clients. For more information, search for *Symantec Endpoint Protection Manager 11.x communication troubleshooting* on the Symantec Support Web site. ■ Windows Server 2003 Standard Edition/Enterprise Edition/Datacenter Edition/Storage Edition ■ Windows Server 2008 Standard/Windows Server 2008 Enterprise/Windows Server 2008 Datacenter/Windows Web Server 2008 (R2 and all Service Packs supported) ■ Windows Essential Business Server 2008 Standard Edition/Windows Essential Business Server 2008 Premium Edition (R2 and all Service Packs supported) ■ Windows Small Business Server 2008 Standard Edition/Windows Small Business Server 2008 Premium Edition (R2 and all Service Packs supported) **Note:** If you use Microsoft Clustering services for the Symantec Endpoint Protection Manager server, you must install the Symantec Endpoint Protection Manager on the local volume.
Memory	1 GB RAM minimum (2-4 GB recommended) for most systems	The following amounts of RAM are required: ■ 1 GB RAM minimum (2-4 GB recommended) for most systems ■ 4 GB RAM minimum for all editions of Windows Small Business Server 2008 and Windows Essential Business Server 2008

Table 2-1 System requirements for the Symantec Endpoint Protection Manager and embedded database *(continued)*

Component	32-bit	64-bit
Hard disk	4 GB for the server, plus an additional 4 GB for the database for most systems	The following hard disk space is required: ■ 4 GB for the server, plus an additional 4 GB for the database for most systems ■ Small Business Server 2008: 60 GB for the server ■ Essential Business Server 2008: 45 GB for the server
Display	VGA (640x480) or higher resolution video adapter and monitor	VGA (640x480) or higher resolution video adapter and monitor
Database	The Symantec Endpoint Protection Manager includes an embedded database. You may also choose to use one of the following versions of Microsoft SQL Server: ■ Microsoft SQL Server 2000 with Service Pack 4 or later ■ Microsoft SQL Server 2005 with Service Pack 2 ■ Microsoft SQL Server 2008 **Note:** Microsoft SQL Server is optional.	The Symantec Endpoint Protection Manager includes an embedded database. You may also choose to use one of the following versions of Microsoft SQL Server: ■ Microsoft SQL Server 2000 with Service Pack 3 or later ■ Microsoft SQL Server 2005 with Service Pack 2 ■ Microsoft SQL Server 2008 **Note:** Microsoft SQL Server is optional.
Other requirements	The following other requirements must be met: ■ Internet Information Services server 5.0 or later with World Wide Web services enabled ■ Internet Explorer 6.0 or later ■ Static IP address (recommended)	The following other requirements must be met: ■ Internet Information Services server 5.1 or later with World Wide Web services enabled ■ Internet Explorer 6.0 or later ■ Static IP address (recommended)

System requirements for the Symantec Endpoint Protection Manager and console

The manager and console are installed on all servers that are configured as additional sites on your network. "Additional sites" include any site you add, such as a replication partner or additional site for failover or load balancing.

Table 2-2 System requirements for the Symantec Endpoint Protection Manager and console

Component	32-bit	64-bit
Processor	1 GHz Intel Pentium III for most systems	The following processor speeds are supported: ■ 2 GHz for Small Business Server 2008 Premium Edition ■ 2.5 GHz for Essential Business Server 2008 Premium Edition 1GHz on x64 works only with the following processors: ■ Intel Xeon with Intel EM64T support ■ Intel Pentium IV with EM64T support ■ AMD 64-Bit Opteron ■ AMD 64-Bit Athlon **Note:** Itanium is not supported.

Table 2-2 System requirements for the Symantec Endpoint Protection Manager and console *(continued)*

Component	32-bit	64-bit
Operating system	The following operating systems are supported: ■ Windows 2000 Professional/Server/Advanced Server/Datacenter Server with Service Pack 3 or later ■ Windows XP Professional with Service Pack 1 or later **Note:** Windows XP supports a limited number of concurrent users if the clients are in "push" mode. Use "pull" mode on Windows XP servers for up to 100 clients. For more information, search for *Symantec Endpoint Protection Manager 11.x communication troubleshooting* on the Symantec Support Web site. ■ Windows Small Business Server 2000/ Windows Small Business Server 2003 ■ Windows Server 2003 Standard Edition/Enterprise Edition/Datacenter Edition/Storage Edition/Web Edition ■ Windows Server 2008 Standard/Windows Server 2008 Enterprise/Windows Server 2008 Datacenter (all Service Packs supported)	The following operating systems are supported: ■ Windows XP Professional with Service Pack 1 or later **Note:** Windows XP supports a limited number of concurrent users if the clients are in "push" mode. Use "pull" mode on Windows XP servers for up to 100 clients. For more information, search for *Symantec Endpoint Protection Manager 11.x communication troubleshooting* on the Symantec Support Web site. ■ Windows Server 2003 Standard Edition/Enterprise Edition/Datacenter Edition/Storage Edition ■ Windows Server 2008 Standard/Windows Server 2008 Enterprise/Windows Server 2008 Datacenter (R2 and all Service Packs supported) ■ Windows Essential Business Server 2008 Standard Edition/Windows Essential Business Server 2008 Premium Edition (R2 and all Service Packs supported) ■ Windows Small Business Server 2008 Standard Edition/Windows Small Business Server 2008 Premium Edition (R2 and all Service Packs supported) **Note:** If you use Microsoft Clustering services for the Symantec Endpoint Protection Manager server, you must install the Symantec Endpoint Protection Manager on the local volume.
Memory	1 GB RAM minimum (2-4 GB recommended) for most systems	The following amounts of RAM are required: ■ 1 GB RAM minimum (2-4 GB recommended) for most systems ■ 4 GB RAM minimum for all editions of Windows Small Business Server 2008 and Windows Essential Business Server 2008

Table 2-2 System requirements for the Symantec Endpoint Protection Manager and console *(continued)*

Component	32-bit	64-bit
Hard disk	4 GB for most systems	The following hard disk space is required: ■ 4 GB for most systems ■ Small Business Server 2008: 60 GB ■ Essential Business Server 2008: 45 GB
Display	XGA (1024x768) or higher resolution video adapter and monitor	XGA (1024x768) or higher resolution video adapter and monitor
Other requirements	The following other requirements must be met: ■ Internet Information Services server 5.0 or later with World Wide Web services enabled ■ If using Internet Information Services 7.0 or later (Windows Server 2008), CGI, ASP.net, and IIS 6.0 Management Compatibility must also be installed. ■ Internet Explorer 6.0 or later ■ Static IP address (recommended)	The following other requirements must be met: ■ Internet Information Services server 5.1 or later with World Wide Web services enabled ■ If using Internet Information Services 7.0 or later (Windows Server 2008), CGI, ASP.net, and IIS 6.0 Management Compatibility must also be installed. ■ Internet Explorer 6.0 or later ■ Static IP address (recommended)

System requirements for the Symantec Endpoint Protection Remote Console

The Symantec Endpoint Protection Remote Console has less stringent requirements. They are described in the following table.

Table 2-3 System requirements for the Symantec Endpoint Protection Remote Console

Component	32-bit	64-bit
Processor	1 GHz Intel Pentium III for most systems	The following processor speeds are supported: ■ 2 GHz for Small Business Server 2008 Premium Edition ■ 2.5 GHz for Essential Business Server 2008 Premium Edition 1GHz on x64 works only with the following processors: ■ Intel Xeon with Intel EM64T support ■ Intel Pentium IV with EM64T support ■ AMD 64-Bit Opteron ■ AMD 64-Bit Athlon **Note:** Itanium is not supported.

Table 2-3 System requirements for the Symantec Endpoint Protection Remote Console *(continued)*

Component	32-bit	64-bit
Operating system	The following operating systems are supported: ■ Windows 2000 Professional/Server/Advanced Server/Datacenter Server with Service Pack 3 or later ■ Windows XP Professional with Service Pack 1 or later **Note:** Windows XP supports a limited number of concurrent users if the clients are in "push" mode. Use "pull" mode on Windows XP servers for up to 100 clients. For more information, search for *Symantec Endpoint Protection Manager 11.x communication troubleshooting* on the Symantec Support Web site. ■ Windows Vista (all x86 versions) ■ Windows 7 (all x86 versions) ■ Windows Server 2003 Standard Edition/Enterprise Edition/Datacenter Edition/Storage Edition/Web Edition ■ Windows Server 2008 Standard/Windows Server 2008 Enterprise/Windows Server 2008 Datacenter/Windows Web Server 2008 (all Service Packs are supported) ■ Windows Small Business Server 2000/Windows Small Business Server 2003	The following operating systems are supported: ■ Windows XP Professional with Service Pack 1 or later **Note:** Windows XP supports a limited number of concurrent users if the clients are in "push" mode. Use "pull" mode on Windows XP servers for up to 100 clients. For more information, search for *Symantec Endpoint Protection Manager 11.x communication troubleshooting* on the Symantec Support Web site. ■ Windows Vista (all x64 versions) ■ Windows 7 (all x64 versions) ■ Windows Server 2003 Standard Edition/Enterprise Edition/Datacenter Edition/Storage Edition ■ Windows Server 2008 Standard/Windows Server 2008 Enterprise/Windows Server 2008 Datacenter/Windows Web Server 2008. Windows Server 2008 (R2 and all Service Packs are supported) ■ Windows Essential Business Server 2008 Standard Edition/Windows Essential Business Server 2008 Premium Edition (R2 and all Service Packs are supported) ■ Windows Small Business Server 2008 Standard Edition/Windows Small Business Server 2008 Premium Edition (R2 and all Service Packs are supported)
Memory	512 MB RAM minimum (1-2 GB recommended) for most systems	512 MB RAM minimum (1-2 GB recommended) for most systems
Hard disk	15 MB	15 MB
Display	VGA (640x480) or higher resolution video adapter and monitor	VGA (640x480) or higher resolution video adapter and monitor
Browser	Internet Explorer 6.0 or later	Internet Explorer 6.0 or later

System requirements for Symantec Protection Center and Symantec Endpoint Protection Manager Web console

To register Symantec Endpoint Protection Manager with Symantec Protection Center, you must use a Symantec Endpoint Protection Manager account that includes reporting rights.

Table 2-4 System requirements for Symantec Protection Center and Symantec Endpoint Protection Manager Web console

Component	Requirement
Browser	Internet Explorer 7 or later
Browser settings	Enhanced Security Configuration disabled Internet Explorer 8: run in Compatibility Mode
Display	SXGA (1280X1024) or higher resolution video adapter and monitor **Note:** Lower resolutions my require scrolling to view the entire display.

System requirements for the Symantec Endpoint Protection client software

To install client software on Windows computers, you must have administrator user rights to the computer or to the Windows domain, and log on as administrator. The Symantec software installation program launches a second installation program on the computer to create and start services, and to modify the Windows registry.

To install client software on Mac computers, you can use Symantec Endpoint Protection Manager only to configure client install packages. You then distribute the packages by using some other mechanism.

Table 2-5 System requirements for the Symantec Endpoint Protection client software

Component	32-bit	64-bit
Processor	1 GHz Intel Pentium III for most systems	The following processor speeds are supported: ■ 2 GHz for Small Business Server 2008 Premium Edition ■ 2.5 GHz for Essential Business Server 2008 Premium Edition 1GHz on x64 works only with the following processors: ■ Intel Xeon with Intel EM64T support ■ Intel Pentium IV with EM64T support ■ AMD 64-Bit Opteron ■ AMD 64-Bit Athlon **Note:** Itanium is not supported.

Table 2-5 System requirements for the Symantec Endpoint Protection client software *(continued)*

Component	32-bit	64-bit
Operating system	The following operating systems are supported: ■ Mac OS X 10.4 - 10.6 ■ Windows 2000 Professional/Server/Advanced Server/Datacenter Server with Service Pack 3 or later ■ Windows XP Professional/XP Embedded with Service Pack 1 or later **Note:** Windows XP supports a limited number of concurrent users if the clients are in "push" mode. Use "pull" mode on Windows XP servers for up to 100 clients. For more information, search for *Symantec Endpoint Protection Manager 11.x communication troubleshooting* on the Symantec Support Web site. ■ Windows Server 2003 R2, Standard Edition/Enterprise Edition/Datacenter Edition/Storage Edition/Web Edition ■ Windows Server 2003 with Service Pack 1, Standard Edition/Enterprise Edition/Datacenter Edition/Storage Edition/Web Edition ■ Windows Server 2003 with SP2, Standard Edition/Enterprise Edition/Datacenter Edition/Storage Edition/Web Edition ■ Windows Vista (all x86 versions and Service Packs) ■ Windows 7 (all x86 versions) ■ Windows Fundamentals for Legacy PCs ■ Windows Server 2008 Standard/Windows Server 2008 Enterprise/Windows Server 2008 Datacenter/Windows Web Server 2008 (all Service Packs supported). Core installations are supported. ■ Windows Small Business Server 2000/Windows Small Business Server 2003	The following operating systems are supported: ■ Mac OS X -- N/A ■ Windows XP Professional with Service Pack 1 or later **Note:** Windows XP supports a limited number of concurrent users if the clients are in "push" mode. Use "pull" mode on Windows XP servers for up to 100 clients. For more information, search for *Symantec Endpoint Protection Manager 11.x communication troubleshooting* on the Symantec Support Web site. ■ Windows Server 2003 R2, Standard Edition/Enterprise Edition/Datacenter Edition/Storage Edition ■ Windows Server 2003 with Service Pack 1, Standard Edition/Enterprise Edition/Datacenter Edition/Storage Edition ■ Windows Server 2003 with SP2, Standard Edition/Enterprise Edition/Datacenter Edition/Storage Edition ■ Windows Vista (all x64 versions and Service Packs) ■ Windows 7 (all x64 versions) ■ Windows Server 2008 Standard/Windows Server 2008 Enterprise/Windows Server 2008 Datacenter/Windows Web Server 2008 (R2 and all Service Packs supported). Core installations are supported. ■ Windows Essential Business Server 2008 Standard Edition/Windows Essential Business Server 2008 Premium Edition (R2 and all Service Packs supported) ■ Windows Small Business Server 2008 Standard Edition/Windows Small Business Server 2008 Premium Edition (R2 and all Service Packs supported)

Table 2-5 System requirements for the Symantec Endpoint Protection client software *(continued)*

Component	32-bit	64-bit
Memory	The following amounts of RAM are required: ■ 256 MB of RAM (512 MB recommended) for Mac OS X 10.4 ■ 512 MB for Mac OS X 10.5 ■ 1 GB for Mac OS X 10.6 ■ 256 MB RAM minimum (1 GB recommended) for Windows XP, Windows XP Embedded, and Windows Fundamentals for Legacy PCs ■ 1 GB RAM minimum (2-4 GB recommended) for Windows Vista, Windows 7, Windows Server 2003 (all editions), and Windows Server 2008 (all editions)	The following amounts of RAM are required: ■ 1 GB RAM minimum (2-4 GB recommended) for most systems ■ 4 GB RAM minimum for all editions of Windows Small Business Server 2008 and Windows Essential Business Server 2008
Hard disk	300 MB for Mac 600 MB for Windows	700 MB for Windows
Display	VGA (640x480) or higher resolution video adapter and monitor	XGA (1,024x768) or higher-resolution video adapter and monitor
Other requirements	Internet Explorer 6.0 or later Terminal server clients that connect to a computer with antivirus protection have the following additional requirements: ■ Microsoft Terminal Server RDP (Remote Desktop Protocol) client ■ Citrix Metaframe (ICA) client 1.8 or later if using Citrix Metaframe server on Terminal Server	Internet Explorer 6.0 or later

Note: The Push Deployment Wizard does not check to verify that Internet Explorer 6.0 or later is installed on computers when it is required. If the target computers do not have the correct version of Internet Explorer, the installation fails without informing you.

System requirements for the Symantec Network Access Control client software

To install Symantec client software, you must have administrator user rights to the computer or to the Windows domain, and log on as administrator. The Symantec software installation program launches a second installation program on the computer to create and start services, and to modify the Windows registry.

Table 2-6 System requirements for the Symantec Network Access Control client software

Component	32-bit	64-bit
Processor	1 GHz Intel Pentium III for most systems	The following processor speeds are supported: ■ 2 GHz for Small Business Server 2008 Premium Edition ■ 2.5 GHz for Essential Business Server 2008 Premium Edition 1GHz on x64 works only with the following processors: ■ Intel Xeon with Intel EM64T support ■ Intel Pentium IV with EM64T support ■ AMD 64-Bit Opteron ■ AMD 64-Bit Athlon **Note:** Itanium is not supported.

Table 2-6 System requirements for the Symantec Network Access Control client software *(continued)*

Component	32-bit	64-bit
Operating system	The following operating systems are supported: ■ Windows 2000 Professional/Server/Advanced Server/Datacenter Server with Service Pack 3 or later ■ Windows XP Professional/XP Embedded with Service Pack 1 or later **Note:** Windows XP supports a limited number of concurrent users if the clients are in "push" mode. Use "pull" mode on Windows XP servers for up to 100 clients. For more information, search for *Symantec Endpoint Protection Manager 11.x communication troubleshooting* on the Symantec Support Web site. ■ Windows Server 2003 R2, Standard Edition/Enterprise Edition/Datacenter Edition/Storage Edition/Web Edition ■ Windows Server 2003 with Service Pack 1, Standard Edition/Enterprise Edition/Datacenter Edition/Storage Edition/Web Edition ■ Windows Server 2003 with SP2, Standard Edition/Enterprise Edition/Datacenter Edition/Storage Edition/Web Edition ■ Windows Vista (all x86 versions and Service Packs) ■ Windows 7 (all x86 versions) ■ Windows Server 2008 Standard/Windows Server 2008 Enterprise/Windows Server 2008 Datacenter/Windows Web Server 2008 (all Service Packs supported). Core installations are supported. ■ Windows Small Business Server 2000/Windows Small Business Server 2003	The following operating systems are supported: ■ Windows XP Professional with Service Pack 1 or later **Note:** Windows XP supports a limited number of concurrent users if the clients are in "push" mode. Use "pull" mode on Windows XP servers for up to 100 clients. For more information, search for *Symantec Endpoint Protection Manager 11.x communication troubleshooting* on the Symantec Support Web site. ■ Windows Server 2003 R2, Standard Edition/Enterprise Edition/Datacenter Edition/Storage Edition/Web Edition ■ Windows Server 2003 with Service Pack 1, Standard Edition/Enterprise Edition/Datacenter Edition/Storage Edition/Web Edition ■ Windows Server 2003 with SP2, Standard Edition/Enterprise Edition/Datacenter Edition/Storage Edition/Web Edition ■ Windows Vista (all x64 versions and Service Packs) ■ Windows 7 (all x64 versions) ■ Windows Server 2008 Standard/Windows Server 2008 Enterprise/Windows Server 2008 Datacenter/Windows Web Server 2008 (R2 and all Service Packs supported). Core installations are supported. ■ Windows Essential Business Server 2008 Standard Edition/Windows Essential Business Server 2008 Premium Edition (R2 and all Service Packs supported) ■ Windows Small Business Server 2008 Standard Edition/Windows Small Business Server 2008 Premium Edition (R2 and all Service Packs supported)

Table 2-6 System requirements for the Symantec Network Access Control client software *(continued)*

Component	32-bit	64-bit
Memory	The following amounts of RAM are required: ■ 256 MB RAM minimum (1 GB recommended) for Windows XP and Windows Fundamentals for Legacy PCs ■ 1 GB RAM minimum (2-4 GB recommended) for Windows Vista, Windows 7, Windows Server 2003 (all editions), and Windows Server 2008 (all editions)	The following amounts of RAM are required: ■ 1 GB RAM minimum (2-4 GB recommended) for most systems ■ 4 GB RAM minimum for all editions of Windows Small Business Server 2008 and Windows Essential Business Server 2008
Hard disk	240 MB (Symantec Network Access Control client only) 600 MB (Symantec Network Access Control client and Symantec Endpoint Protection client)	220 MG (Symantec Network Access Control client only) 700 MB (Symantec Network Access Control client and Symantec Endpoint Protection client)
Display	VGA (640x480) or higher resolution video adapter and monitor XGA (1,024x768) or higher resolution video adapter and monitor	XGA (1,024x768) or higher resolution video adapter and monitor
Other requirements	Internet Explorer 6.0 or later Terminal server clients that connect to a computer with antivirus protection have the following additional requirements: ■ Microsoft Terminal Server RDP (Remote Desktop Protocol) client ■ Citrix Metaframe (ICA) client 1.8 or later if using Citrix Metaframe server on Terminal Server	Internet Explorer 6.0 or later

Note: The Push Deployment Wizard does not check to verify that Internet Explorer 6.0 or later is installed on computers when it is required. If the target computers do not have the correct version of Internet Explorer, the installation fails without informing you.

System requirements for the Symantec AntiVirus client for Linux

You can install the Symantec AntiVirus client for Linux on unmanaged clients in an environment that contains Symantec Endpoint Protection. The Symantec AntiVirus client for Linux includes real-time antivirus file protection through Auto-Protect scans and file system scans by using manual and scheduled scans.

The following operating systems are supported:

- Red Hat Enterprise Linux 3.x, 4.x, 5.x
- SuSE Linux Enterprise (server/desktop) 9.x, 10.x
- Novell Open Enterprise Server (OES/OES2)
- Ubuntu 7.x, 8.x, 9.x
- Debian 4.x, 5.x
- Fedora 11.x, 12.x
- VMWare ESX 2.5.x, 3.x

For information about the system requirements, installation on Linux, and the command-line interface, see the *Symantec AntiVirus for Linux Implementation Guide*.

For information about using the Symantec AntiVirus client on Linux, see the *Symantec AntiVirus for Linux Client Guide*.

The guides are located in the docs folder of the product CD that contains the Symantec AntiVirus client software for Linux. The *Symantec AntiVirus for Linux Implementation Guide* is also available at the following location: ftp://ftp.symantec.com/public/english_us_canada/products/symantec_antivirus/symantec_antivirus_corp/10.1/manuals/SAV_Linux_Impl.pdf.

System requirements for the Quarantine Console

The Quarantine Console has the following requirements.

Table 2-7 System requirements for the Quarantine Console

Component	32-bit
Processor	600 MHz Intel Pentium III

Table 2-7 System requirements for the Quarantine Console *(continued)*

Component	32-bit
Operating system	The following operating systems are supported: ■ Windows 2000 Professional/Server/Advanced Server/Datacenter Server with Service Pack 3 or later ■ Windows XP Professional with Service Pack 1 or later ■ Windows Server 2003 Standard Edition/Enterprise Edition/Datacenter Edition/Web Edition ■ Windows Vista (x86) Home Basic Edition/Home Premium Edition/Business Edition/Enterprise Edition/Ultimate Edition ■ Windows 7 (x86) ■ Windows Server 2008 Standard Edition/Enterprise Edition/Datacenter Edition/Web Edition (Core and Full)
Memory	64 MB of RAM
Hard disk	35 MB
Display	XGA (1,024x768) or higher-resolution video adapter and monitor
Other requirements	The following other requirements must be met: ■ Internet Explorer 5.5 Service Pack 2 or later ■ Microsoft Management Console version 1.2 or later If MMC is not already installed, you need 3 MB free disk space (10 MB during installation).
Note regarding operating systems	The Quarantine Console was not tested on 64-bit operating systems.

System requirements for the Central Quarantine Server

The Central Quarantine Server has the following requirements.

Table 2-8 System requirements for the Central Quarantine Server

Component	32-bit	64-bit
Processor	600 MHz Intel Pentium III	Not tested

Table 2-8 System requirements for the Central Quarantine Server *(continued)*

Component	32-bit	64-bit
Operating system	The following operating systems are supported: ■ Windows 2000 Professional/Server/Advanced Server/Datacenter Server with Service Pack 3 or later ■ Windows XP Professional with Service Pack 1 or later ■ Windows Server 2003 Standard Edition/Enterprise Edition/Datacenter Edition/Web Edition ■ Windows Vista (x86) Home Basic Edition/Home Premium Edition/Business Edition/Enterprise Edition/Ultimate Edition	Not tested
Memory	128 MB of RAM	Not tested
Hard disk	40 MB, 500 MB to 4 GB recommended for quarantined items, and 250-MB swap file	Not tested
Display	XGA (1,024x768) or higher-resolution video adapter and monitor	Not tested
Other requirements	■ Internet Explorer 5.5 Service Pack 2 or later	Not tested

Internationalization requirements

Certain restrictions apply when you install Symantec Endpoint Protection Manager in a non-English or mixed-language environment. You can use the following internationalization (I18N) guidelines when you plan your installation.

Table 2-9 Internationalization guidelines

Components	Requirements
Computer names, domain names, server names, and work group names	Non-English characters are supported with the following limitations: ■ The Find Unmanaged Computers feature may not work for those names that use either a double-byte character set or a high-ASCII character set. These names include host names, domain names, and user names. See "Deploying client software with Find Unmanaged Computers" on page 107. ■ Double-byte character set names or high-ASCII character set names may not appear properly on the Symantec Endpoint Protection Manager console or on the client user interface. ■ Long double-byte or high-ASCII character set host names cannot be longer than what NetBIOS allows. If the host name is longer than what NetBIOS allows, the Home, Monitors, and Reports pages do not appear on the Symantec Endpoint Protection Manager console. ■ A client computer that is named with a double-byte or high-ASCII character name does not work as a Group Update Provider.
English characters	English characters are required in the following situations: ■ To deploy a client package to a remote computer. ■ To define the server data folder on the page of the Management Server Configuration Wizard. ■ To define the installation path for the Symantec Endpoint Protection Manager. ■ To define the credentials when you deploy the client to a remote computer. ■ To define a group name. You can create a client package for those groups whose names contain non-English characters. However, you may not be able to deploy the client package by using the Push Deployment Wizard when the group name contains non-English characters. ■ To push non-English characters to the client computers. Some non-English characters that are generated on the server side may not appear properly on the client user interface. For example, a double-byte character set location name does not appear properly on non-double-byte character set named client computers.

Table 2-9 Internationalization guidelines *(continued)*

Components	Requirements
User Information client computer dialog box	Double-byte or high-ASCII characters must not be used when providing feedback in the User Information client computer dialog box after you install the exported package.
Enabling I18N support in SQL 2000	Double-byte, high-ASCII, or mixed language environments are required when using a SQL 2000 database to enable batch mode processing. You can enable I18n support in SQL 2000. On the Symantec Endpoint Protection Manager, open the following file: `c:\...\Symantec Endpoint Protection Manager\tomcat\etc\conf.properties`. Then edit the file to add the following line: scm.log.batchmode=1. Save and then close the file. Restart the Symantec Endpoint Protection Manager service.

About VMware support

Symantec software is supported on VMware.

Table 2-10 VMware support

Symantec software	VMware support
Symantec Endpoint Protection Manager, console, and database components	The management server is supported on the following versions of VMware: ■ VMware WS 5.0 (workstation) or later ■ VMware GSX 3.2 (enterprise) or later ■ VMware ESX 2.5 or later ■ VMware VMotion The management server is supported on the following guest VMware operating systems: ■ Windows 2000 Professional/Server/Advanced Server with Service Pack 3 or later (console only) ■ Windows Server 2003 Editions ■ Windows Server 2003 x64 Editions ■ Windows XP Home Edition/Professional (console only) ■ Windows XP Professional x64 Edition (console only) ■ Windows Server 2008 SP2, R2, Small Business Server/Essential Business Server 2008 ■ Windows Vista x86 and x64 Editions
Symantec Endpoint Protection and Symantec Network Access Control clients	The client components are supported on the following versions of VMware: ■ VMware WS 5.0 (workstation) or later ■ VMware GSX 3.2 (enterprise) or later ■ VMware ESX 2.5 or later ■ VMware VMotion The client components are supported on the following guest VMware operating systems: ■ Windows 2000 Professional/Server/Advanced Server ■ Windows Server 2003 x86 and x64 Editions ■ Windows Server 2008 x86 and x64 Editions ■ XP Professional/Home Edition Windows ■ XP Professional x64 Edition ■ Windows Vista x86 and x64 Editions

About Microsoft Virtual Server support

Symantec software is supported on the following Microsoft Virtual Servers:

- Microsoft Virtual Server 2005
- Windows Server 2008 Hyper-V

About Symantec Endpoint Protection Manager compatibility with other products

Some products may cause conflicts with Symantec Endpoint Protection when they are installed on the same server. You need to configure the Symantec Endpoint Protection Manager installation if one or more of the following products is installed on the same server:

- Symantec Backup Exec 10, 10D, or 11D
- Symantec Brightmail
- Symantec Enterprise Vault
- Symantec Ghost Solution Suite 2.0
- Symantec Mail Security for Exchange
- Symantec NetBackup
- Microsoft Outlook Web Access
- Microsoft SharePoint
- Microsoft Windows Update Services

In most cases, port changes are required to allow these programs to run concurrently with Symantec Endpoint Protection.

For information about the configuration changes, see Addressing Symantec Endpoint Protection compatibility issues.

Chapter 3

Planning for the installation

This chapter includes the following topics:

About choosing a database type

Symantec Endpoint Protection Manager uses a database to store information about clients and settings. The database is created as part of the configuration process. You must decide which type to use before you install the management server. You cannot use the console until you have configured the management server to use a database.

Table 3-1 Types of database that Symantec Endpoint Protection Manager uses

Database type	Description
Embedded database	The embedded database is included with Symantec Endpoint Protection Manager. The embedded database files are included with the installation files contained on the product disc. The embedded database is the easiest to install and configure and supports up to 5,000 clients. See "About embedded database settings" on page 64.
Microsoft SQL Server database	You must install Microsoft SQL Server before you install the Symantec Endpoint Protection Manager. You should consider purchasing and installing Microsoft SQL Server for the following reasons: ■ You must support more than 5,000 clients. Each management server that uses Microsoft SQL Server can support up to 50,000 clients. If your organization has more than 50,000 clients, you can install another management server. ■ You want to support failover and load balancing. See "About failover and load balancing" on page 80. If you create a Microsoft SQL Server database, you must first install an instance of Microsoft SQL server, and configure it for communication with the management server. If you plan to set up additional management servers for replication you must use a SQL Server database for the management server. See "About SQL Server configuration settings" on page 69.

About client firewalls and communication ports

If your Symantec Endpoint Protection Manager and clients run firewall software, you must open certain ports so that communication between the management server and clients is possible. Alternatively, you can permit the application Rtvscan.exe on all computers to send and receive traffic through your firewalls. The remote management server and the client installation tools require that TCP port 139 be opened.

Table 3-2 Ports for client and server installation and communication

Function	Component	Protocol and port
Push Deployment Wizard deployment	Management server and client	TCP 139 and 445 on management servers and clients UDP 137 and 138 on management servers and clients TCP ephemeral ports on management servers and clients
Find Unmanaged Computers feature	Management server and client	TCP 139 and 445 on management servers TCP ephemeral ports on clients
Group Update Provider communication	Management server and Group Update Provider Group Update Provider and clients	TCP 2967 on all devices **Note:** This port is the default port, which can be changed.
General communication	Management server and client	SEPM installation with the Default Web site, TCP 80 on management servers SEPM installation with a Custom Web site, TCP 8014 on management servers, which is the default and which can be changed TCP ephemeral ports on clients **Note:** Port 80 can also be changed to TCP 443 (HTTPS). The manager listens on the Tomcat default port TCP 8005.
General communication	Remote management server console and management server	TCP 8443 on management servers TCP ephemeral ports and 9090 on consoles **Note:** This port number is configurable.

Table 3-2 Ports for client and server installation and communication *(continued)*

Function	Component	Protocol and port
Replication communication	Site to site between database servers	TCP 8443 between database servers
Remote Symantec Endpoint Protection Manager console installation	Management server and remote management server console	TCP 9090 on remote management servers TCP ephemeral ports on remote consoles **Note:** This port number is configurable.
External database communication	Remote Microsoft SQL servers and management server	TCP 1433 on remote Microsoft SQL servers TCP ephemeral ports on management servers **Note:** Port 1433 is the default port.
Symantec Network Access Control Enforcer communication	Management server and Enforcer	TCP 1812 on management servers TCP Ephemeral ports on enforcers **Note:** RADIUS servers also use port 1812, so do not install Symantec Endpoint Protection Manager on the same server. This port is not configurable on Symantec Endpoint Protection Manager. Client authentication by the Enforcer on UDP 39,999
Migration and Deployment Wizard	Symantec Endpoint Protection Manager and legacy Symantec management server	TCP 139, TCP 445, TCP ephemeral ports, and UDP 137 on management servers TCP 139, TCP 445, TCP ephemeral ports, and UDP 137 on legacy Symantec management servers

Table 3-2 Ports for client and server installation and communication *(continued)*

Function	Component	Protocol and port
LiveUpdate	LiveUpdate client and server	TCP ephemeral ports on clients TCP 80 on LiveUpdate servers

About disabling and modifying Windows firewalls

Most versions of Windows contain a firewall that may prevent certain types of Symantec product communications. If these firewalls are enabled, you might not be able to install client software remotely with remote installation and deployment tools. If there are computers in your network that run these operating systems, you must configure the firewalls to allow for these communications. The versions of Windows that do not include firewalls are Windows XP without Service Pack 2 or later, and Windows 2000.

To use the Windows firewalls, you must configure them to support communications by opening ports or by specifying trusted programs.

Before you can install client software remotely, you must allow traffic from TCP ports 1024-5000 to TCP ports 139 and 445 on the clients. Stateful inspection permits the return traffic automatically. You must also permit clients to receive traffic from server TCP ports 1024-5000 on TCP port 139. And you must permit clients to send traffic from TCP port 139 to TCP ports 1024-5000 on servers. Legacy communications require that UDP port 2967 be open on all computers.

See "About Windows and Symantec firewalls" on page 53.

See "About turning off Windows Firewall" on page 54.

See "About modifying Windows Vista, Windows Server 2008, and Windows 7 Firewall" on page 54.

About Windows and Symantec firewalls

If you install the Symantec firewall, the installer automatically disables Windows firewalls that are enabled. If you do not install the Symantec firewall feature, the installer does not disable Windows firewalls.

The firewalls that run on Windows Vista, Windows Server 2008, and Windows 7 support both IPv4 and IPv6. The Symantec firewall supports IPv4 only. The default Symantec firewall rule base, however, contains a rule that blocks all IPv6 traffic.

Warning: Do not delete the rule that blocks IPv6. Do not change its filter action from **Block** to **Allow**.

This rule is created for the Ethernet protocol. When you display the services for a rule, and then add a service, you get access to the Ethernet protocol. You can then select the IPv6 protocol type for the Ethernet protocol.

About turning off Windows Firewall

Most versions of Windows include a firewall that is called Windows Firewall. This firewall can interfere with remote installation and communications between management servers and clients.

You are not required to disable the Windows firewall if you can create and configure rules to open the appropriate ports that permit deployment. If you cannot create and configure the firewall rules, disable Windows Firewall before you remotely deploy the client software.

Note: In Windows XP with Service Pack 1, the Windows Firewall is called Internet Connection Firewall.

After the client software is installed, you can disable Windows Firewall. Also, the Windows Firewall that runs on Windows Server 2008 Server Core is disabled by using a `netsh` command.

See "About client firewalls and communication ports" on page 50.

About modifying Windows Vista, Windows Server 2008, and Windows 7 Firewall

Windows Vista, Windows Server 2008, and Windows 7 contain a firewall that is enabled by default. If the firewall is enabled, you might not be able to install client software remotely from Symantec Endpoint Protection Manager console and other remote installation tools. You must configure Windows Firewall to allow components to communicate with each other. You must configure Windows Firewall before you install client software. You can also temporarily disable Windows Firewall on your clients before you deploy the client software.

You must configure Windows Firewall to allow file and printer sharing before you install client software on Windows Vista, Windows Server 2008, and Windows 7.

Note: Client installation automatically modifies Windows Firewall during installation on Window Vista to allow specific processes access to your network and the Internet. You are not required to make any further modifications.

About preparing Windows computers for remote deployment

You may need to change some of the settings for the operating system on the client computers to which you want to deploy client software.

Table 3-3 Client operating system configuration settings for remote deployment

Client operating system	Configuration required
Windows XP in a workgroup	Disable simple file sharing. Simple file sharing may prevent deployment of client software.
Windows Vista, Windows Server 2008, and Windows 7	■ Disable the File Sharing Wizard. ■ Enable network discovery by using the Network and Sharing Center. ■ Verify that your account has elevated user rights.
Windows Vista, Windows Server 2008, and Windows 7 in an Active Directory domain	The account used to deploy client software must be a domain administrator, and have elevated privileges on the client computer.

About preparing a Windows Server 2003 server for installation using a Remote Desktop connection

The Symantec Endpoint Protection Manager requires access to the system registry for installation and normal operation. To install software using a Remote Desktop connection, you must configure the server to which you are connecting to allow for remote control. You can then connect to the server from a remote computer by using a remote console session or you can shadow the console session.

For more information about Remote Desktop and Terminal Services, see the Windows documentation.

Preparing your client computers for installation

Before you install client software on your computers, you should first determine the state of these computers.

Table 3-4 displays the conditions that you should evaluate before you begin the client software installation process:

Table 3-4 Tasks for preparing client computers for installation

Tasks	Description
Remove viruses and risks before you install or upgrade client computers.	Some threats can directly interfere with the installation or operation of the client software. For the computers that do not have an antivirus scanner installed, you can perform a virus check from Symantec Security Response. If the virus check finds a virus, it directs you to manual removal instructions in the virus encyclopedia if they are available. You can find virus check at the Symantec Security Response Web site at the following URL: http://securityresponse.symantec.com
Determine if third-party security software is installed on your computers.	Third-party security software includes other antivirus or anti-Adware and antispyware software. These programs can affect the performance and effectiveness of the client software. Symantec does not recommend that you run two antivirus programs on one computer. Likewise, it may be problematic to run two anti-Adware or antispyware programs, and two firewall programs. This recommendation is important if both programs provide real-time protection. Both programs can create a resource conflict and can drain the computer's resources as the programs try to scan and repair the same files.
Deploy client software in a test environment.	The test environment can be an independent network of computers that is modeled after your production environment. Or, the test network can comprise a small group of computers from your actual production network See "Configuring and deploying client software on Windows computers" on page 98.

Required computer restarts when installing or migrating

In some cases, the computer on which you install Symantec Endpoint Protection software must be restarted to complete the installation process.

A computer restart is required in any of the following scenarios:

- All client computers that do not run MSI 3.1. Client installations upgrade MSI to 3.1 if 3.1 does not run on client computers, and this upgrade requires a restart.
- Symantec Endpoint Protection client installation that installs Network Threat Protection and the firewall.
- Symantec Sygate Enterprise Protection server migrations.

Section 2

Installation

Chapter 4

Installing and configuring the Symantec Endpoint Protection Manager

This chapter includes the following topics:

- About uninstalling Symantec Endpoint Protection Manager

Installing the product for the first time

You can use the following main steps to install the product on a computer on which a version is not already installed.

Table 4-1 Process for installing the product

Step	Action	Description
Step 1	Review system and installation requirements	Confirm that your network and the computers you plan to use meet the requirements to install and run the software. See "System requirements" on page 25.
Step 2	Plan and prepare for the installation	Decide which type of database to use, plan your deployment, and prepare client computers. See "About failover and load balancing" on page 80. See "About preparing Windows computers for remote deployment" on page 55. See "Preparing your client computers for installation" on page 56.
Step 3	Install Symantec Endpoint Protection Manager	Run the installation program from the product disc. The program first installs the management server software. It then configures the management server and creates the database. Follow the procedure that corresponds to the type of database you select. See "Installing and configuring the Symantec Endpoint Protection Manager with an embedded database" on page 65. See "Installing and configuring Symantec Endpoint Protection Manager with a SQL Server database" on page 74.

Table 4-1 Process for installing the product *(continued)*

Step	Action	Description
Step 4	Create and deploy a client installation package	After you configure the database, you are asked if you want to run the Migration and Deployment Wizard. This wizard creates and then pushes out a default client software installation package. Alternately, you can: ■ Use the Migration and Deployment Wizard from the Start menu at any time. ■ Create and deploy client software at a later time using the Find Unmanaged Computers utility in the console. See "Deploying client software with Find Unmanaged Computers" on page 107. If you install for a test environment you can create and install default client software packages. Those clients are assigned to the Default Group and use the default policies. If there are a large number of computers in your production environment, you may want to create custom security policies first. You can then create custom client installation packages before deploying to the clients. **Note:** If this installation is an upgrade deployment from Symantec Endpoint Protection, there is no need to re-deploy the client. The installation of Symantec Network Access Control activates the Symantec Network Access Control features on the client without further deployment. See "About Symantec client installation software" on page 96. See "Configuring and deploying client software on Windows computers" on page 98. See "Creating client installation packages" on page 104. See "Deploying client software on Windows computers with the Push Deployment Wizard" on page 106. See "Exporting client installation packages for Mac computers" on page 100. See "About deploying Mac client installation packages" on page 100.

About embedded database settings

You can specify the following values when you configure the Symantec Endpoint Protection Manager to use an embedded database.

See "Installing and configuring the Symantec Endpoint Protection Manager with an embedded database" on page 65.

Table 4-2 Embedded database settings

Setting	Default	Description
Select IIS Web site configuration options	Use the custom Web site	■ Create a custom Web site Creates an independent Symantec Web server for Symantec Endpoint Protection Manager. ■ TCP Port The port that is used for a custom Web site. You should confirm the port used is not blocked by a firewall. ■ Use the default Web site Installs the Symantec Endpoint Protection IIS Web application in the Default IIS Web site. The site works with other Web applications installed in the Web site.
Server name	*local host name*	Name of the computer that runs the Symantec Endpoint Protection Manager.
Server port	8443	TCP port number on which the Symantec Endpoint Protection Manager listens.
Web console port	9090	HTTP port used for remote console connections.
Server data folder	\\Program Files\Symantec Endpoint Protection Manager\data	Directory in which the Symantec Endpoint Protection Manager places data files including backups, replicated logs, and other files. The installer creates this directory if it does not exist.
Site name	Site *local host name*	Site name of the highest level container under which all features are configured and run with the Symantec Endpoint Protection Manager.

Table 4-2 Embedded database settings *(continued)*

Setting	Default	Description
Encryption password	None	Password that encrypts communication between the Symantec Endpoint Protection Manager, clients, and optional Enforcer hardware devices. The password can be from 1-32 alphanumeric characters and is required. When the server is configured in Simple mode, the encryption password is set to the same password as the admin account. Document this password and put it in a secure location. You cannot change or recover the password after you create the database. You must also enter this password for disaster recovery purposes if you do not have a backed up database to restore. See "Preparing for disaster recovery" on page 201.
User Name	admin	Name of the default user that is used to log on to the Symantec Endpoint Protection Manager console for the first time. (not configurable)
Password	None	The password that is specified for the admin account during server configuration.
Email address (optional)	None	System notifications are sent to the email address specified.

Installing and configuring the Symantec Endpoint Protection Manager with an embedded database

Installing with the embedded database is the easiest way to install Symantec Endpoint Protection Manager. The embedded database supports up to 5,000 clients. If you choose to configure the management server in Simple mode, the embedded database is selected automatically.

The installation of Symantec Endpoint Protection Manager is divided into three parts:

- The first part installs the management server and console.
- The second part configures the management server and creates the database.

- The third part creates and deploys client software to the client computers. You can deploy the client software during the management server installation or later. You must deploy the client software on the computer that runs the management server.

Each part consists of a wizard. When the wizard for each part completes, a prompt that asks you whether or not you want to continue with the next wizard displays.

To install Symantec Endpoint Protection Manager

1. Insert the product disc into the drive, and start the installation. For downloaded products, open the CD1 folder and double-click Setup.exe.
2. On the **Welcome** page, do one of the following actions:
   - To install Symantec Endpoint Protection, click **Install Symantec Endpoint Protection Manager**.
   - To install Symantec Network Access Control, click **Install Symantec Network Access Control**, and then click **Install Symantec Endpoint Protection Manager**.
3. On the **Welcome** page of the **Installation Wizard**, click **Next**.

   A check is performed to see if the computer meets the minimum system requirements. If it does not, a message indicates which resource does not meet the minimum requirements. You can click **Yes** to continue installing Symantec Endpoint Protection Manager, but performance can be adversely affected.
4. On the **License Agreement** page, check **I accept the terms in the license agreement**, and then click **Next**.
5. On the **Destination Folder** page, accept or change the installation directory, and then click **Next**.
6. On the **Select Web site** page, do one of the following:
   - To configure the Symantec Endpoint Protection Manager IIS Web as the only Web server on this computer, check **Create a custom Web site**, and then accept or change the **TCP Port**.

     Note: This setting is recommended for most installations as it is less likely to conflict with other programs.
   - To let the Symantec Endpoint Protection Manager IIS Web server run with other Web sites on this computer, check **Use the default Web site**.
7. Click **Next**.

8 On the **Ready to Install the Program** page, click **Install**.

9 When the installation finishes, and the **Install Wizard Completed** page appears, click **Finish**.

Wait for the **Management Server Configuration Wizard** page to appear, which can take several seconds. If you are prompted to restart the computer, restart the computer, log on, and the wizard appears automatically for you to continue.

10 Follow the steps for the appropriate mode of configuration that you select: **Simple** or **Advanced**.

To configure the Symantec Endpoint Protection Manager with an embedded database in Simple mode

1 On the **Management Server Configuration Wizard** page, select **Simple**, and then click **Next**.

2 Provide and confirm a password of 6 or more characters. Optionally, provide an administrator email address.

The password is the admin account password that you use to log on to the Symantec Endpoint Protection Manager console. The password is also used as the encryption password necessary for disaster recovery and, if you are installing Symantec Network Access Control, to add Enforcers. After installation, the encryption password does not change, even if the password for the admin account is changed.

Document this password for when you install Symantec Endpoint Protection in your production environment.

3 Click **Next**.

4 On the **Data Collection** page, do one of the following:

- To let Symantec Endpoint Protection send information about how you use this product to Symantec, check the checkbox.
- To decline to send information about how you use this product to Symantec, uncheck the checkbox.

5 The configuration summary page displays the values that are used to install Symantec Endpoint Protection Manager. You can print a copy of the settings to maintain for your records, or click **Next**.

Wait while the installation creates the database, which can take several minutes.

6 On the **Management Server Configuration Wizard Completed** page, do one of the following:

- To deploy client software with the **Migration and Deployment Wizard**, click **Yes**, and then click **Finish**.
- To log on to the Symantec Endpoint Protection Manager console first, and then deploy client software, click **No**, and then click **Finish**.

To configure the Symantec Endpoint Protection Manager with an embedded database in Advanced mode

1. On the **Management Server Configuration Wizard** page, select **Advanced**, and then click **Next**.
2. Select the number of clients you want this server to manage, and then click **Next**.

   This selection appears only when you install the Symantec Endpoint Protection Manager for the first time on this computer.
3. Check **Install my first site**, and then click **Next**.
4. On the server information page, accept or change the default values, and then click **Next**.
5. On the site name page, in the **Site** name box, accept or change the default name, and then click **Next**.
6. On the encryption password page, provide and confirm a password, and then click **Next**.

   Document this password and store it in a safe, secure location. You cannot change or recover the password after you create the database. You must also enter this password for disaster recovery purposes if you do not have a backed up database to restore.

   After you install Symantec Endpoint Protection Manager and become comfortable with administration tasks, you must secure the cryptographic files that you need for disaster recovery.
7. On the database type page, check **Embedded database**, and then click **Next**.
8. On the system administrator account page, provide and confirm a password of 6 or more characters. Optionally, provide an administrator email address. Click **Next**.

   Use the user name and password that you set here to log on to the console for the first time.

   Wait while the installation creates the database, which can take several minutes.
9. On the **Management Server Configuration Wizard Completed** page, do one of the following:

- To deploy client software with the **Migration and Deployment Wizard**, click **Yes**, and then click **Finish**.
- To log on to the Symantec Endpoint Protection Manager console first, and then deploy client software, click **No**, and then click **Finish**.

See "Configuring and deploying client software on Windows computers" on page 98.

About SQL Server configuration settings

If you install Symantec Endpoint Protection Manager with a Microsoft SQL Server database, there are specific configuration requirements for SQL Server. You can install Symantec Endpoint Protection Manager with either a local database or a remote database.

See "Installing and configuring Symantec Endpoint Protection Manager with a SQL Server database" on page 74.

Before you create the database, Symantec recommends that you install a new instance of SQL Server that conforms to Symantec installation and configuration requirements. You can install a database in an existing instance, but the instance must be configured properly or your database installation fails. For example, if you select a case-sensitive SQL collation your installation fails.

Warning: Symantec Endpoint Protection Manager authenticates to Microsoft SQL Server with a clear text database owner user name and password. To maximize the security posture of remote Microsoft SQL Server communications, collocate both servers in a secure subnet.

Table 4-3 Required SQL Server configuration settings

Configuration setting	Installation requirement
Instance name	Do not use the default name. Create a name such as SEPM. By default, a database named Sem5 is created in the SQL Server instance when you install the Symantec Endpoint Protection Manager. The default instance is unnamed. It is supported, but can cause confusion if you install multiple instances on one computer.

Table 4-3 Required SQL Server configuration settings *(continued)*

Configuration setting	Installation requirement
Authentication configuration	Mixed Mode or Windows Authentication mode See "About SQL Server database authentication modes" on page 73.
sa password	Set this password when you set Mixed Mode authentication.
Enabled protocol	TCP/IP
IP addresses for TCP/IP (SQL Server 2005 and 2008 only)	Enable IP1 and IP2
TCP/IP port numbers for IP1, IP2, and IPALL (SQL Server 2005 and 2008 only)	Set TCP Dynamic Ports to blank, and specify a TCP Port number. The default port is typically 1433. You specify this port number when you create the database. The Symantec Endpoint Protection Manager database does not support dynamic ports.
Remote connections (SQL Server 2005 and 2008 only)	Must be enabled. TCP/IP protocol must also be specified.

If your database is located on a remote server, you must also install SQL Server client components on the computer that runs Symantec Endpoint Protection Manager.

During Symantec Endpoint Protection Manager installation, you make decisions about what database values to set. You must make these decisions before you start the installation.

Table 4-4 SQL Server database settings

Setting	Default	Description
Select IIS Web site configuration options	Use the default Web site	■ Use the default Web site Installs the Symantec Endpoint Protection IIS Web application in the default IIS Web site. The site works with any other Web application that is installed in the Web site. ■ TCP Port The port that is used by the Web site created. ■ Create a custom Web site Creates an independent Symantec Web server for Symantec Endpoint Protection Manager.
Server name	*local host name*	Name of the computer that runs the Symantec Endpoint Protection Manager.
Server port	8443	Port number on which the management server listens.
Web console port	9090	The HTTP port that is used for remote console connections.
Server data folder	C:\Program Files\Symantec Endpoint Protection Manager\data	Directory in which the Symantec Endpoint Protection Manager places data files including backups, replication, and other Symantec Endpoint Protection Manager files. The installer creates this directory if it does not exist.
Site name	Site *local host name*	Site name of the highest level container under which all features are configured and run with the Symantec Endpoint Protection Manager.
Encryption password	None	The password that encrypts communication between the Symantec Endpoint Protection Manager, clients, and optional Enforcer hardware devices. The password can be from 1-32 alphanumeric characters and is required. Document this password and put it in a secure location. You cannot change or recover the password after you create the database. You must also enter this password for disaster recovery purposes if you do not have a backed up database to restore. See "Preparing for disaster recovery" on page 201.

Table 4-4 SQL Server database settings *(continued)*

Setting	Default	Description
Database server	*local host name*	Name of the Microsoft SQL Server and the optional instance name. If the database server was installed with the default instance, which is no name, type either *host name* or the host's *IP address*. If the database server was installed with a named instance, type either *host name**instance_name* or *IP address**instance_name*. Using *host name* only works with properly configured DNS. If you install to a remote database server, you must first install the SQL Server client components on the computer that runs the Symantec Endpoint Protection Manager.
SQL Server Port	1433	The port used to send and receive traffic to the SQL Server. Port 0, which is used to specify a random, negotiated port, is not supported.
Database Name	sem5	Name of the database that is created.
User	sem5	Name of the database user account that is created. The user account has a standard role with read and write access. The name can be a combination of alphanumeric values and the special characters `~#%_+=|:./`. The special characters `` `!@$^&*()-{}[]\\<;>,? `` are not allowed. The following names are also not allowed: sysadmin, server admin, setupadmin, securityadmin, processadmin, dbcreator, diskadmin, bulkadmin.
Password	None	The password to associate with the database user account. The name can be a combination of alphanumeric values and the special characters `~#%_+=|:./`. The special characters `` `!@$^&*()-{}[]\\<;>,? `` are not allowed.
SQL client folder	SQL Server 2000: C:\Program Files\Microsoft SQL Server\80\Tools\Binn SQL Server 2005: C:\Program Files\Microsoft SQL Server\90\Tools\Binn SQL Server 2008: C:\Program Files\Microsoft SQL Server\100\Tools\Binn	Location of the local SQL Client Utility directory that contains bcp.exe.

Table 4-4 SQL Server database settings *(continued)*

Setting	Default	Description
DBA user	None	Name of the database server administrator account, which is typically sa.
DBA password	None	Name of the password that is associated with the database user account.
Database data folder	Automatically detected after clicking Default SQL Server 2000: C:\Program Files\Microsoft SQL Server\MSSQL\Data SQL Server 2005: C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data SQL Server 2008: C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Data	Location of the SQL Server data directory. If you install to a remote server, the volume identifier must match the identifier on the remote server. ■ If you install to a named instance on SQL Server 2000, the instance name is appended to MSSQL with a dollar sign. For example, \MSSQL$*instance name*\Data. ■ If you install to a named instance on SQL Server 2005, the instance name is appended to MSSQL with a dot numeric identifier. For example, \MSSQL.1*instance name*\Data. ■ If you install to a named instance on SQL Server 2008, the instance name is appended to MSSQL10. For example \MSSQL10.*instance name*\Data. **Note:** Clicking Default displays the correct installation directory, if you entered the database server and instance name correctly. If you click Default and the correct installation directory does not appear, your database creation fails.
Admin User Name	admin	Name of the default user name that is used to log on to the Symantec Endpoint Protection Manager console for the first time. (not changeable)
Admin Password	None	The password that you specified during server configuration to use with the admin user name.
Email address (optional)	None	System notifications are sent to the email address specified.

About SQL Server database authentication modes

The Symantec Endpoint Protection Manager supports two modes of SQL Server database authentication:

- Windows Authentication mode

- Mixed mode

Microsoft SQL Server can be configured to use either Windows Authentication or Mixed mode authentication. Mixed mode authentication allows the use of either Windows or SQL Server credentials. When SQL Server is configured to use Mixed mode, Symantec Endpoint Protection Manager may be set to use either Windows Authentication or Mixed mode authentication. When SQL Server is set to use Windows Authentication mode, Symantec Endpoint Protection Manager must also be configured to use Windows Authentication mode.

For the remote database connections that use the Windows Authentication mode, be aware of the following requirements:

- For deployments in an Active Directory environment, the Symantec Endpoint Protection Manager and SQL Server must be located in the same Windows domain.
- For deployments in a Workgroup environment, the Windows account credentials must be the same for the local computers and the remote computers.

See "About SQL Server configuration settings" on page 69.

Installing and configuring Symantec Endpoint Protection Manager with a SQL Server database

When you configure the Symantec Endpoint Protection Manager to use a SQL Server database you can specify either a local or a remote SQL Server. You can install the Symantec Endpoint Protection Manager on the same computer that runs Microsoft SQL Server 2000, 2005, or 2008. You can then create the Symantec Endpoint Protection Manager database on the local SQL server. Alternatively, you can install the Symantec Endpoint Protection Manager on a computer that does not have Microsoft SQL Server 2000, 2005, or 2008 installed. In this case, you create the Symantec Endpoint Protection Manager database on a remote SQL server.

In either scenario, make sure that the appropriate SQL Server components are properly configured.

Note: Microsoft SQL Server 2000 is supported on English-language Windows operating systems only.

Note: If you create a new database, SQL Server automatically manages your database with the **simple** recovery model and enables Auto Shrink.

See "About SQL Server configuration settings" on page 69.

To install the Symantec Endpoint Protection Manager

1. Insert the product disc into the drive, and start the installation.
2. In the **Welcome** panel, do one of the following actions:
   - To install for Symantec Endpoint Protection, click **Install Symantec Endpoint Protection Manager**.
   - To install for Symantec Network Access Control, click **Install Symantec Network Access Control**, and then click **Install Symantec Endpoint Protection Manager**.
3. On the **Welcome** pane of the Installation Wizard, click **Next**.

   A check is performed to see if the computer meets the minimum system requirements. If it does not, a message is displayed indicating which resource does not meet the minimum requirement. You can click **Yes** to continue the installation of Symantec Endpoint Protection Manager, but performance can be adversely affected.
4. In the **License Agreement** panel, check **I accept the terms in the license agreement**, and then click **Next**.
5. In the **Destination Folder** panel, accept or change the installation directory, and then click **Next**.
6. On the **Select Web Site** panel, do one of the following actions:
   - To configure the Symantec Endpoint Protection Manager IIS Web as the only Web server on this computer, check **Create a custom Web site**. Confirm or change the TCP port number that is displayed.
   - To let the Symantec Endpoint Protection Manager IIS Web server run with other Web sites on this computer, check **Use the default Web site**.
7. Click **Next**.
8. On the **Ready to Install the Program** panel, click **Install**.
9. When the installation finishes and the Installation Wizard Complete panel appears, click **Finish**.

   The Server Configuration Wizard panel can take up to 15 seconds to appear. If you are prompted to restart the computer, restart the computer. When you log on, the Server Configuration Wizard panel appears automatically.

To configure the Symantec Endpoint Protection Manager to use a Microsoft SQL Server database

1. In the **Management Server Configuration Wizard** panel, select **Advanced**, and then click **Next**.
2. Select the number of clients that you want the server to manage, and then click **Next**.
3. Click **Install my first site**, and then click **Next**.
4. In the **Server Information** panel, accept or change the default values, and then click **Next**.
5. In the **Site Information** panel, in the Site name box, accept or change the default name, and then click **Next**.
6. In the **Create Encryption Password** panel, in the Create encryption password boxes, type a password, and then click **Next**.

   Document this password and put it in a secure location. You cannot change or recover the password after you create the database. You must also enter this password for disaster recovery purposes if you do not have a backed up database to restore.
7. In the **Database type** selection panel, select **Microsoft SQL Server**, and then click **Next**.
8. Do one of the following:
   - If the database does not exist, check **Create a new database** (recommended).
   - If the database exists, check **Use an existing database**.

   An existing database must define file groups PRIMARY, FG_CONTENT, FG_LOGINFO, FG_RPTINFO, and FG_INDEX. The user account for database access must have privileges db_ddladmin, db_datareader, and db_datawriter. If these requirements are not met, your installation fails. A best practice is to define a new database.
9. Click **Next**.
10. In the **Microsoft SQL Server Information** panel, type your values for the following boxes:
    - Database server
      If you created a new instance, the format is *servername_or_IPaddress\instance_name*.
    - SQL server port
    - Database name

- User
- Password
- Confirm password (only when creating a new database)
- SQL Client folder
- DBA user (only when you create a new database)
- DBA password (only when you create a new database)
- Database data folder

11 Click **Next**.

12 Specify and confirm a password for the Symantec Endpoint Protection Manager admin account. Optionally, provide an administrator email address.

13 Click **Next**.

14 In the **Warning** dialog prompt, read and understand the warning information about clear text communications, and then click **OK**.

15 In the **Configuration Completed** panel, do one of the following actions:

- To deploy client software with the Migration and Deployment Wizard and the Push Deployment Wizard, click **Yes**.
  See "Deploying client software on Windows computers with the Push Deployment Wizard" on page 106.
- To log on to the Symantec Endpoint Protection Manager console first, and then deploy client software, click **No**.

After you install Symantec Endpoint Protection Manager and become comfortable with administration tasks, you must secure your cryptographic files. These files are used to recover from a disaster. You must also document your encryption password that you enter during Symantec Endpoint Protection Manager installation.

See "Preparing for disaster recovery" on page 201.

About installing multiple instances of Symantec Endpoint Protection Manager

See "About choosing a database type" on page 49.

See "Installing and configuring the Symantec Endpoint Protection Manager with an embedded database" on page 65.

See "Installing and configuring Symantec Endpoint Protection Manager with a SQL Server database" on page 74.

If the network that supports your business is small and located in one geographic location, you need to install only one Symantec Endpoint Protection Manager. If your network is geographically dispersed, you may need to install additional management servers for load balancing and bandwidth distribution purposes. If your network is very large, you can install additional sites with additional databases and configure them to share data with replication. To provide additional redundancy, you can install additional sites for failover support..

See "Running additional Symantec Endpoint Protection Manager consoles" on page 78.

Running additional Symantec Endpoint Protection Manager consoles

You can run additional Symantec Endpoint Protection Manager consoles on other computers. These consoles let you log on to Symantec Endpoint Protection Manager remotely to manage Symantec Endpoint Protection.

You can run either of the following consoles:

- The Web console
  This console requires Internet Explorer 7 or Internet Explorer 8, with Enhanced Security Configuration disabled.
- The remote console
  This console requires Java Runtime software. If your computer does not have the correct version of Java Runtime, the correct version installs automatically. You may have to adjust your Internet Explorer settings for ActiveX and Java to permit installation.

If you are used to performing remote administration on legacy systems by using the Java remote console, you may continue to do so. If you are new to remotely administering Symantec Endpoint Protection, the Web console is recommended.

See "About installing multiple instances of Symantec Endpoint Protection Manager" on page 77.

Note: If you export client installation packages from a remote console, the packages are stored on the computer on which the console is running.

To run the remote console

1. On the computer where you want to run the remote console, start Internet Explorer.
2. In the address bar, type **http://*computer_name*:9090**.

   where *computer_name* is the computer name or IP address of the computer where the Symantec Endpoint Protection Manager is installed.
3. Click the link to download and install the Symantec Endpoint Protection Manager remote console.

   If necessary, follow the on-screen instructions to download and install the Java Runtime Environment.
4. In the **Security Warning** dialog box, click **Run**.
5. In the **Create shortcut** dialog box, click **Yes**.

   Click **Configure** to open the Java configuration dialog.
6. In the Logon prompt, type a user name and password for the Symantec Endpoint Protection Manager, and then click **Log On**.

To run the Web console

1. On the computer where you want to run the Web console, start Internet Explorer.
2. In the address bar, type **http://*computer_name*:9090**.

   where *computer_name* is the computer name or the IP address of the computer where Symantec Endpoint Protection Manager is installed.

   If Symantec Endpoint Protection Manager is installed on this computer, you can also click **Start > All Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager Web Access**.

3 Click the link to launch the Symantec Endpoint Protection Manager Web console.

If the Web page security certificate warning appears, click **Continue to this website (not recommended)** and add the self-signed certificate to Internet Explorer.

This message means that Internet Explorer does not recognize the linked site as being secure. Internet Explorer relies on security certificates to determine if a site is secure.

For instructions to add the security certificate to Internet Explorer, see the Symantec Technical Support Knowledge Base article, How to add the self-signed certificate for Symantec Protection Center or Symantec Endpoint Protection Manager to Internet Explorer

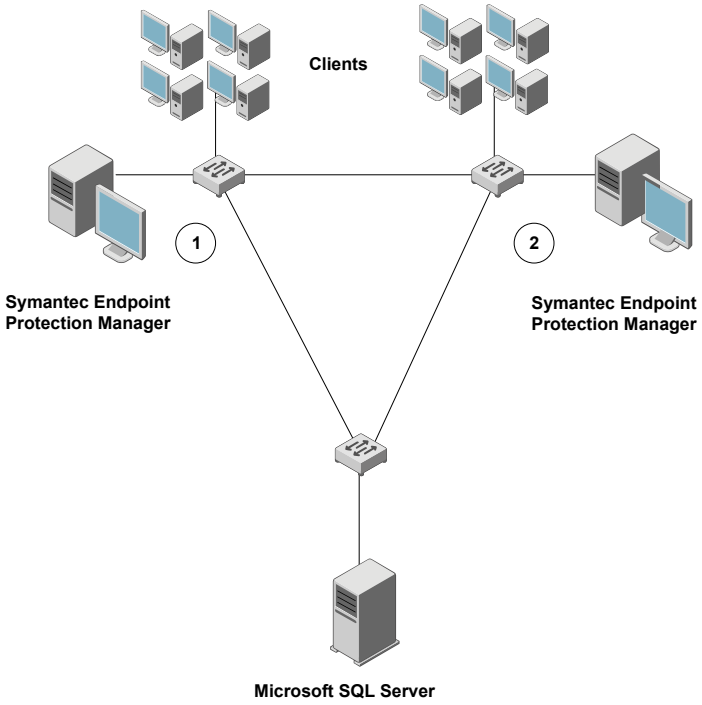
4 In the Logon prompt, type a user name and password for the Symantec Endpoint Protection Manager, and then click **Log On**.

About failover and load balancing

You can install two or more management servers that communicate with one Microsoft SQL Server and configure them for failover or load balancing. Failover configuration causes one server to pick up the client communications load if another server becomes unavailable. Load balancing configuration causes servers to share the client communications load and automatically implements failover if one of the servers goes offline.

See "About installing and configuring the Symantec Endpoint Protection Manager for failover or load balancing" on page 81.

Figure 4-1 Failover and load balancing



Note: This illustration shows components on different subnets. Management servers and database servers can be on the same subnets.

In this illustration, the servers are identified with the numbers 1 and 2, which signify a failover configuration. In a failover configuration, all clients send traffic to and receive traffic from server 1. If server 1 goes offline, all clients send traffic to and receive traffic from server 2 until server 1 comes back online. The database is illustrated as a remote installation, but it also can be installed on a computer that runs the Symantec Endpoint Protection Manager.

About installing and configuring the Symantec Endpoint Protection Manager for failover or load balancing

Failover and load balancing configurations are supported in Microsoft SQL Server installations only. Failover configurations are used to maintain communication

when clients cannot communicate with a Symantec Endpoint Protection Manager. Load balancing is used to distribute client management between management servers. You can configure failover and load balancing by assigning priorities to management servers in Management Server lists.

See "About failover and load balancing" on page 80.

Load balancing occurs between the servers assigned to Priority 1 in a Management Server list. If more than one server is assigned to Priority 1, the clients randomly choose one of the servers and establish communication with it. If all Priority 1 servers fail, clients connect with the server assigned to Priority 2.

Note: The management console is installed when you install a server for failover or load balancing.

Installing and configuring servers for failover and load balancing is a two-part process. First, you install a Symantec Endpoint Protection Manager on a computer and add it to an existing site. Second, you log on to the Symantec Endpoint Protection Manager console, and configure the new Symantec Endpoint Protection Manager.

See "Installing a management server for failover or load balancing" on page 82.

See "Configuring failover and load balancing for Symantec Endpoint Protection Manager" on page 83.

Installing a management server for failover or load balancing

Failover and load balancing installations are supported only when the original Symantec Endpoint Protection Manager uses Microsoft SQL Server. The SQL Server Native Client files also must be installed on the computer on which you install a site for failover or load balancing.

See "About failover and load balancing" on page 80.

You do not install servers for failover or load balancing when the first Symantec Endpoint Protection Manager site is configured to use the embedded database.

To install a management server for failover or load balancing

1. Install Symantec Endpoint Protection Manager.
2. In the Management Server Configuration Wizard panel, check **Advanced**, and then click **Next**.

3 Select the number of clients you expect the server to manage, and then click **Next**.

Check **Install an additional management server to an existing site**, and then click **Next**.

4 In the Server Information panel, accept or change the default values, and then click **Next**.

5 In the Microsoft SQL Server Information dialog box, enter the remote server values for the following boxes:

- Database server*instance_name*
- SQL server port
- Database name
- User
- Password
- SQL Client folder (on the local computer)
  If this box is not automatically populated with the correct path, the Microsoft SQL Client Utility is not installed or it is not installed correctly.

6 Click **Next**.

7 Specify and confirm a password for the Symantec Endpoint Protection Manager admin account. Optionally, provide an administrator email address.

8 Click **Next**.

9 In Warning prompt, read and understand the text message, and then click **OK**.

10 In Management Server Completed panel, click **Finish**.

Configuring failover and load balancing for Symantec Endpoint Protection Manager

By default, the management servers are assigned the same priority when configured for failover and load balancing. If you want to change the default priority after installation, you can do so by using the Symantec Endpoint Protection Manager console. Failover and load balancing can be configured only when a site includes more than one management server.

See "About failover and load balancing" on page 80.

To configure failover and load balancing for Symantec Endpoint Protection Manager

1. In the Symantec Endpoint Protection Manager console, click **Policies**.
2. In the View Policies pane, to the right of Policy Components, click the up arrow so that it becomes a down arrow, and then click **Management Server Lists**.
3. In the Tasks pane, click **Add a Management Server List.**
4. In the Management Server Lists dialog box, under Management Servers, click **Add > New Priority** once per priority that you want to add.
5. Under Management Servers, click **Priority 1**.
6. Click **Add > New Server**.
7. In the Add Management Server dialog box, in the Server Address box, type the fully qualified domain name or IP address of a Symantec Endpoint Protection Manager.

   If you type an IP address, be sure that it is static, and that all clients can resolve the IP address.
8. Click **OK**.
9. Do one of the following:
   - To configure load balancing with the other server, click **Priority 1**.
   - To configure failover with the other server, click **Priority 2**.
10. Click **Add > New Server**.
11. In the Add Management Server dialog box, in the Server Address box, type the fully qualified domain name or IP address of a Symantec Endpoint Protection Manager.

    If you type an IP address, be sure that it is static, and that all clients can resolve it.
12. Click **OK**.
13. Optionally, change the priority of a server to adjust the configuration for load balancing or failover. Select a server, and then do one of the following:
    - Click **Move Up**.
    - Click **Move Down**.
14. In the Management Server Lists dialog box, click **OK**.

    You must then apply the Management Server List to a group.

To apply the Management Server List

1. In the Management Server Lists pane, under Management Server Lists, under Name, highlight the Management Server List that you created.
2. In the lower-left Tasks pane, click **Assign the list**.
3. In the Apply Management Server List dialog box, check the groups to which to apply the list.
4. Click **Assign**.
5. In the Assign Management Server List dialog box, click **Yes**.

Upgrading from the embedded database to a SQL Server database

If you use an embedded database, you may decide to upgrade to a SQL Server database. Some features, such as replication, are only available when the Symantec Endpoint Protection Manager is configured to use a SQL Server database. Upgrading from an embedded to a SQL Server database can also facilitate converting a test deployment to a production network.

The following bullets summarize the process and procedures that you must follow:

- Back up the Java keystore certificate file and the server.xml file and move or copy the files from the \Symantec\Symantec Endpoint Protection Manager\ directory.
  See "Backing up the keystore and server.xml files" on page 86.
- Back up the embedded database and move or copy the backup .zip file to a new location. The default path is C:\Program Files\Symantec\Symantec Endpoint Protection Manager\data\backup.
  See "Backing up the embedded database" on page 86.
- Install an instance of SQL Server 2000, SQL Server 2005, or SQL Server 2008.
  See "About SQL Server configuration settings" on page 69.
- Uninstall the Symantec Endpoint Protection Manager and embedded database by using the Change uninstallation option.
  See "Uninstalling the Symantec Endpoint Protection Manager with an embedded database" on page 87.
- Reinstall the Symantec Endpoint Protection Manager with a SQL Server database.
  You must reinstall the Symantec Endpoint Protection Manager on the same computer, or on a computer with the original IP address and host name.

- Restore the Java keystore certificate.
  See "Restoring the original Java keystore file" on page 89.
- Reconfigure the Symantec Endpoint Protection Manager with the SQL Server database.
  See "Reconfiguring the Symantec Endpoint Protection Manager with a SQL Server database" on page 90.

Note: Perform these upgrade procedures on test computers before you perform these upgrade procedures on production computers.

Warning: Do not upgrade without creating or being in possession of a well-formed disaster recovery file. Do not try this upgrade before moving your backed up keystore, server.xml file, and database out of the \Symantec\Symantec Endpoint Protection Manager\ directory. These files are deleted during the uninstallation process.

See "Preparing for disaster recovery" on page 201.

Backing up the keystore and server.xml files

If you have not prepared for disaster recovery, you must copy or move keystore and server.xml files before you uninstall the Symantec Endpoint Protection Manager. The uninstallation process deletes these files from their original location.

See "Preparing for disaster recovery" on page 201.

To back up the keystore and server.xml files

- Move or copy all files in the following directory to a directory that is not beneath \Symantec\Symantec Endpoint Protection Manager\

  \Symantec\Symantec Endpoint Protection Manager\Server Private Key Backup\

  The files are named keystore_*date*.jks and server_*date*.xml

Backing up the embedded database

Make a backup of the existing embedded database to use for system upgrades and to protect against data loss. For instance, you can restore this database to Microsoft SQL Server after reconfiguring the management server during an upgrade.

To back up the embedded database

1. On the computer that runs the embedded database, click **Start > Programs > Symantec Endpoint Protection Manager > Database Back Up and Restore**.
2. In the Database Back up and Restore dialog box, click **Back Up**.

   This backup may take a few minutes. The backup files are .zip files that are saved in \\Program Files\Symantec\Symantec Endpoint Protection Manager\data\backup\.
3. Click **OK**.
4. When the backup is complete, click **Exit**.
5. Move or copy the backup file to a different location that is not a subfolder of the installation folder \Symantec\Symantec Endpoint Protection Manager.

   If you do not move or copy the backup file the upgrade fails because the backup file is removed when the application is uninstalled.

Installing an instance of Microsoft SQL 2000, 2005, or 2008

You can Install Microsoft SQL Server 2000, 2005, or 2008 with either Windows Authentication or SQL server authentication. You must know what port your server uses for network communications. You must enter this port number when you reinstall the Symantec Endpoint Protection Manager with a Microsoft SQL Server database.

To install an instance of Microsoft SQL Server 2000, 2005, or 2008

- Install and configure a Microsoft SQL Server instance on the computer that runs the Symantec Endpoint Protection Manager and the embedded database, or on a different computer.

See "About SQL Server configuration settings" on page 69.

See "About SQL Server database authentication modes" on page 73.

See "Installing and configuring Symantec Endpoint Protection Manager with a SQL Server database" on page 74.

Uninstalling the Symantec Endpoint Protection Manager with an embedded database

Use the Windows Add or Remove Programs utility to uninstall Symantec Endpoint Protection Manager.

To uninstall the Symantec Endpoint Protection Manager with an embedded database

1. Click **Start > Settings > Control Panel > Add or Remove Programs**.
2. In the Add or Remove Programs dialog box, click **Symantec Endpoint Protection Manager > Change**.
3. In the Welcome panel, click **Next**.
4. In the Program Maintenance panel, check **Remove**, and then click **Next**.
5. In the Remove panel, check **Remove the database during uninstall**, and then click **Next**.
6. In the Remove the Program panel, click **Remove**.

   If an error message appears about file access, restart the computer, and repeat this procedure without logging on to the Symantec Endpoint Protection Manager.

Reinstalling the Symantec Endpoint Protection Manager with a Microsoft SQL database

You need the original encryption password to reinstall the Symantec Endpoint Protection Manager with a Microsoft SQL database. This password should be in your well-formed disaster recovery file. If it is not, you must find someone who knows the password.

To reinstall the Symantec Endpoint Protection Manager with a Microsoft SQL database

1. Open your well-formed disaster recovery file.
2. Insert the product disc, and begin the installation for Symantec Endpoint Protection Manager with a Microsoft SQL Server database.

   See "Installing and configuring Symantec Endpoint Protection Manager with a SQL Server database" on page 74.
3. When the Welcome to the Management Server Configuration Wizard panel appears, check **Install my first site**, and then click **Next**.
4. Continue the installation and enter the same values that you used for the embedded database. For example, enter the same server name and port that was used for the embedded database installation. Enter the same encryption password that was used for the embedded database installation, and so forth. These values are required to correctly regenerate the sylink.xml file.

5 When the installation completes, and the Management Server Configuration Wizard Completed panel appears, check **No**, and then click **Finish**.

6 Log on to the Symantec Endpoint Protection Manager.

Restoring the original Java keystore file

The keystore file contains the public certificate that is used to secure communications. You use the keystore file as part of the disaster recovery process. You also use this when you upgrade from an embedded database to a SQL Server database. You need the original private key password to restore this file. This password is in your well-formed disaster recovery file if one was created during the original installation. The password is also in the server_*timestamp*.xml file.

See "Preparing for disaster recovery" on page 201.

To restore the original Java keystore file

1 Log on to the console, and then click **Admin**.

2 In the Admin pane, under Tasks, click **Servers**.

3 Under View Servers, expand Local Site, and then click the computer name that identifies the local site.

4 Under Tasks, click **Manage Server Certificate**.

5 In the Welcome panel, click **Next**.

6 In the Manage Server Certificate panel, check **Update the Server Certificate**, and then click **Next**.

7 Under Select the type of certificate to import, check **JKS keystore**, and then click **Next**.

If you have implemented one of the other certificate types, select that type.

8 In the JKS Keystore panel, click **Browse**, locate and select your backed up keystore_*timestamp*.jks keystore file, and then click **OK**.

9 Open your disaster recovery text file, and then select and copy the keystore password.

10 Activate the JKS Keystore dialog box, and then paste the keystore password into the Keystore password box and the Key password box.

The only supported paste mechanism is Ctrl + V.

11 Click **Next**.

If you get an error message that says you have an invalid keystore file, you probably entered invalid passwords. Retry the password copy and paste.

12 In the Complete panel, click **Finish**.

13 Log off the console.

Reconfiguring the Symantec Endpoint Protection Manager with a SQL Server database

You must know which port SQL Server uses for network communications. You enter this port number when you configure the Symantec Endpoint Protection Manager with a SQL Server database.

See "About SQL Server configuration settings" on page 69.

You need the original encryption password to reinstall the Symantec Endpoint Protection Manager with a SQL Server database. This password should be in your well-formed disaster recovery file. If it is not, you must find someone who knows the password.

To reconfigure the Symantec Endpoint Protection Manager with a SQL Server database

1 Click **Start > Settings > Control Panel > Administrative Tools > Services**.

2 In the Services window, in the right pane, right-click **Symantec Endpoint Protection Manager**, and then click **Stop**.

3 Click **Start > Programs > Symantec Endpoint Protection Manager > Database Back Up and Restore.**

4 In the Database Back Up and Restore dialog box, click **Restore**.

5 In the prompt, click **Yes**.

6 In the Select Backup file dialog box, browse to and select the database to restore, and then click **OK**.

7 After the database is restored, click **Exit.**

8 Click **Start > Programs > Symantec Endpoint Protection Manager > Management Server Configuration Wizard**.

9 On the Welcome panel, check **Reconfigure the management server**, and then click **Next**.

10 Complete the reconfiguration.

Be sure that your input values match the values that you entered when you installed the Symantec Endpoint Protection Manager. For example, if you created a named instance, be sure to append the instance name to the host name as in *host_name**instance_name*

11 Log on to the Symantec Endpoint Protection Manager, and then click **Clients**.

12 Right-click each group, and then click **Run Command on Group > Update Content**.

If the clients do not respond after about one half hour, restart the clients.

About installing and configuring Symantec Endpoint Protection Manager for replication

Replication configurations are supported with both embedded and Microsoft SQL Server databases. Replication configurations are used for redundancy. Data from one database is replicated (duplicated) on another database. If one database fails, you can still manage and control all clients because the other database contains the client information.

Installing and configuring servers for replication is a two-part process. In an existing installation site, you first install a new Symantec Endpoint Protection Manager and database for replication with an existing manager. Second, you log on to the Symantec Endpoint Protection Manager and select and schedule the items to replicate.

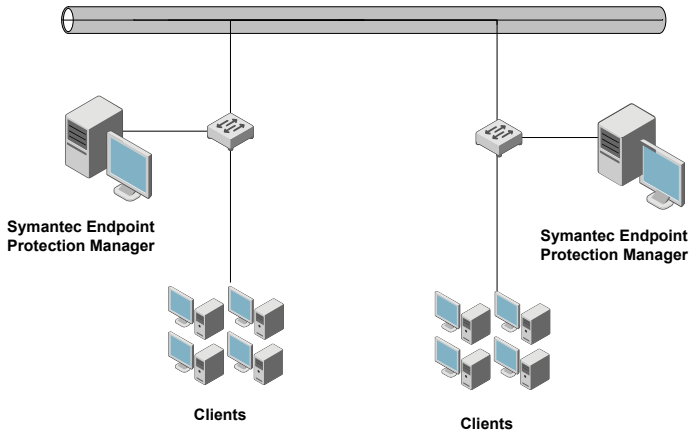
When you select the items to replicate, you can choose logs and packages. Packages also include the updates to virus definitions, client components, and client software. The size of packages and updates can grow to several gigabytes of information if you download updates in multiple languages. You must consider the amount of data you replicate when you select these options, along with the bandwidth consumption. One client package is generally 180 MB in size when compressed.

You can install and configure both the embedded database server and Microsoft SQL Server for replication. Replication configuration causes data to be duplicated between databases so that both databases contain the same information, preferably on different database servers on different computers. If one database server crashes, you can continue to manage the entire site by using the information on the database server that did not crash.

Note: Symantec Endpoint Protection Manager configures and controls this replication. This replication is not native SQL Server replication.

In the following illustration, the management servers manage their respective clients. If one of the servers goes offline, however, the other server can manage the clients from the server that went offline.

Figure 4-2 An example of replication



See "Installing Symantec Endpoint Protection Manager for replication" on page 92.

Installing Symantec Endpoint Protection Manager for replication

You can install servers for replication with both the embedded and Microsoft SQL Server databases. If you want to install a Microsoft SQL Server database for replication, you must first install Microsoft SQL Server.

See "About installing and configuring Symantec Endpoint Protection Manager for replication" on page 91.

To install Symantec Endpoint Protection Manager for replication

1. Install Symantec Endpoint Protection Manager.
2. In the Management Server Configuration Wizard panel, click **Advanced**.
3. Select the number of clients you expect the server to manage, and then click **Next**.

   This panel is displayed only when installing the Symantec Endpoint Protection Manager on the computer for the first time.
4. Check **Install an additional site**, and then click **Next**.
5. In the Server Information panel, accept or change the default values, and then click **Next**.
6. Accept or change the name in the Site Name box, and then click **Next**.

7 In the Replication Information panel, type values in the following boxes:

Replication server name	The name or IP address of the remote Symantec Endpoint Protection Manager
Replication server port	The default value is 8443
Administrator Name	The account name that is used to log on to the console with administrator user rights
Password	Provide a password that is associated with the Administrator Name that is specified

8 Click **Next**.

9 In the Certificate Warning dialog box, click **Yes**.

10 In the Database Server Choice panel, do one of the following actions, and then click **Next**.

- Check **Embedded database**, and then complete the installation.
  See "Installing and configuring the Symantec Endpoint Protection Manager with an embedded database" on page 65.
- Check **Microsoft SQL Server**, and then complete the installation.
  See "Installing and configuring Symantec Endpoint Protection Manager with a SQL Server database" on page 74.

See "Configuring the Symantec Endpoint Protection Manager for replication" on page 93.

Configuring the Symantec Endpoint Protection Manager for replication

You use the Symantec Endpoint Protection Manager console to configure servers for replication. The administrator logon credentials are the credentials that are used at the first site that you specify for replication.

To configure the Symantec Endpoint Protection Manager for replication

1 On the computer on which you installed the Symantec Endpoint Protection Manager as an additional site, log on to the Symantec Endpoint Protection Manager console.

2 In the console, click **Admin**, and then click **Servers**.

3 Under View Server, expand Local Site, expand Replication Partner, right-click **Site <remote_host>**, and then click **Edit Properties**.

4 In the Replication Partner Properties dialog box, set the options that you want for logs, packages, and replication frequency, and then click **OK**.

   Refer to context-sensitive Help and the *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control* for details about these settings.

5 Right-click **Site <remote_host>**, and then click **Replicate Now**.

6 Click **Yes**.

7 Click **OK**.

About uninstalling Symantec Endpoint Protection Manager

When you uninstall Symantec Endpoint Protection Manager, all Symantec components are uninstalled except exported client installation packages. However, you have the option to not uninstall the embedded database and Microsoft SQL Server database and backup files. For all installations, the database backup files are located on the computer that runs the Symantec Endpoint Protection Manager.

You use the standard Windows Add or Remove Programs feature to uninstall Symantec Endpoint Protection Manager. You must select Change to have the option to uninstall the database. If you select Remove, the database is not uninstalled.

You must turn off replication before you attempt to uninstall a Symantec Endpoint Protection Manager that is set up for replication. After you turn off replication, you can restart the computer from which you want uninstall the Symantec Endpoint Protection Manager, and then you can perform the uninstallation.

Note: You must manually delete all directories that contain exported client installation packages, including those directories that were created with the Migration and Deployment Wizard. You must also manually delete all backup files and directories, including those backup files and directories that contain private keys, certificates, and database files.

Chapter 5

Installing Symantec client software

This chapter includes the following topics:

About Symantec client installation software

Two products of Symantec client installation software are available, Symantec Endpoint Protection and Symantec Network Access Control. Symantec Endpoint Protection is available for Windows clients and for Mac clients.

See "About installing protection components on the client" on page 96.

See "About deploying 32-bit and 64-bit clients" on page 97.

Note: Symantec Endpoint Protection installations on a Windows client can require up to 500 MB of hard disk space during the installation process. They can require up to 300 MB of hard disk space on a Mac client. If this amount is not available, the installation fails.

See "Configuring and deploying client software on Windows computers" on page 98.

About installing protection components on the client

Symantec Endpoint Protection contains many components that you can select to install or not install. When you install Symantec Endpoint Protection, you have the following options as to what components to install:

- Core Files
  This option is required for all installations.
- Antivirus and Antispyware Protection
  This option installs core antivirus and antispyware software, and lets you select Antivirus Email Protection:
  - Antivirus Email Protection

    Note: For performance reasons, the Symantec Endpoint Protection installer blocks Internet Email Auto-Protect from installation on supported Microsoft Server operating systems. For example, you cannot install Internet Email Auto-Protect on a computer that runs Windows Server 2003.

  Note: Only Core Files and Antivirus and Antispyware Protection are available for Mac clients. Antivirus Email Protection is not available for Mac clients.

- Proactive Threat Protection

This option does not install core software, but lets you select these components:

- TruScan Proactive Threat Scan
- Application and Device Control

- Network Threat Protection
  This option does not install core software, but lets you select Firewall and Intrusion Prevention.

Note: Symantec Endpoint Protection also installs Symantec Network Access Control software, but Symantec Network Access Control is not enabled. When you update Symantec Endpoint Protection Manager for Symantec Network Access Control, the client Symantec Network Access Control feature automatically appears in the client user interface. Therefore, if you install Symantec Endpoint Protection and purchase Symantec Network Access Control at a later date, you do not need to install Symantec Network Access Control client software. If your client computers run Symantec Network Access Control, and if you purchased Symantec Endpoint Protection software at a later date, you must install the client software. You do not need to first uninstall Symantec Network Access Control.

About deploying 32-bit and 64-bit clients

Groups can contain both 32-bit clients and 64-bit clients. However, you must deploy both 32-bit packages and 64-bit packages separately to the clients. The 32-bit clients block the 64-bit installation packages and the 64-bit clients block the 32-bit installation packages due to the version mismatch.

If your environment has a mix of Symantec Endpoint Protection clients and Symantec Network Access Control clients, it is a best practice to group these clients separately. For example, a best practice is to not place Symantec Endpoint Protection clients in a group that also contains Symantec Network Access Control clients. Also, if you install Symantec Endpoint Protection Manager for Symantec Network Access Control, the Symantec Endpoint Protection clients automatically support Symantec Network Access Control.

When you create client installation packages with the management server, you can specify a group to contain the clients. If you reinstall a client software package on clients, and if the package specifies a different group, the clients still appear in their original group. The clients do not appear in the new group. You can only move clients to new groups with the management server.

Configuring and deploying client software on Windows computers

The Migration and Deployment Wizard lets you configure a client software package. The Push Deployment Wizard then optionally appears to let you deploy the client software package to Windows computers.

Note: This procedure has you select a directory in which to place installation files. You may want to create this directory before you start this procedure. Also, you need to authenticate with administrative credentials to the Windows Domain or Workgroup that contain the computers.

Computers that run firewalls, Windows XP, Windows Vista, or Windows Server 2008 have special requirements. Firewalls must permit remote deployment over TCP ports 139 and 445. Also, disable simple file sharing on the computers that are in workgroups and that run Windows XP. On Windows Vista and Windows Server 2008, you must enable network discovery.

See "About disabling and modifying Windows firewalls" on page 53.

See "About preparing Windows computers for remote deployment" on page 55.

You can also use the Find Unmanaged Computers utility that lets you locate the client computers that do not run client software and then install the client software on those computers.

See "Deploying client software with Find Unmanaged Computers" on page 107.

Note: You can use the Migration and Deployment Wizard to create a client software package for Mac computers. You cannot use the Push Deployment Wizard to deploy the package.

See "Exporting client installation packages for Mac computers" on page 100.

To configure and deploy client software on Windows computers

1. Start the Migration and Deployment Wizard by doing one of the following:
   - On the Windows Start menu, click **Start > Programs > Symantec Endpoint Protection Manager > Migration and Deployment Wizard**.
     The path may be different depending on the version of Windows that you use.
   - On the last panel of the Management Server Configuration Wizard, click **Yes**, and then click **Finish**.

See "Installing and configuring the Symantec Endpoint Protection Manager with an embedded database" on page 65.

2 In the Welcome to the Migration and Deployment Wizard panel, click **Next**.

3 In the **What would you like to do panel**, check **Deploy the Windows client**, and then click **Next**.

4 In the next panel, check **Specify the name of a new group that you wish to deploy clients to**, type a group name in the box, and then click **Next**.

After you have deployed client software and logged on to the console, you can locate this group in the console.

5 In the next panel, uncheck any types of protection that you do not want to install (Symantec Endpoint Protection only), and then click **Next**.

6 In the next panel, check the installation options that you want for packages, files, and user interaction.

7 Click **Browse**, locate and select a directory in which to place the installation file(s), and then click **Open**.

8 Click **Next**.

9 In the next panel, check **Yes**, and then click **Finish**.

It can take several minutes to create and export the installation package for your group before the Push Deployment Wizard appears.

To deploy the client software with the Push Deployment Wizard

1 In the Push Deployment Wizard, under **Available computers**, expand the trees and select the computers on which to install the client software, and then click **Add >**.

2 In the Remote Client Authentication dialog box, type the user name and password, and then click **OK**.

The user name and password must be able to authenticate to the Windows Domain or Workgroup that contains the computers.

3 When you have selected all of the computers and they appear in the right pane, click **Finish**.

See "Starting the Symantec Endpoint Protection client" on page 119.

Exporting client installation packages for Mac computers

The Migration and Deployment Wizard lets you export a client software package for Mac clients. You must then deploy the package manually.

See "Configuring and deploying client software on Windows computers" on page 98.

See "About deploying Mac client installation packages" on page 100.

You can also create and export client installation packages for Mac computers from the Admin page of the Symantec Endpoint Protection Manager console.

See "Creating client installation packages" on page 104.

To export client installation packages for Mac computers

1. Start the Migration and Deployment Wizard by doing one of the following:
   - On the Windows Start menu, click **Start > Programs > Symantec Endpoint Protection Manager > Migration and Deployment Wizard**.
     The path may be different depending on the version of Windows that you use.
   - On the last panel of the Management Server Configuration Wizard, click **Yes**, and then click **Finish**.
     See "Installing and configuring the Symantec Endpoint Protection Manager with an embedded database" on page 65.
2. In the Welcome to the Migration and Deployment Wizard panel, click **Next**.
3. In the **What would you like to do panel**, check **Export the Mac client install package**, and then click **Next**.
4. In the next panel, type the name of the group to deploy this client package to, specify the location to save the client install package to, and then click **Next**.
5. Click **Finish**.

About deploying Mac client installation packages

To install Symantec Endpoint Protection on a Mac client, you export the client installation package and then deploy the package manually. You can use any method that you have available in your network: email, a script, URL (FTP or HTTP), or third-party software such as Apple Remote Desktop.

See "Exporting client installation packages for Mac computers" on page 100.

Warning: The Mac client install package is automatically exported as a .zip file. To expand the package to the Apple install format .mpkg, you must use either the Mac Archive Utility or the ditto command. You cannot use either the Mac unzip command or any Windows unzip application.

You can also install Symantec Endpoint Protection silently on Mac clients by running the following command from the Terminal application on the Mac:

```
/usr/sbin/installer -pkg pathToPackage -target MountPoint
```

where *pathToPackage* is the location of the install package, and *MountPoint* is the location to place the package on the client computer.

You must be logged in as root to run the silent install. Otherwise, you can append `sudo` to the beginning of the silent install command.

About installing unmanaged client software on Windows computers

Clients can either be managed or unmanaged. If you do not want to use the management server to manage client software, you can install unmanaged client software. However, the installation of unmanaged Symantec Network Access Control client software is not recommended.

Unmanaged client software can be installed in the following ways:

- Using the installation program on the installation disc
- Deploying unmanaged client installation packages by using Symantec Endpoint Protection Manager
- Using the Push Deployment Wizard from the tools CD.

Installing unmanaged client software on Windows computers by using the product disc

You can install unmanaged Symantec Endpoint Protection client software by using the Setup.exe file on the product disc. The installation program installs the client software by using an installation wizard.

The Server Core installation of Windows Server 2008 offers a command-line interface only. You can, however, also manage Server Core installations using remote management tools. Client software can be installed by using the installation CD from a local or a shared network location.

Note: On Windows Vista and Windows Server 2008, you can click **Continue** for any User Account Control dialogs that appear when you perform these procedures.

To install unmanaged Symantec Endpoint Protection client software by using the installation CD

1. Insert the installation disc into the drive, and start the installation program if it does not start automatically.
2. Click **Install Symantec Endpoint Protection Client**.
3. On the Welcome panel, click **Next**.
4. On the License Agreement Panel, click **I accept the terms in the license agreement**, and then click **Next**.
5. Confirm that **Unmanaged computer** is selected, and then click **Next**.

   This panel appears only if installing the Symantec Endpoint Protection client software for the first time on this computer.
6. On the Setup Type panel, do one of the following actions:
   - Click **Typical** to install the client software with most common options, and then click **Next**.
   - Click **Custom** to choose which components are installed and the options used to install them, and then click **Next**.
     On the Custom Setup panel, select the features you want to install and how you want to install them. Confirm the installation location, or click **Change** to select a different location, and then click **Next**.
7. On the Protection Options panel, click **Next**.

   You can optionally uncheck **Enable Auto-Protect** and **Run LiveUpdate** upon completion of the installation, and then click **Next**.

   On Windows Vista you can also choose to turn off Windows Defender.
8. On the Ready to Install the Program panel, click **Install**.
9. On the Wizard Complete panel, click **Finish**.

   If the Run LiveUpdate option is selected during installation, LiveUpdate launches when the installation in finished. You may be prompted to restart you computer.

To install unmanaged Symantec Network Access Control client software by using the product disc

1. Insert the product disc into the drive, and start the installation program if it does not start automatically.
2. Click **Install Symantec Network Access Control**, and then click **Install Symantec Network Access Control**.
3. On the Welcome panel, click **Next**.
4. On the License Agreement Panel, click **I accept the terms in the license agreement**, and then click **Next**.
5. On the Destination Folder panel, confirm or change the destination folder that appears, and then click **Next**.
6. On the Ready to Install panel, click **Install**.
7. On the Wizard Completed panel, click **Finish**.

   You may be prompted to restart your computer.

To install unmanaged Symantec Endpoint Protection 64-bit client software on 64-bit Windows Server 2008 Server Core

1. Insert the product disc into the drive.
2. Change directories to the root directory of the product disc.
3. Type **cd SEPWIN64\X64**, and then press **Enter**.
4. Type **vcredist_x64.exe**, and press **Enter**.
5. Change directories to the root directory of the product disc.
6. Type **Setup.exe**, and press **Enter**
7. Follow the steps of the installation wizard to complete the installation.

To install unmanaged Symantec Endpoint Protection client software on Windows Server 2008 Server Core (all other clients)

1. Insert the product disc in the drive.
2. Open a command prompt.
3. Change directories to the root directory of the product disc.
4. Type **Setup.exe**, and then press **Enter**
5. Follow the steps of the installation wizard to complete the installation.

About deploying unmanaged client software on Windows computers using the console

You can export unmanaged client install packages from Symantec Endpoint Protection Manager. After you export the unmanaged packages, you do not assign the packages to any groups. If you assign the packages to groups, the clients in the group appear in the console after software installation. However, you cannot manage these clients.

About deploying unmanaged client software on Windows computers using the Push Deployment Wizard

You can deploy unmanaged software with the Push Deployment Wizard. You can start the wizard by using the ClientRemote.exe file. The file is located in the Tools\PushDeploymentWizard folder on the product disc that contains additional tools.

When asked to specify the folder containing the client software, do one of the following:

- To deploy the Symantec Endpoint Protection client, select the SEP folder on the product disc.
- To deploy the Symantec Network Access Control client, select the SNAC folder on the product disc.

Creating client installation packages

Two types of packages are available:

- The default installation package that is created when you install the Symantec Endpoint Protection Manager.
- A customized client package that is created especially for a particular group or set of groups. This type of installation package may contain customized group policies and settings.

You can create either type of package as a 32-bit package, a 64-bit package, or a Mac package.

When you install the default package, clients appear in the Default group and receive the default policies. A customized package is not typically assigned to the Default group.

You can create client installation packages for groups at any time. If you create customized policies that do not change often, you can create a client installation package for the group that uses these policies. This package can then be installed

on new computers that are added to the group. However, a new client installation package is not needed to change policies. Changes to policies are automatically propagated to clients in the group to which the policies apply.

Note: Client installation packages should be deployed with the silent or the unattended option to computers running Microsoft Windows Server 2008 or Microsoft Vista (x64). Only the silent option should be used for the installation packages that are deployed to computers running Microsoft Vista (x86). When a silent deployment is used, the applications that plug into Symantec Endpoint Protection, such as Microsoft Outlook and Lotus Notes, must be restarted.

Note: For more information about client installation packages, see the *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control*.

To create client installation packages

1. In the Symantec Endpoint Protection Manager console, click **Admin**.
2. In the Tasks pane, click **Install Packages**.
3. In the right pane, under Package Name, select the package to export.
4. In the lower-left pane, under Tasks, click **Export Client Install Package**.
5. In the Export Package dialog box, click **Browse**.
6. In the Select Export Folder dialog box, browse to and select the directory to contain the exported package, and then click **OK**.
7. In the Export Package dialog box, set the other options according to your installation goals.

   For details about the other options in this dialog box, click **Help**.
8. Click **OK**.

For more information, see Symantec Support Knowledge Base article How to Deploy Symantec Endpoint Protection to your client computers using the Migration and Deployment Wizard

About deploying client software on Windows computers from a mapped drive

After you export a client installation package to a directory, you can share that directory and then have users map the directory from client computers. Then, the users can install the client software from the mapped drive.

See "Creating client installation packages" on page 104.

Note: During Symantec Endpoint Protection client software installation, the mapped drive becomes temporarily disconnected. This activity is known and expected. This activity does not occur when you install Symantec Network Access Control client software.

Deploying client software on Windows computers with the Push Deployment Wizard

The Push Deployment Wizard appears automatically when you use the Migration and Deployment Wizard, or you can use the Windows Start menu to start it. You must decide what client software package you want to deploy before you run the wizard, and must know the folder where the package exists. You have to locate it during deployment.

To deploy client software with the Push Deployment Wizard

1. Start the Migration and Deployment Wizard by doing one of the following:
   - On the Windows Start menu, click **Start > Programs > Symantec Endpoint Protection Manager; Migration and Deployment Wizard**.
     The path may be different depending on the version of Windows you use.
   - On the last panel of the Management Server Configuration Wizard, click **Yes**, and then click **Finish**.
2. In the Welcome panel, click **Next**.
3. Click **Deploy the client** (Symantec Endpoint Protection only), and then click **Next**.
4. Click **Select an existing client install package to deploy**, and then click **Finish**.
5. In the Push Deployment Wizard panel, click **Browse**, navigate to and select the folder that contains the installation package you want to deploy, and then click **OK**.

6 In the Select Computers panel, under Available computers, select the computers on which to install the client software.

As an alternative, you can import a workgroup or domain of computers, and also a text file list of computers.

See "Importing a list of computers from a text file" on page 108.

7 Click **Add**.

8 In the Remote Client Authentication dialog box, type a user name and password, and then click **OK**.

The user name must be able to authenticate to the Windows Domain or Workgroup that contains the computers.

9 When you have selected all of the computers and they appear in the right pane, click **Finish**.

Deploying client software with Find Unmanaged Computers

You can deploy client software by using Find Unmanaged Computers in the Symantec Endpoint Protection Manager console. The utility lets you discover the client computers that do not run client software and then install the client software on those computers.

Note: You can use this utility only to discover Windows client computers. Mac client computers are listed in the utility as Unknown, and Mac client install packages must be deployed separately.

See "Exporting client installation packages for Mac computers" on page 100.

Note: This utility places unmanaged computers in the unknown category if the LAN Manager authentication levels are incompatible with the six authentication levels defined. Symantec recommends the level Send NTLM 2 response only. The policy to edit is under Local Policy Settings > Security Settings > Local Policies > Security Options > [Network security] LAN Manager authentication level. Also, this utility does not properly recognize Windows 2000 operating systems when run from a default Windows Server 2003 installation. To work around this limitation, you run the Symantec Endpoint Protection Manager service as Administrator rather than System in the Services panel.

Warning: This utility detects and displays a variety of networking devices in the unknown computers tab. For example, this utility detects router interfaces and places them in the unknown computers tab. You should use caution when you deploy client software to devices that appear in the unmanaged computers tab. Verify that these devices are valid targets for client software deployment.

You can also deploy client software by using the Push Deployment Wizard.

See "Deploying client software on Windows computers with the Push Deployment Wizard" on page 106.

To deploy client software by using Find Unmanaged Computers

1. In the Symantec Endpoint Protection Manager console, click **Clients**.
2. In the Tasks pane, click **Find Unmanaged Computers**.
3. In the Find Unmanaged Computers window, under Search By, check **IP address range**, and enter the IP addresses for the range to search.

   Scanning a range of 100 IP addresses that do not exist takes approximately 5.5 minutes. Optionally, specify a computer name.
4. Under Logon Credentials, complete the User name, Password, and Domain-Workgroup boxes with the logon credentials that permit administration and installation.
5. Click **Search Now**.
6. On either the Unknown Computers or Unmanaged Computers tabs, do one of the following:
   - Check each computer on which you want to install client software.
   - Click **Select All**.
7. Under Installation, select the installation package, the installation option, and the features that you want to install.
8. To install to a group other than the default group, click **Change**, select a different group, and then click **OK**.
9. When you are ready to install the client software, click **Start Installation**.

Importing a list of computers from a text file

Instead of selecting Windows computers during Push Deployment Wizard installation, you can import a list of Windows computers from a text file.

You can create a text file that contains a list of the IP addresses for the computers to include. You can import this text file during the Push Deployment Wizard, and then deploy the client software to the specified computers.

The text file used must contain each IP address on a separate line. You can comment out the IP addresses that you do not want to import with a semicolon (;) or a colon (:). For example, you may want to temporarily remove addresses on a subnet that is unavailable during the deployment.

Note: The use of a text file is not recommended for IP addresses assigned by DHCP.

To import a text file of computers that you want to install

1. In a text editor such as Notepad, create a new text file.
2. In the Select Computers panel, click **Select**.
3. In the Client Details dialog box, click **Import**.
4. Locate and double-click the text file that contains the IP addresses to import.

   During the authentication process, you may need to provide a user name and password for the computers that require authentication. The installation program also checks for error conditions. You are prompted to view this information on an individual computer basis or to write the information to a log file for later viewing.
5. Finish the installation.

About installing and deploying client software with Altiris

You can install and deploy Symantec client software on Windows computers by using software from Altiris, now part of Symantec. Altiris provides a free Integrated Component for Symantec Endpoint Protection that provides default installation capabilities, integrated client management, and high-level reporting.

Altiris software enables information technology organizations to manage, secure, and service heterogeneous IT assets. It also supports software delivery, patch management, and many other management capabilities. Altiris software helps IT align services to drive business objectives, deliver audit-ready security, automate tasks, and reduce the cost and complexity of management.

For information about the Integrated Component for Symantec Endpoint Protection, see the Symantec Support Knowledge base article, Symantec Endpoint Protection Integration Component 6.0 Release Notes.

For information about Altiris, go to the following URL:

http://www.altiris.com

To download the Integration Component for Symantec Endpoint Protection or other Altiris solutions, go to the following URL:

http://www.altiris.com/Download.aspx

Third-party installation options

Symantec client software supports installation using third-party tools to deploy client software. However, this support requires advanced knowledge of Windows or third-party management tools. Larger-scale networks are more likely to benefit by using these advanced options to install Symantec client software.

See "About installing clients using third-party products" on page 110.

See "About customizing installations by using .msi options" on page 110.

See "About installing clients with Microsoft SMS 2003" on page 110.

See "About installing clients with Active Directory Group Policy Object" on page 112.

About installing clients using third-party products

You can install Symantec clients by using a variety of third-party products, such as Microsoft Active Directory, Tivoli, Microsoft Systems Management Server (SMS), and Novell ZENworks. The only tested and supported third-party products are Novell ZENworks, Microsoft Active Directory, and Microsoft SMS.

About customizing installations by using .msi options

The Symantec client software installation packages are Windows Installer (.msi) files that are fully configurable and are deployed by using the standard Windows Installer options. You can use the environment management tools that support .msi deployment, such as Active Directory or Tivoli, to install clients on your network.

See "About configuring msi command strings" on page 193.

About installing clients with Microsoft SMS 2003

System administrators can use Microsoft Systems Management Server (SMS) to install Symantec client software. We assume that system administrators who use SMS have previously installed software with SMS. As a result, we assume that

you do not need detailed information about installing Symantec client software with SMS.

Symantec client installation software requires that Microsoft Installer 3.1 run on client computers before the installation. This software is automatically installed if it is not on client computers, but only when you deploy with a single executable setup.exe. This software is not automatically installed if you deploy with the msi file. Computers that run Windows Server 2003 with Service Pack 2, and Windows Vista include Microsoft Installer 3.1 or greater. If necessary, first deploy WindowsInstaller-x86.exe that is contained in the SEP and the SNAC installation directories on the installation CD. Upgrading to msi 3.1 also requires a computer restart.

Note: This note applies to SMS version 2.0 and earlier: If you use SMS, turn off the **Show Status Icon On The Toolbar For All System Activity** feature on the clients in the **Advertised Programs Monitor**. In some situations, Setup.exe might need to update a shared file that is in use by the Advertised Programs Monitor. If the file is in use, the installation fails.

To create and distribute Symantec client software with SMS 2003, you typically complete the following tasks:

- Create a software installation package with Symantec Endpoint Protection Manager that contains the software and policies to install on your client computers. Additionally, this software installation package must contain a file named Sylink.xml, which identifies the server that manages the clients.
- Create a source directory and copy Symantec client installation files into that source directory. For example, you would create a source directory that contains the installation files for Symantec client software.
- Create a package, name the package, and identify the source directory as part of the package.
- Configure the Program dialog box for the package to specify the executable that starts the installation process, and possibly specify the msi with parameters.
- Distribute the software to specific Collections with Advertising.

Warning: You must include a Sylink.xml file in client installation packages that you created by using the files on the product disc. You must include a Sylink.xml file that is created after you install and use Symantec Endpoint Protection Manager. The Sylink.xml file identifies the management server to which the clients report. If you do not include this file the client is installed as an unmanaged client. As a result, all clients are installed with default settings and do not communicate with a management server.

For more information on using SMS, see Microsoft Systems Management Server documentation.

About installing clients with Active Directory Group Policy Object

You can install client software by using a Windows 2000/2003 Active Directory Group Policy Object. The procedures for installing client software with Active Directory Group Policy Object assume that you have installed this software and use Windows 2003 Active Directory.

The installation software requires that client computers contain and can run Windows Installer 3.1 or later. Computers meet this requirement if they run Windows XP with Service Pack 2 and higher, Windows Server 2003 with Service Pack 1 and higher, and Windows Vista. If client computers do not meet this requirement, all other installation methods automatically install Windows Installer 3.1 by bootstrapping it from the installation files.

For security reasons, Windows Group Policy Object does not permit bootstrapping to the executable file WindowsInstaller*.exe from the installation files. Therefore, before you install Symantec client software, you must run this file on the computers that do not contain and run Windows Installer 3.1. You can run this file with a computer startup script. If you use a GPO as an installation method, you must decide how to update the client computers that do not run Windows Installer 3.1.

The Symantec client installation uses standard Windows Installer .msi files. As a result, you can customize the client installation with .msi properties.

See "About customizing installations by using .msi options" on page 110.

Finally, confirm that your DNS server is set up correctly. The correct setup is required because Active Directory relies on your DNS server for computer communication. To test the setup, you can ping the Windows Active Directory computer, and then ping in the opposite direction. Use the fully qualified domain name. The use of the computer name alone does not call for a new DNS lookup. Use the following format:

```
ping computername.fullyqualifieddomainname.com
```

Table 5-1 Steps for installing the client software by using Active Directory Group Policy Object

Step	Action
Step 1	Create the administrative install image. See "Creating the administrative installation image" on page 113.
Step 2	Copy Sylink.xml to the installation files. See "Copying a Sylink.xml file to the installation files" on page 114.
Step 3	Stage the administrative install image. See "Staging the installation files" on page 115.
Step 4	Create a GPO software distribution. You should also test GPO installation with a small number of computers before the production deployment. If DNS is not configured properly, GPO installations can take an hour or more. See "Creating a GPO software distribution" on page 115.
Step 5	Create a Windows Installer 3.1 startup script. See "Creating a Windows Installer 3.1 Startup script" on page 117.
Step 6	Add computers to the organizational unit. See "Adding computers to an organizational unit and installation software" on page 118.

See "Uninstalling client software with Active Directory Group Policy Object" on page 119.

Creating the administrative installation image

Group Policy Object installations that use Windows Installer 3.0 and lower require administrative images of the client installation files. This image is not a requirement for 3.1 and higher installations and is optional. If you do not create the administrative image, you must still copy the contents of the SEP folder on the CD to your computer.

See "About installing clients with Active Directory Group Policy Object" on page 112.

To create the administrative installation image

1. Copy the contents of SEP folder on the CD to your computer.
2. From a command prompt, navigate to the SEP folder and type `msiexec /a "Symantec AntiVirus.msi"`

3 In the Welcome panel, click **Next**.

4 In the Network Location panel, enter the location where you want to create the administrative install image, and then click **Install**.

5 Click **Finish**.

Copying a Sylink.xml file to the installation files

When you install Symantec Endpoint Protection Manager, the installation creates a file named Sylink.xml. Symantec Endpoint Protection clients read the contents of this file to know which management server manages the client. If you do not copy this file to the installation files before you install the client software, the clients are installed as unmanaged. You must create at least one new group with the management console before you copy the file. If you do not, the Sylink.xml file causes the clients to appear in the Default group.

Note: Packages that are exported with the Symantec Endpoint Protection Manager console include a Sylink.xml file.

See "About installing clients with Active Directory Group Policy Object" on page 112.

To copy Sylink.xml file to the installation files

1 If you have not done so, install a Symantec Endpoint Protection Manager.

2 Locate a Sylink.xml file in one of the outbox folders.

By default, these folders are located at \\Program Files\Symantec\Symantec Endpoint Protection Manager\data\outbox\agent*uid*\ where *uid* represents a unique name for the package folder, such as 8F171749C0A85C820163FBAA230DBF18. You may have to open and read the Sylink.xml files in the different *uid* folders with a text editor to find the file you want.

3 If necessary, copy Sylink.xml to removable media.

4 Copy Sylink.xml by using one of the following methods:

- If you created an administrative installation file image, overwrite the Sylink.xml file in folder.*install_directory*\Program Files\Symantec Endpoint Protection Manager\.
- If you did not create an administrative installation file image, copy the SEP folder on the product disc to a folder on your computer. Then, to create a managed client, copy the Sylink.xml file into that destination folder.

Staging the installation files

You can stage the installation files for deployment. To do so, share the folder that contains the client installation files. Assign user permissions for the users that log on to the clients to which you want to deploy the package.

See "About installing clients with Active Directory Group Policy Object" on page 112.

To stage the installation files

1. If necessary, copy the folder that contains the client installation files to a folder that is shared.
2. Right-click the folder, and then click **Sharing and Security**.
3. In the Properties dialog box, on the Sharing tab, check **Share this folder**, and then click **Permissions**.
4. In the Permissions dialog box, under Group or user names, click **Everyone**, and then click **Remove**.
5. Click **Add**.
6. Under Enter the object names to select, type **Authenticated Users**, and then click **Check Names**.
7. Type **Domain Computers**, click **Check Names**, and then click **OK**.
8. In the Permissions dialog box, click **Apply**, and then click **OK**.

Creating a GPO software distribution

The procedure assumes that you have installed Microsoft's Group Policy Management Console with Service Pack 1 or later. The procedure also assumes that you have computers in the Computers group or some other group to which you want to install client software. You can drag these computers into a new group that you create.

Note: If User Account Control (UAC) is enabled, you must enable **Always install with elevated privileges** for **Computer Configuration** and **User Configuration** to install Symantec client software with a GPO. You set these options to allow all Windows users to install Symantec client software.

See "About installing clients with Active Directory Group Policy Object" on page 112.

To create a GPO package

1. On the Windows Taskbar, click **Start > Programs > Administrative Tools > Group Policy Management**.
2. In the Active Directory Users and Computers window, in the console tree, right-click the domain, and then click **Active Directory Users and Computers**.
3. In the **Active Directory Users and Computers** window, right-click the Domain, and then click **New > Organizational Unit**.
4. In the New Object dialog box, in the Name box, type a name for your organizational unit, and then click **OK**.
5. In the Active Directory Users and Computers window, click **File > Exit**.
6. In the Group Policy Management window, in the console tree, right-click the organizational unit that you created, and then click **Create and Link a GPO Here**.

   You may need to refresh the domain to see your new organizational unit.
7. In the New GPO dialog box, in the Name box, type a name for your GPO, and then click **OK**.
8. In the right pane, right-click that GPO that you created, and then click **Edit**.
9. In the Group Policy Object Editor window, in the left pane, under the Computer Configuration, expand **Software Settings**.
10. Right-click **Software installation**, and then click **New > Package**.
11. In the Open dialog box, type the Universal Naming Convention (UNC) path that points to and contains the MSI package.

    Use the format as shown in the following example:

    ***server name**SharedDir*\Symantec AntiVirus.msi**
12. Click **Open**.
13. In the Deploy Software dialog box, click **Assigned**, and then click **OK**.

    The package appears in the right pane of the Group Policy Object Editor window if you select Software Installation.

To configure templates for the package

1. In the Group Policy Object Editor window, in the console tree, display and enable the following settings:
   - Computer Configuration > Administrative Templates > System > Logon > Always wait for the network at computer startup and logon

- Computer Configuration > Administrative Templates > System > Group Policy > Software Installation policy processing
- User Configuration > Administrative Templates > Windows Components > Windows Installer > Always Install with elevated privileges

2 Close the Group Policy Object Editor window.

3 In the Group Policy Management window, in the left pane, right-click the GPO that you edited, and then click **Enforced**.

4 In the right pane, under Security Filtering, click **Add**.

5 In the dialog box, under Enter the object name to select, type **Domain Computers**, and then click **OK**.

Creating a Windows Installer 3.1 Startup script

You must install Windows Installer 3.1 on the computers that contain and run earlier versions of Windows Installer. You can display Windows Installer versions by running msiexec /? in a command prompt. Windows Installer 3.1 is required for the GPO installation package. How you install Windows Installer 3.1 on computers is up to you.

Note: Restricted users cannot run Windows Installer 3.1, and restricted users with elevated privileges cannot run Windows Installer 3.1. Restricted users are set with the local security policy.

One way to install Windows Installer 3.1 is with a GPO computer startup script. Startup scripts execute before the GPO .msi installation files when computers restart. If you use this approach, be aware that the startup script executes and reinstalls Windows Installer every time the computer is restarted. If you install it in silent mode, however, users experience a slight delay before they see the logon screen. Symantec client software is only installed one time with a GPO.

See "About installing clients with Active Directory Group Policy Object" on page 112.

To install Windows Installer 3.1

1 In the Group Policy Management Window, in the console tree, expand your organizational unit, right-click your package, and then click **Edit**.

2 In the Group Policy Object Editor window, in the console tree, expand **Computer Configuration > Windows Settings**, and then click **Scripts (Startup/Shutdown)**.

3 In the right pane, double-click **Startup**.

4 In the Startup Properties dialog box, click **Show Files**.

5 In a new window, Copy the WindowsInstaller-893803-x86.exe file from the GPO installation file folder to the Startup window and folder.

6 Redisplay the Startup Properties dialog box, and then click **Add**.

7 In the Add a Script dialog box, click **Browse**.

8 In the Browse dialog box, select the Windows Installer executable file, and then click **Open**.

9 In the Add a Script dialog box, in the Script Parameters box, type `/quiet /norestart`, and then click **OK**.

10 In the Startup Properties dialog box, click **OK**.

11 Exit the Group Policy Object Manager window.

Adding computers to an organizational unit and installation software

You can add computers to an organizational unit. When the computers restart, the client software installation process begins. When users log on to the computers, the client software installation process completes. The group policy update, however, is not instantaneous, so it may take time for this policy to propagate. The procedure, however, contains the commands that you can run on the client computers to update the policy on demand.

See "About installing clients with Active Directory Group Policy Object" on page 112.

To add computers to the organizational unit and install software

1 On the Windows Taskbar, click **Start > Programs > Administrative Tools > Active Directory Users and Computers**.

2 In the Active Directory Users and Computers window, in the console tree, locate one or more computers to add to the organizational unit that you created for GPO installation.

Computers first appear in the Computers organizational unit.

3 Drag and drop the computers into the organization unit that you created for the installation.

4 Close the Active Directory Users and Computers window.

5 To quickly apply the changes to the client computers (for testing), open a command prompt on the client computers.

6 Type one of the following commands, and then press **Enter**.

- On the computers that run Windows 2000, type **secedit /refreshpolicy machine_policy**.

- On the computers that run Windows XP and later, type **gpupdate**.

7 Click **OK**.

Uninstalling client software with Active Directory Group Policy Object

You can uninstall the client software that you installed with Active Directory.

To uninstall client software with Active Directory Group Policy Object

1 On the Windows Taskbar, click **Start > Programs > Administrative Tools > Group Policy Management**.

The version of Windows that you use may display All Programs instead of Programs in the Start menu.

2 In the Group Policy Management window, in the console tree, expand the domain, expand **Computer Configuration**, expand **Software Settings**, right-click **Software Installation**, and then click **Properties**.

3 On the **Advanced** tab, check **Uninstall this application when it falls out of the scope of management**, and then click **OK**.

4 In the right pane, right-click the software package, and then click **Remove**.

5 In the Remove Software dialog box, check **Immediately uninstall the software from users and computers**, and then click **OK**.

6 Close the Group Policy Object Editor window, and then close the Group Policy Management window.

The software uninstalls when the client computers are restarted.

Starting the Symantec Endpoint Protection client

You can start the client user interface on both managed and unmanaged clients using the Windows Start menu. You can also double-click the icon in the Windows taskbar.

Windows Server 2008 Server Core provides only a command-line interface. You can start the client user interface manually by executing the SymCorpUI.exe file that is stored in the Symantec Endpoint Protection installation folder.

To start the Symantec Endpoint Protection client

- Do one of the following:
  - On the Windows Start menu click **Start > All Programs > Symantec Endpoint Protection > Symantec Endpoint Protection**.

- On the Windows Start menu click **Start > All Programs > Symantec Network Access Control > Symantec Network Access Control**.
- On the Windows taskbar in the notification area, double-click the Symantec Endpoint Protection or Symantec Network Access Control icon.

To start the Symantec Endpoint Protection client on Windows Server 2008 Server Core

1. At a command prompt, do one of the following:
   - On 32-bit Windows Server 2008 Server Core servers, run the following command:
     ```
     cd C:\Program Files\Symantec\Symantec Endpoint Protection Manager
     ```
   - On 64-bit Windows Server 2008 Server Core servers, run the following command:
     ```
     cd C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager
     ```
2. Run the following command:
   ```
   symcorpui
   ```

About uninstalling the Symantec Endpoint Protection client

You can uninstall client software with the Windows Add and Remove utility. If you uninstall Symantec Endpoint Protection client software that runs a policy that blocks hardware devices, the devices are still blocked after you uninstall the software. To unblock the devices, use the Windows Device Manager.

Uninstalling client software on Windows Server 2008 Server Core

The Server Core installation of Windows Server 2008 offers a command-line interface only. You can, however, manage Server Core installations by using remote management tools.

To uninstall client software on Windows Server 2008 Server Core

1. Start Registry Editor by using the Regedit command.
2. Navigate to the following key:

   HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall

3 Select and copy the Key name of the {uninstall-string} key for Symantec Endpoint Protection.

4 At a command prompt, execute the following command:

```
msiexec.exe /x {uninstall_string}
```

Chapter 6

Installing Quarantine and LiveUpdate servers

This chapter includes the following topics:

About installing and configuring the Central Quarantine

The Quarantine Server receives virus and security risk submissions from Symantec Endpoint Protection clients and forwards these submissions to Symantec. The Quarantine Console lets you manage the Quarantine Server and these submissions. If you determine that your network requires a central location for all quarantined files, you can install the Central Quarantine.

The Central Quarantine is composed of the Quarantine Server and the Quarantine Console. The Quarantine Console and the Quarantine Server can be installed on the same or different supported Windows computers.

Note: If you install the Quarantine Server or Quarantine Console from the individual installation folders on the CD, you must run Setup.exe rather than run the .msi file. You use Setup.exe to ensure that all of the files that Windows Installer requires are installed on the destination computer before the .msi installation package runs.

For more information, see the *Symantec Central Quarantine Implementation Guide* on the product disc.

Installation of the Central Quarantine requires the following tasks in the following order:

- Installing the Quarantine Console
- Installing the Quarantine Server
- Configuring groups to use the Central Quarantine

Note: You install the Quarantine Console first and then you install the Quarantine Server. Then you restart the Quarantine Server.

Installing the Quarantine Console

The Quarantine Console lets you manage submissions to the Quarantine Server.

See "About installing and configuring the Central Quarantine" on page 123.

To install the Quarantine Console

1. On the computer on which the Symantec Endpoint Protection Manager console is installed, insert the installation CD into the CD-ROM drive.

   If your computer is not set automatically to run a CD, you must manually run Setup.exe.
2. In the main panel, click **Install Other Administrator Tools > Install Central Quarantine Console**.
3. Follow the on-screen instructions to complete the installation.

Installing the Quarantine Server

The Quarantine Server receives virus submissions. The Quarantine Server requires a restart after installation.

See "About installing and configuring the Central Quarantine" on page 123.

To install the Quarantine Server

1. On the computer on which you want to install the Quarantine Server, insert the installation CD into the CD-ROM drive.

   If your computer is not set automatically to run a CD, you must manually run Setup.exe.
2. Click **Install Other Administrator Tools > Install Central Quarantine Server**.
3. In the Welcome panel, click **Next**.

4. In the License Agreement panel, click **I accept the terms in the license agreement**, and then click **Next**.
5. In the Destination Folder panel, do one of the following actions:
   - To accept the default destination folder, click **Next**.
   - Click **Change**, locate and select a destination folder, click **OK**, and then click **Next**.
6. In the Setup Type panel, select the following:
   - **Internet based (Recommended)**, and then click **Next**.

   The email option is no longer supported.
7. In the Maximum Disk Space panel, type the amount of disk space to make available on the server for Central Quarantine submissions from clients, and then click **Next**.
8. In the Contact Information panel, type your company name, your Symantec contact ID/account number, and contact information, and then click **Next**.
9. In the Web Communication panel, change the gateway address if necessary, and then click **Next**.

   By default, the Gateway Name field is filled in with the gateway address.
10. In the Alerts Configuration panel, check **Enable Alerts** to use AMS, and then click **Next**.
11. In the Ready to Install the Program panel, click **Install**, and then follow the prompts to complete the installation.
12. Write down the IP address or host name of the computer on which you installed the Quarantine Server and the port number.

    This information is required when you configure client programs to forward items to the Central Quarantine.

Configuring groups to use the Central Quarantine

To configure Central Quarantine network communications, you must specify the port on which the Quarantine Server listens. You must also create and apply an Antivirus and Antispyware Policy that specifies the Quarantine Server computer and port. You configure the Quarantine Server listening port with the Symantec Quarantine Console, and you create the policy with the Symantec Endpoint Protection Manager console.

Note: The Quarantine Console user interface lets you select the IP protocol or the SPX protocol and specify the port number to configure. This IP protocol and port number is TCP. Do not select SPX. The TCP port number that you enter is not what appears for the server's port when you use tools like netstat -a. For example, if you enter port number 33, netstat -a displays TCP port 8448. The hexadecimal numbers and the decimal numbers misconvert and transpose. For more details, see: Quarantine Server appears to be using a different port than it is configured to use

See "About installing and configuring the Central Quarantine" on page 123.

To configure the Quarantine Server

1. In the Symantec Central Quarantine console, in the left pane, in the Console Root tree, right-click **Symantec Central Quarantine**, and then click **Properties**.
2. On the General tab, under Protocols, check **Listen on IP**.

   SPX is no longer supported.
3. In the Listen on IP Port box, type the port number on which to listen for client submissions.

   This port number is TCP/IP. Do not enter an IANA well-known port number without doing research to see if it is used in your network. For example, do not enter port number 21 because it is reserved for FTP communications.
4. Click **OK**.

To configure an Antivirus and Antispyware Policy

1. In the Symantec Endpoint Protection Manager console, click **Policies**.
2. In the View Policies pane, click **Antivirus and Antispyware**.
3. In the Tasks pane, click **Add an Antivirus and Antispyware Policy**.

   You can also edit an existing policy.
4. In the Antivirus and Antispyware Policy window, in the left pane, click **Submissions**.
5. Under Quarantined Items, check **Allow client computers to automatically submit quarantined items to a Quarantine Server**.
6. In the Server name box, type the fully qualified domain name or IP address of the Quarantine Server.
7. In the Port number box, accept or change the default port number.

8 In the Retry box, accept or change the retry interval to use when client to Quarantine Server communications fail.

9 Click **OK**.

10 On the Assign Policy warning dialog, click **Yes**.

11 Select the groups for the policy, and then click **Assign**.

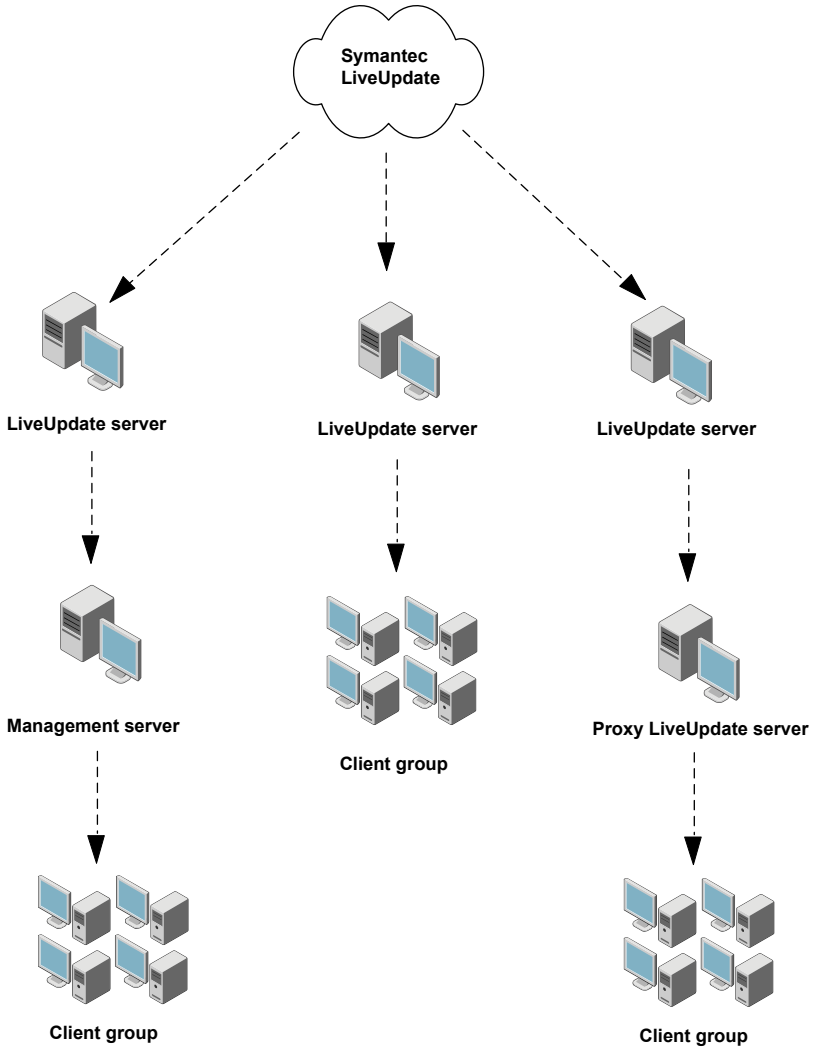
12 Click **Yes** to confirm the policy changes.

About using a Symantec LiveUpdate server

LiveUpdate is the utility that updates client computers with antivirus definitions, intrusion detection signatures, product patches, and so on. In unmanaged environments, LiveUpdate on client computers is typically configured to connect directly to Symantec LiveUpdate servers. In managed environments of small-to-medium networks, LiveUpdate on client computers is typically configured to connect to a Symantec Endpoint Protection Manager.

In large managed networks, bandwidth conservation issues through Internet gateways can be very important. When these issues are important, you can install and configure one or more LiveUpdate servers to download updates. Then you can distribute the updates to management servers or directly to clients.

Figure 6-1 LiveUpdate distribution architectures



The architecture on the left is the simplest to implement. To implement this architecture, you modify a setting for the management site. The architecture in the center is a little more difficult to implement. To implement this architecture, you modify a setting for the management site and modify the LiveUpdate Policy that is applied to the group. The architecture on the right is the most difficult to implement with the addition of the LiveUpdate proxy server.

For more information about the implementation of LiveUpdate architectures, see the *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control*.

For the latest configuration procedures for a LiveUpdate server, refer to the *Symantec LiveUpdate Administrator Getting Started Guide* in the Documentation folder on the product disc.

Section 3

Migrating and upgrading

Chapter 7

Upgrading to the latest Maintenance Release

This chapter includes the following topics:

Upgrading to a new release of Symantec Endpoint Protection or Symantec Network Access Control

You can upgrade to the latest maintenance release of Symantec Endpoint Protection or Symantec Network Access Control. Before you install a new version

of the software, you must perform certain tasks as part of your upgrade plan to ensure a successful upgrade.

The information in this section is specific to upgrading software in environments where a version of Symantec Endpoint Protection or Symantec Network Access Control 11.x is already installed.

Table 7-1 Process for upgrading to the latest maintenance release

Step	Action	Description
Step 1	Back up the database	Back up the database used by the Symantec Endpoint Protection Manager to ensure the integrity of your client information. See "Backing up the database" on page 134.
Step 2	Turn off replication	Turn off replication on all sites that are configured as replication partners. This avoids any attempts to update the database during the installation. See "Turning off replication before upgrading or migrating" on page 136.
Step 3	Stop the Symantec Endpoint Protection Manager service	The Symantec Endpoint Protection Manager service must be stopped during the installation. See "Stopping the Symantec Endpoint Protection Manager service" on page 137.
Step 4	Upgrade the Symantec Endpoint Protection Manager software	Install the new version of the Symantec Endpoint Protection Manager on all sites in your network. The existing version is detected automatically, and all settings are saved during the upgrade. See "Upgrading the Symantec Endpoint Protection Manager" on page 137.
Step 5	Turn on replication after the upgrade	Turn on replication when the installation is complete to restore your configuration. See "Turning on replication after migration or upgrade" on page 138.
Step 6	Upgrade Symantec client software	Upgrade your client software to the latest version. See "About upgrading client software" on page 139.

Backing up the database

Before you upgrade, you should back up the database.

See "Upgrading to a new release of Symantec Endpoint Protection or Symantec Network Access Control" on page 133.

Warning: When you restore a database backup, you must use the same version of Symantec Endpoint Protection Manager that you used to create the backup.

Note: The path in the Windows Start menu that is used in this section may vary depending on the version of Windows that you use.

To back up the database

1. On the Windows Start menu, click **Start > Programs > Symantec Endpoint Protection Manager > Database Back Up and Restore**.
2. In the Database Backup and Restore dialog, click **Back Up**.
3. When the Message prompt appears, click **Yes**.
4. When the backup completes, click **OK**.

   This backup may take a few minutes. The backup files are .zip files that are saved in \\Program Files\Symantec\Symantec Endpoint Protection Manager\data\backup\.
5. In the Database Backup and Restore dialog, click **Exit**.

Migrating to Microsoft SQL Server 2008 from a previous version

You must reconfigure the Symantec Endpoint Protection Manager after you migrate to SQL Server 2008 from a previous version of SQL Server.

To reconfigure Symantec Endpoint Protection Manager after migration to Microsoft SQL 2008

1. Click **Start > All Programs > Symantec Endpoint Protection Manager > Management Server Configuration Wizard.**
2. On the Welcome panel, check **Reconfigure the management server** and then click **Next**.
3. Make sure that the following information is retained from the previous Symantec Endpoint Protection Manager installation:
   - Server name
   - Server port

- Web console port
- Server data folder

4 Click **Next**.

5 On the **Database type** selection panel, click **Microsoft SQL Server** and then click **Next**.

6 Make sure that the following database parameters are correct:

- Database server
- SQL server port
- Database name
- Authentication
  See "About SQL Server database authentication modes" on page 73.
- User and Password

7 In the **SQL Client folder** dialog box, type the SQL Client folder location. The SQL Client folder is typically located in one of the following locations:

- SQL 2000: C:\Program Files\Microsoft SQL\Server\80\Tools\Binn
- SQL 2005: C:\Program Files\Microsoft SQL\Server\90\Tools\Binn
- SQL 2008: C:\Program Files\Microsoft SQL\Server\100\Tools\Binn

8 Click **Next** and then complete the wizard with no other changes.

See "Upgrading to a new release of Symantec Endpoint Protection or Symantec Network Access Control" on page 133.

Turning off replication before upgrading or migrating

If your site uses replication, you must turn off replication before you upgrade Symantec Endpoint Protection Manager. You must turn off replication at each site that is configured as a replication partner.

See "Upgrading to a new release of Symantec Endpoint Protection or Symantec Network Access Control" on page 133.

To turn off replication

1 Log on to the Symantec Endpoint Protection Manager console.

2 On the Servers tab, in the left pane, expand Local Site, and then expand Replication Partners.

3 For each site that is listed under Replication Partners, right-click the site, and then click **Delete**.

4 In the Delete Partner prompt, click **Yes**.

5 Log off the console, and repeat this procedure at all sites that replicate data.

Stopping the Symantec Endpoint Protection Manager service

Before you upgrade, you must manually stop the Symantec Endpoint Protection Manager service on every management server in your site. After you upgrade, the service starts automatically.

Warning: You must stop the Symantec Endpoint Protection Manager service before you perform this procedure or you corrupt your existing installation of Symantec Endpoint Protection Manager.

See "Upgrading to a new release of Symantec Endpoint Protection or Symantec Network Access Control" on page 133.

To stop the Symantec Endpoint Protection Manager service

1 Click **Start > Settings > Control Panel > Administrative Tools > Services**.

2 In the Services window, under Name, scroll to and right-click **Symantec Endpoint Protection Manager**.

3 Click **Stop**.

4 Close the Services window.

Warning: Close the Services window or your upgrade can fail.

5 Repeat this procedure for all installations of Symantec Endpoint Protection Manager.

Upgrading the Symantec Endpoint Protection Manager

You must upgrade the Symantec Endpoint Protection Manager that is defined as the primary site. You must also upgrade the software on all servers you plan to configure as additional sites, such as replication partners.

See "Upgrading to a new release of Symantec Endpoint Protection or Symantec Network Access Control" on page 133.

To upgrade Symantec Endpoint Protection Manager

1. In the server to upgrade, insert one of the following product discs, and start the installation:
   - Symantec Endpoint Protection
   - Symantec Network Access Control
2. Do one of the following:
   - In the Symantec Endpoint Protection panel, click **Install Symantec Endpoint Protection Manager**.
   - In the Symantec Network Access Control panel, click **Install Symantec Network Access Control**, and then click **Install Symantec Endpoint Protection Manager**.
3. In the Welcome panel, click **Next**.
4. In the License Agreement panel, click **I accept the terms in the license agreement**, and then click **Next**.
5. In the Ready to Install the Program panel, click **Install**.

   In the Install Wizard Completed panel, click **Finish**.

   The Management Server Upgrade Wizard starts.
6. In the Management Server Upgrade Wizard Welcome panel, click **Next**.
7. In the Information panel, click **Continue**.
8. When the Upgrade completes, click **Next**.
9. In the Upgrade Succeeded panel, click **Finish**.
10. Delete the Internet Explorer temporary files to assure that the updated files are used when you log on to the console.

Turning on replication after migration or upgrade

After you migrate or upgrade the servers that used replication, you must turn on replication. After migration, you add a replication partner to enable replication. You must add replication partners only on the computer on which you first installed the management server. Replication partners automatically appear on the other management servers.

See "Upgrading to a new release of Symantec Endpoint Protection or Symantec Network Access Control" on page 133.

To turn on replication after migration or upgrade

1. Log on to the Symantec Endpoint Protection Manager console if you are not logged on.
2. On the Servers tab, in the left pane, expand **Local Site**, and then expand **Replication Partners**.
3. For each site that is listed under Replication Partners, right-click the site, and then click **Add Partner**.
4. In the Add Replication Partner panel, click **Next**.
5. In the Remote Site Information panel, enter the identifying information about the replication partner, enter the authentication information, and then click **Next**.
6. In the Schedule Replication panel, set the schedule for when replication occurs automatically, and then click **Next**.
7. In the Replication of Log Files and Client Packages panel, check the items to replicate, and then click **Next**.

   Package replication uses large amounts of traffic and hard disk space.
8. In the Completing the Add Replication Partner Wizard panel, click **Finish**.
9. Repeat this procedure for all computers that replicate data with this computer.

About upgrading client software

You can use several methods to upgrade Symantec client software. Some methods can take up to 30 minutes. Therefore, you may want to upgrade client software when most users are not logged on to their computers.

Table 7-2 Methods to upgrade Symantec Endpoint Protection and Symantec Network Access Control client software

Upgrade method	Description
AutoUpgrade	Use AutoUpgrade to update clients in one or more groups from the Symantec Endpoint Protection Manager console. See "Upgrading clients by using AutoUpgrade" on page 140.
LiveUpdate Settings Policy	Configure a LiveUpdate Settings Policy for a group that defines a LiveUpdate server and allows clients to run LiveUpdate. See "Updating client software with a LiveUpdate Settings Policy" on page 141.

Table 7-2 Methods to upgrade Symantec Endpoint Protection and Symantec Network Access Control client software *(continued)*

Upgrade method	Description
Product disc	Use the installation program on the product disc to install a new version of the client.
Other methods	Use one of the other supported methods of installing client software. See "About Symantec client installation software" on page 96.

If the Symantec Network Access Control client is also installed, you should upgrade both the Symantec Endpoint Protection client and the Symantec Network Access Control client. You can assign both the Symantec Endpoint Protection package and the Symantec Network Access Control package to the same group. In this case, make sure that the Maintain Features option is selected.

See "Upgrading to a new release of Symantec Endpoint Protection or Symantec Network Access Control" on page 133.

Upgrading clients by using AutoUpgrade

The AutoUpgrade process lets you automatically upgrade the Symantec Endpoint Protection client software for all the clients that are contained in a group. For example, you can use AutoUpgrade to upgrade clients from the MR2 release to the MR3 release. You can also add a client installation package by using the client installation files from the product disc.

You must test the AutoUpgrade process before you attempt to upgrade a large number of clients in your production network. If you do not have a test network, you can create a test group. You can add a few non-critical clients to the test group and upgrade them by using AutoUpgrade. You can confirm the upgrade completed successfully by verifying the version number of the client software that appears in the About dialog box.

See "About upgrading client software" on page 139.

To upgrade clients by using AutoUpgrade

1. In the Symantec Endpoint Protection Manager console, click **Admin**.
2. Click **Install Packages**.
3. Under Tasks, click **Upgrade Groups with Package**.
4. In the Welcome to the Upgrade Groups Wizard panel, click **Next**.
5. In the Select Client Install Package panel, select the appropriate client installation package, and then click **Next**.

6 In the Specify Groups panel, select the groups that contain the client computers that you want to upgrade, and then click **Next**.

7 In the Package Upgrade Settings panel, select **Download from the management server**.

You can optionally stage and select a package on a Web server.

8 Click **Upgrade Settings**.

9 On the **General** tab, select **Maintain existing client features when updating**.

You can optionally add or remove features when upgrading.

10 Uncheck **Upgrade Schedule**.

This is required only when upgrading from versions earlier than MR2.

11 Optionally, on the **Notification** tab, customize the user notification settings. You can customize the message displayed on the client computer during the upgrade.

12 For more information about schedule and notification settings, click **Help**.

13 Click **OK**.

14 In the Upgrade Groups Wizard, click **Next**.

15 Click **Finish**.

Updating client software with a LiveUpdate Settings Policy

You can update Symantec client product software automatically by permitting product updates with a LiveUpdate Settings Policy. When product updates are permitted, patches are installed on clients when a LiveUpdate session runs. The session can be scheduled or manually started. When the policy is configured to deny product updates, client software can be updated only manually using the Symantec Endpoint Protection Manager console.

When the Symantec Endpoint Protection Manager downloads and processes LiveUpdate updates, it creates a microdef from the update when a group is updated. The microdef automatically appears as a new package. The new package appears in the Client Install Packages pane. You can then select the package and update groups and locations manually with the Upgrade Groups with Package feature.

See "About upgrading client software" on page 139.

To update Symantec client software with a LiveUpdate Settings Policy

1. In the Symantec Endpoint Protection Manager console, click **Policies**.
2. Under View Policies, click on and highlight **LiveUpdate**.
3. In the right pane, on the LiveUpdate Settings tab, click a LiveUpdate Policy.
4. In the lower-left pane, under Tasks, click **Edit the Policy**.
5. Under LiveUpdate Policy, click **Advanced Settings**.
6. In the Advanced Settings pane, under Product Update Settings, do one of the following:
   - To automatically update client software, check **Download Symantec Endpoint Protection product updates using a LiveUpdate server**.
   - To manually update client software with the Upgrade Groups with Package feature with the Symantec Endpoint Protection Manager console, uncheck **Download Symantec Endpoint Protection product updates using a LiveUpdate server**.
7. Click **OK**, and then apply the policy to a group or a location in a group.

About upgrading to Symantec Endpoint Protection or Symantec Network Access Control

Symantec Endpoint Protection Manager supports management and deployment of the following Symantec Endpoint Protection client software:

- Symantec Endpoint Protection
- Symantec Network Access Control

You can upgrade from Symantec Endpoint Protection with Symantec Network Access Control. You can also upgrade Symantec Network Access Control with Symantec Endpoint Protection. To do so, install the new version of the Symantec Endpoint Protection Manager on each server where the Symantec Endpoint Protection Manager is already installed.

Warning: You must stop the Symantec Endpoint Protection Manager service before upgrading your existing installation of Symantec Endpoint Protection Manager. If you do not, you may corrupt your existing installation of Symantec Endpoint Protection Manager.

About upgrading Symantec Endpoint Protection clients with Symantec Network Access Control

Symantec Endpoint Protection clients include Symantec Network Access Control and do not need to be upgraded. After you upgrade Symantec Endpoint Protection Manager for Symantec Network Access Control, you can apply Host Integrity Policies to your existing clients.

About upgrading Symantec Network Access Control clients with Symantec Endpoint Protection

You upgrade Symantec Network Access Control clients by installing Symantec Endpoint Protection on those clients. The installation automatically detects Symantec Network Access Control client, removes it, and then installs Symantec Endpoint Protection client software. You can deploy the client software by using any of the supported client deployment methods.

Chapter 8

Migrating Symantec AntiVirus and Symantec Client Security

This chapter includes the following topics:

Migrating from Symantec AntiVirus and Symantec Client Security

You can optionally migrate the computers that run Symantec legacy virus protection software. During migration, the database in Symantec Endpoint Protection Manager is populated with the group data and policy data from the legacy installation. The management server creates installation packages for the legacy clients.

You should test all migration procedures in a test environment before you migrate legacy Symantec AntiVirus and Symantec Client Security clients and servers.

Table 8-1 displays the process to migrate legacy client computers and servers.

Table 8-1 Migrating Symantec AntiVirus and Symantec Client Security clients and servers

Step	Description
Step 1: Uninstall the reporting servers	Uninstall the reporting servers, and optionally delete the database files. See "Uninstalling and deleting reporting servers" on page 156.

Table 8-1 Migrating Symantec AntiVirus and Symantec Client Security clients and servers *(continued)*

Step	Description
Step 2: Prepare the legacy installation	Use the Symantec System Center to configure settings for the management server and the clients that prepare them for migration. Use the following steps to prepare your legacy installation for migration: ■ Disable scheduled scans. The migration might fail if a scan is running during migration. See "Disabling scheduled scans" on page 152. ■ Modify the Quarantine purge options. See "Configuring Central Quarantine and quarantined files" on page 152. ■ Delete histories. See "Deleting histories" on page 153. ■ Disable LiveUpdate. Conflicts might occur if LiveUpdate runs on the client computers during migration. See "Disabling LiveUpdate" on page 153. ■ Turn off roaming service. Migration might hang and fail to complete if the roaming service is running on the client computers. See "Turning off the roaming service" on page 154. ■ Unlock server groups. Unpredictable results might occur if the server groups are locked. See "Unlocking server groups" on page 155. ■ Turn off Tamper Protection. Tamper Protection can cause unpredictable results during migration. See "Turning off Tamper Protection" on page 155. See your Symantec legacy virus protection software documentation for more information.
Step 3: Install Symantec Endpoint Protection Manager	Install Symantec Endpoint Protection Manager with either the embedded database or a SQL Server database. See "Installing and configuring the Symantec Endpoint Protection Manager with an embedded database" on page 65. See "Installing and configuring Symantec Endpoint Protection Manager with a SQL Server database" on page 74.

Table 8-1 Migrating Symantec AntiVirus and Symantec Client Security clients and servers *(continued)*

Step	Description
Step 4: Migrate legacy clients and servers	Read about migrating the legacy server groups and client groups and settings. See "About packages and deployment" on page 160. See "About migrating groups and settings from Symantec System Center" on page 157. See "About the settings that are not migrated" on page 160. Migrate the legacy server groups and client groups and settings. See "Migrating server and client group settings" on page 164.
Step 5: Uninstall the legacy management server	Uninstall the Symantec System Center.
Step 6. Verify migrated data	Verify and optionally adjust the migrated group settings and policy settings. In Symantec Endpoint Protection Manager, you can verify that: ■ The **LiveUpdate Settings Policy** and the **Antivirus and Antispyware Policy** for the management server and the client were properly migrated. If you modified disabled scheduled scans in the Symantec System Center for migration, you should change them back to the original settings. ■ The servers appear in the correct groups in the Symantec Endpoint Protection Manager console. See "About verifying the updates to your migrated policies" on page 167. For more information, see the *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control.*
Step 7: Deploy the client software	Install a client installation package on the computer that ran the Symantec System Center. You can use the wizard if you do not deploy client installation packages with third-party tools such as SMS. See "Configuring and deploying client software on Windows computers" on page 98.

Supported and unsupported migration paths

You must understand which migrations are supported, blocked, and unsupported. If you have the legacy software that blocks migration, you must uninstall this software. If you have the legacy software that is not supported for migration, decide whether or not to uninstall it. For example, if you run Symantec AntiVirus on Netware computers, you can continue to run your legacy software on those computers.

See "Migrations that are supported" on page 149.

See "Migrations that are blocked" on page 149.

See "Migrations that are not supported" on page 150.

Migrations that are supported

The client installation detects the following software and migrates the software if it is detected:

- Symantec AntiVirus client and server 9.x and later
- Symantec Client Security client and server 2.x and later

See "Migrations that are blocked" on page 149.

See "Migrations that are not supported" on page 150.

Migrations that are blocked

The client installation routines check for the existence of the following software and blocks migration if this software is detected:

- Symantec AntiVirus client and server 8.x and earlier
- Symantec Client Security client and server 1.x
- Symantec Client Firewall 5.0
- Symantec System Center, all versions
- Symantec Reporting Server 10.x
- Confidence Online Heavy by Whole Security, all versions
- Norton AntiVirus and Norton Internet Security, all versions

You must uninstall this software first and then install Symantec Endpoint Protection clients.

See "Migrations that are supported" on page 149.

See "Migrations that are not supported" on page 150.

Migrations that are not supported

The following software is not migrated and can coexist on the same computer as Symantec Endpoint Protection client software:

- Symantec Client Firewall Administrator, all versions
- LiveUpdate Server
  To install the latest version of LiveUpdate Server, you must first uninstall the legacy version.
- Netware computers that run any version of Symantec AntiVirus
  Netware operating systems are not supported with this version. You can continue to protect these computers with legacy versions.
- Symantec AntiVirus and Symantec Client Security client and the server that runs on Itanium hardware
  Itanium hardware is not supported with this version. Continue to protect these computers with legacy versions.

See "Migrations that are supported" on page 149.

See "Migrations that are blocked" on page 149.

Migrations that are supported and unsupported for the Mac client

Table 8-2 displays the products that can be migrated to the Symantec Endpoint Protection for Mac client.

Table 8-2 Migration paths from Symantec Endpoint Protection for Mac to the Symantec Endpoint Protection Mac client

Migrate from	Migrate to	Supported?
Managed Symantec AntiVirus for Mac client	Managed Symantec Endpoint Protection for Mac client	Yes
Unmanaged Symantec AntiVirus for Mac client	Unmanaged Symantec Endpoint Protection for Mac client	Yes
Unmanaged Symantec AntiVirus for Mac client	Managed Symantec Endpoint Protection for Mac client	Yes
Managed Symantec AntiVirus for Mac client	Unmanaged Symantec Endpoint Protection for Mac client	Yes, but managed client settings are retained.

Table 8-2 Migration paths from Symantec Endpoint Protection for Mac to the Symantec Endpoint Protection Mac client *(continued)*

Migrate from	Migrate to	Supported?
Norton AntiVirus for Mac	Managed or unmanaged Symantec Endpoint Protection for Mac client	No. Client must uninstall Norton products before installing Symantec Endpoint Protection.

See "Migrating from Symantec AntiVirus for Macintosh" on page 166.

About migrating Central Quarantine

To migrate Central Quarantine Console and Server, you must uninstall the current version and then install the new version of both components.

Preparing legacy installations for migration

With the Symantec System Center, you must change settings for clients and servers to simplify the migration process. For example, if a client runs an antivirus scan during migration, migration is blocked until the scan finishes and the migration may fail. Also, you need to disable the uninstallation password feature for client software if it is enabled. If you do not, users are prompted to enter the password in interactive mode.

Note: If you migrate groups and settings from the Symantec System Center, the policies that are migrated for those groups include these modifications. You may want to revert these settings after the migration. For example, you may want to turn on scheduled scans. Also, you do not need to disable the uninstall password if it is enabled. The migration ignores the password.

Preparing Windows legacy installations

These procedures apply to all legacy Windows software installations that are supported for migration.

Note: If you use client groups that do not inherit settings, prepare these groups the same way that you prepare server groups and management servers.

Disabling scheduled scans

If a scan is scheduled to run and is running while the client migration occurs, migration may fail. A best practice is to disable scheduled scans during migration and then enable after migration.

See "Migrating from Symantec AntiVirus and Symantec Client Security" on page 146.

To disable scheduled scans

1. In the Symantec System Center, do one of the following actions:
   - Right-click a management server.
   - Right-click a client group.
2. Click **All Tasks > Symantec AntiVirus > Scheduled Scans**.
3. In the Scheduled Scans dialog box, on the Server Scans tab, uncheck all scheduled scans.
4. On the Client Scans tab, uncheck all scheduled scans, and then click **OK**.
5. Repeat this procedure for all primary management servers, secondary management servers, and all client groups.

Configuring Central Quarantine and quarantined files

Quarantine server no longer supports updates to client computers with the latest definitions. Therefore, you do not want it to update client computers with the latest definitions during a migration. Also, quarantined file migration is not necessary.

See "Migrating from Symantec AntiVirus and Symantec Client Security" on page 146.

To configure Central Quarantine and quarantined files

1. In the Symantec System Center, right-click a server group.
2. Click **All Tasks > Symantec AntiVirus > Quarantine Options**.
3. In the Quarantine Options dialog box, click **Purge Options**.
4. In the Purge Options dialog box, set all time values to 1 day and set all directory size limit values to 1 MB. Check all check boxes.
5. Click **OK**.
6. In the Quarantine Options dialog box, uncheck **Enable Quarantine or Scan and Deliver**.

7 Under When new virus definitions arrive, check **Do nothing**, and then click **OK**.

8 Repeat this procedure for all server groups if you have more than one.

Deleting histories

All histories are now stored in a database. History file deletion speeds the migration process.

See "Migrating from Symantec AntiVirus and Symantec Client Security" on page 146.

To delete histories

1 In the Symantec System Center, right-click a server group.

2 Click **All Tasks > Symantec AntiVirus > Configure History**.

3 In the History Options dialog box, change the Delete after values to 1 day.

4 Click **OK**.

5 Repeat this procedure for all server groups if you have more than one.

Disabling LiveUpdate

If LiveUpdate runs on client computers during migration, conflicts may occur. Therefore, you must turn off LiveUpdate on client computers during migration.

See "Migrating from Symantec AntiVirus and Symantec Client Security" on page 146.

To turn off LiveUpdate

1 In the Symantec System Center, right-click a server group.

2 Click **All Tasks > Symantec AntiVirus > Virus Definition Manager**.

3 In the Virus Definition Manager dialog box, check **Update only the primary server of this server group**, and then click **Configure**.

4 In the Configure Primary Server Updates dialog box, uncheck **Schedule for Automatic Updates**, and then click **OK**.

5 In the Virus Definition Manager dialog box, uncheck the following selections:

- **Update virus definitions from parent server**
- **Schedule client for automatic updates using LiveUpdate**
- **Enable continuous LiveUpdate**

6 Check **Do not allow client to manually launch LiveUpdate**, and then click **OK**.

7 Repeat this procedure for all server groups if you have more than one.

Turning off the roaming service

If the roaming service is running on client computers, the migration might hang and fail to complete. If the roaming service is turned on, you must turn it off before starting the migration.

Note: If your roaming clients run Symantec AntiVirus version 10.x, you must unlock your server groups before you disable the roaming service. This practice helps ensure that roaming clients are properly authenticated with certificates to their parent server.

See "Migrating from Symantec AntiVirus and Symantec Client Security" on page 146.

To turn off the roaming service

1 In the Symantec System Center, right-click a server group.

2 Click **All Tasks > Symantec AntiVirus > Client Roaming Options**.

3 In the Client Roaming Options dialog box, in the Validate parent every minutes box, type **1**.

4 In the Search for the nearest parent every minutes box, type **1**, and then press **OK**.

5 Wait a few minutes.

6 In the Symantec System Center, right-click a server group.

7 Click **All Tasks > Symantec AntiVirus > Client Roaming Options**.

8 In the Client Roaming Options dialog box, uncheck **Enable roaming on clients that have the Symantec AntiVirus Roaming service installed**.

9 Click **OK**.

About preparing Symantec 10.x/3.x legacy installations

Symantec AntiVirus 10.x and Symantec Client Security 3.x provide the additional features that must be properly configured for successful migration.

See "Unlocking server groups" on page 155.

See "Turning off Tamper Protection" on page 155.

See "Uninstalling and deleting reporting servers" on page 156.

Unlocking server groups

If you do not unlock server groups before migration, unpredictable results may occur. Also, if the roaming service is enabled for clients, the unlocking the server group helps ensure that the clients properly authenticate to a parent server. Clients that properly authenticate to a parent server get placed in the database. Clients that get placed in the database automatically appear in the correct legacy group in the console after installation.

See "Migrating from Symantec AntiVirus and Symantec Client Security" on page 146.

To unlock a server group

1. In the Symantec System Center, right-click a locked server group, and then click **Unlock Server Group**.
2. In the Unlock Server Group dialog box, type the authentication credentials if necessary, and then click **OK**.

Turning off Tamper Protection

Tamper Protection can cause unpredictable results during migration. You must turn off Tamper Protection before starting the migration.

See "Migrating from Symantec AntiVirus and Symantec Client Security" on page 146.

To turn off Tamper Protection

1. In the Symantec System Center, right-click one of the following categories:
   - Server group
   - Primary or secondary management server
2. Click **All Tasks > Symantec AntiVirus > Server Tamper Protection Options**.
3. In the Server Tamper Protection Option dialog box, uncheck **Enable Tamper Protection**.
4. Click **OK**.
5. Do one of the following actions:
   - If you selected a server group, repeat this procedure for all server groups if you have more than one.
   - If you selected a management server, repeat this procedure for all management servers in all server groups.

Uninstalling and deleting reporting servers

If you installed one or more reporting servers, you must uninstall these reporting servers, and optionally delete the database files. You must also delete reporting servers from the Symantec System Center. Complete reporting server uninstallation information is available in the Symantec System Center Online Help. Legacy settings were stored in the Windows registry. All settings are now stored in a database along with the reporting data.

See "Migrating from Symantec AntiVirus and Symantec Client Security" on page 146.

To uninstall reporting servers

1. Log on to a computer that runs the reporting server.
2. Click **Start > Settings > Control Panel > Add or Remove Programs**.
3. In the Add or Remove Programs dialog box, click **Symantec Reporting Server**, and then click **Remove**.
4. Follow the on-screen prompts until you delete the reporting server.
5. Repeat this procedure for all reporting servers.

To delete reporting servers from the Symantec System Center

1. In the Symantec System Center, right-click and expand **Reporting**.
2. Right-click each reporting server, and then click **Delete**.

About migrating and not preserving server and client groups and settings

You are not required to migrate groups and settings for legacy clients and servers from the Symantec System Center to the Symantec Endpoint Protection Manager. If you are comfortable with Symantec Endpoint Protection Manager console operations, you can create and export an installation package and deploy it to your legacy clients and servers for migration.

See "Creating client installation packages" on page 104.

Note: A best practice is to create one or more groups and associated policies for your legacy clients and migrate them first. You can then create one or more groups and associated policies for your legacy servers and then migrate them to clients. Finally, you uninstall the Symantec System Center and migrate the legacy management server or client that protected the computer that ran the Symantec System Center.

About migrating groups and settings from Symantec System Center

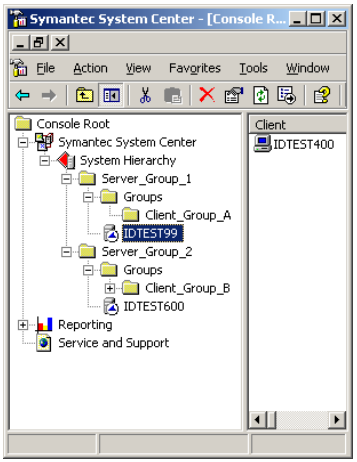
To migrate server and client groups and settings from the Symantec System Center to the Symantec Endpoint Protection Manager, you must read about and understand how this process works. For example, your existing settings in the Symantec System Center may or may not be inherited from server groups. You have to choose whether or not to preserve this inheritance.

Legacy primary and secondary management servers have the settings that apply only to those servers and not to the clients that they manage. The reason is that these servers may need to be protected differently than how the clients that they manage are protected. For example, these servers may provide other services that may need to have certain files types excluded from scans. With the Symantec System Center, you can specify that all servers inherit their settings from those specified for the server group. Or, you can specify custom settings for each server.

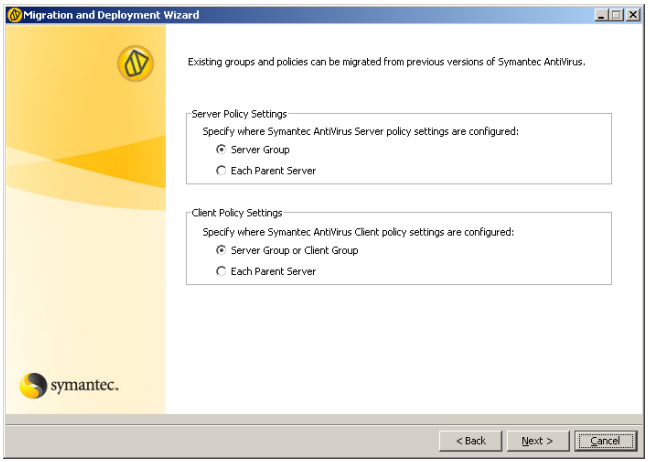
After you migrate settings for management servers, these settings appear in the LiveUpdate Settings Policy and the Antivirus and Antispyware Policies. These policies are applied to the groups that contain the management servers after you migrate them to a Symantec Endpoint Protection client. During migration you decide whether these settings are inherited from the server group, or are specified for each server.

Legacy client settings can also be inherited from the server group or inherited from a management server. After you migrate settings for clients, these settings appear in the LiveUpdate Settings Policy and the Antivirus and Antispyware Policies. During migration you decide whether these setting are inherited from the server group or from the management server.

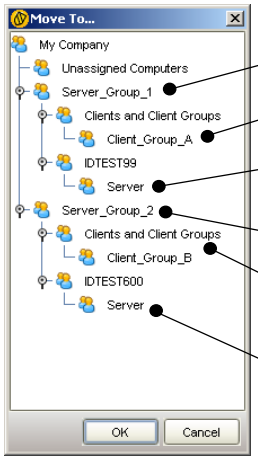
Figure 8-1 Before and after settings that are inherited from server groups



Symantec System Center before migration



Client policy migration setting selection



All client computers that are not in a client group appear here

Client computers in client groups appear here

Each parent server migrated to a client appears in Server

All client computers in this group share all policies

Client group policy inheritance matches the inheritance setting from the Symantec System Center

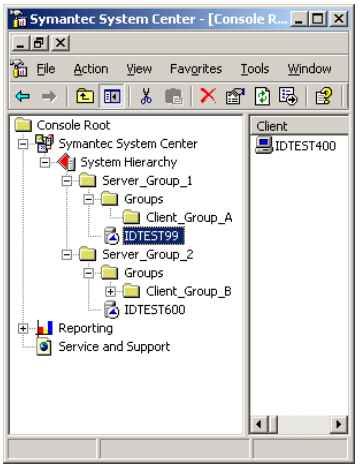
Server group inherits policies from Server_Group_2

Symantec Endpoint Protection Manager Console after settings migration and client deployment

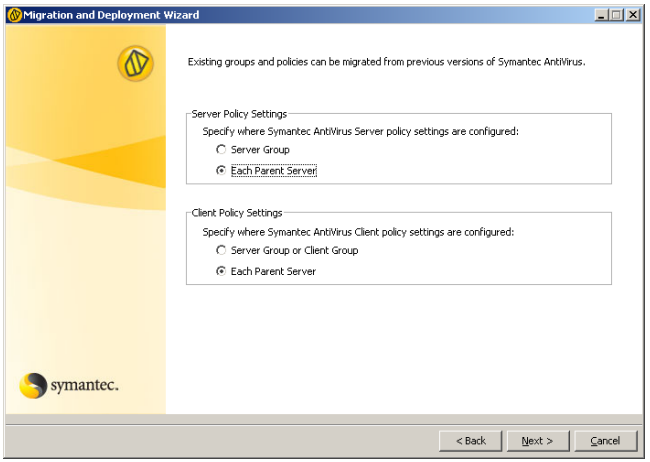
In this scenario, all management servers in Server_Group_1 and Server_Group_2 inherit settings from the server group in the Symantec System Center. After migration to Symantec Endpoint Protection client, each computer that ran a legacy management server appears in a group that is named Server. That group inherits all settings from the group with the same name as the original server group. For example, management server IDTEST99 inherits the policies that are set for Server_Group_1.

In this scenario, all clients inherit the settings from the server group and from any client group that might contain them. All clients that were not contained in a client group in the Symantec System Center, now appear in the group with the same name as the original server group.

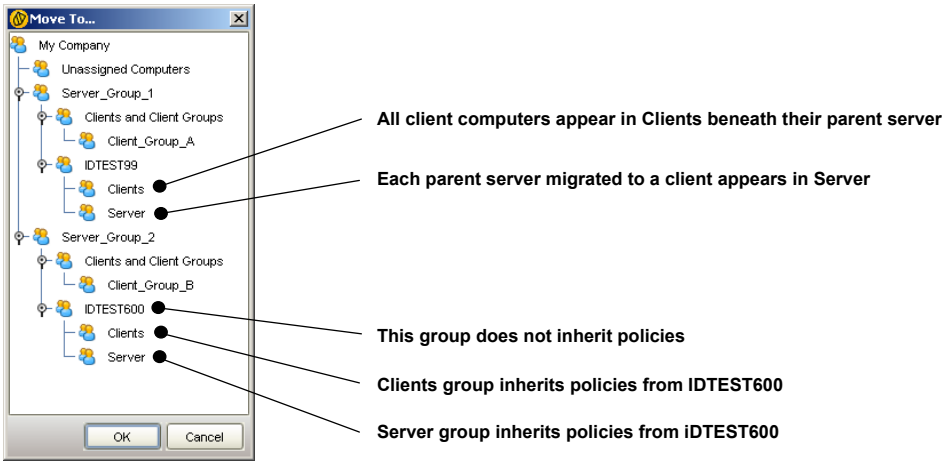
Figure 8-2 Before and after settings that are inherited from parent servers



Symantec System Center before migration



Client policy migration setting selection



Symantec Endpoint Protection Manager Console after migration and client deployment

In this scenario, all management servers in Server_Group_1 and Server_Group_2 inherit settings from each parent server in the Symantec System Center. After migration to Symantec Endpoint Protection client, each computer that ran a legacy

management server appears in a group that is named Server. The groups do not inherit any settings. The new policies are customized for each computer that ran a legacy management server.

In this scenario, all clients inherit the settings that are set for clients at each parent server. If clients are in client groups in the Symantec System Center, they now appear in the Clients group beneath the parent server group in which they were first installed.

About the settings that are not migrated

Tamper Protection settings are not migrated. Tamper Protection is now part of the General Settings for groups. Tamper Protection is not a policy that applies to Locations. By default, Tamper Protection is enabled and protects Symantec processes as well as internal objects. You can enable or disable Tamper Protection only. You do not have granular control over processes or internal objects.

Unlocked settings may or may not be migrated. If the settings are the original installed defaults that were never changed or locked, the settings are not migrated. The settings are not migrated because Windows registry entries were never generated. In some instances, the new Symantec Endpoint Protection default policy settings may correspond to the legacy defaults. In other instances, the new Symantec Endpoint Protection default policy settings may not correspond to the legacy defaults. A best practice is to review all settings that appear after migration in your Antivirus and Antispyware Policies and in your LiveUpdate Settings Policy.

About packages and deployment

To migrate server and client groups and settings from the Symantec System Center to the Symantec Endpoint Protection Manager, you must read about and understand how this process works. For example, your existing settings in the Symantec System Center may or may not be inherited from server groups. You have to choose whether or not to preserve this inheritance.

See "About the client installation packages that are generated during migration" on page 161.

See "Exporting and formatting a list of client computer names to migrate" on page 162.

See "About opening communications ports for migration" on page 163.

See "About preparing client computers for migration" on page 164.

Note: Client computers must run Internet Explorer 6.0 and MSI 3.1 or later or they cannot be migrated.

About the client installation packages that are generated during migration

To perform a migration, you run the Migration and Deployment Wizard. When you run the Migration and Deployment Wizard, you choose the management servers and clients for which to create client installation packages.

Note: Management servers migrate to clients.

After you install these client installation packages on your legacy clients, your migrated clients automatically appear in the appropriate group in the Symantec Endpoint Protection Manager console.

During migration, installation packages are automatically generated for several combinations of client components. For example, an installation package is generated for all Symantec Endpoint Protection features. An installation package is generated for Antivirus and Antispyware protection only, and so forth. These packages are created in a directory that you specify during migration.

In this directory, there are four directories that contain different installation packages with the following names:

- All Client Features_xx-bit
- Antivirus Features Only_xx-bit
- Network Threat Protection Features Only_xx-bit
- Antivirus and Proactive Threat Protection Features Only_xx-bit

For 32-bit installation packages, these packages take 300 MB of disk space and all packages are always generated automatically. For 64-bit installation packages, these packages take more than 300 MB of disk space.

When you use the Migration and Deployment Wizard, you choose whether or not to migrate all management servers and clients that appear in the Symantec System Center. Your other choice is to select individual management servers.

If you decide to migrate specific management servers, you should create separate package-creation directories for each management server or combination of management servers. Then, you can deploy these packages to the respective legacy clients for migration. The clients automatically appear in the correct group in the Symantec Endpoint Protection Manager console.

Note: When you migrate groups and settings, the Migration and Deployment Wizard stores the legacy management server and client IDs in a table in the Symantec Endpoint Protection Manager database. When you migrate legacy management servers and clients to Symantec Endpoint Protection, the newly migrated clients send their legacy IDs to the Symantec Endpoint Protection Manager. When the manager receives the legacy IDs, it places the newly migrated clients in the correct migrated group.

Exporting and formatting a list of client computer names to migrate

The recommended Symantec-supplied client package deployment tool is the Push Deployment Wizard. You can start this tool by double-clicking \Symantec Endpoint Protection\tomcat\bin\ClientRemote.exe. You can also choose to start the Push Deployment Wizard when you use the Migration and Deployment Wizard.

Note: You can use the technique that is described here whether or not you migrate settings from the Symantec System Center. This technique is useful to create lists of all of your legacy clients and servers and to import lists into the Push Deployment Wizard for deployment.

The Push Deployment Wizard automatically detects Windows computers that are powered on. The wizard then lets you select the computers and deploy a selectable installation package to the detected computers. You can select each computer one at a time or you can select the workgroup or domain of computers.

Your other option is to create a text file that contains the names or IP addresses of your legacy clients. Then you import that file into the Push Deployment Wizard for package deployment. You can then manually start the Push Deployment Wizard and deploy packages to clients in stages.

A best practice is to export a list of clients for each management server to a text file. Then you can open it in a spreadsheet and delete all columns except the column that contains the computer name or IP address. You can then save it back to a text file that you can import to the Push Deployment Wizard. This approach lets you deploy to clients by management server, staging your migration.

The downside to this approach is that the Push Deployment Wizard waits about 20 seconds for each computer in the list that is not turned on. The upside to this approach is that you can inspect the log file to see which computers were not turned on. Thus you have a record of which computers are not yet migrated. A best practice in DHCP-enabled environments is to use computer names rather than IP addresses, because the IP addresses can change.

Note: The following procedure provides details about how to use Microsoft Office Excel 2003. You are not required to use Excel. You can use any spreadsheet software that imports text files.

To export and format a list of client computer names to migrate

1. In the Symantec System Center, right-click one of the following, and then click **Export List**:
   - Primary or secondary management server
   - Client group
2. In the Export List dialog box, in the File name box, type a name of a text file.
3. In the Save as type drop-down list, select **Text (Tab Delimited) (*.txt)**, and then click **Save**.
4. Import the file into Microsoft Excel as a Tab delimited text file.

   The last line of the text file should be a computer name and not a blank line.
5. Copy the desired computer names from the Client column into a new a new text file, and then save the file.

About opening communications ports for migration

When you migrate server and client group settings, network communications occur between the Symantec System Center and Symantec Endpoint Protection Manager. If these components run on different computers, and if these computers run firewalls, you need to open communication ports.

Table 8-3 Communication ports used for migration

Symantec System Center	Symantec Endpoint Protection Manager
TCP 139, 445	Ephemeral TCP ports
Ephemeral TCP ports	TCP 139
UDP 137	UDP 137

When you use the Push Deployment Wizard to deploy Symantec Endpoint Protection client software, network communications occur between the legacy servers and clients and Symantec Endpoint Protection Manager. If the legacy servers and clients run firewalls, you must open communication ports.

Table 8-4 Ports used for client software deployment with the Push Deployment Wizard

Client computers	Symantec Endpoint Protection Manager
TCP 139 and 445	Ephemeral TCP ports
Ephemeral TCP ports	TCP 139 and 445
UDP 137, 138	UDP 137, 138

About preparing client computers for migration

Several Windows operating system features can interfere with a successful server and client migration. You need to understand what these features are and handle them appropriately. For example, the computers that run Windows XP and that are part of a Workgroup need to have simple file sharing disabled. If it is not disabled, you cannot authenticate to those computers for remote installation. Computers that run Windows XP that are in a Windows domain do not require that this feature be disabled.

You also need to understand that if you install a Symantec firewall, you disable the Windows firewall. If you do not select to install a Symantec firewall, you do not disable the Windows firewall. In addition, you may need to open ports or disable firewalls before migration.

See "About client firewalls and communication ports" on page 50.

See "About disabling and modifying Windows firewalls" on page 53.

See "About preparing Windows computers for remote deployment" on page 55.

See "Preparing your client computers for installation" on page 56.

Migrating server and client group settings

After you install Symantec Endpoint Protection Manager, you can migrate your management server and client groups. You are not required to migrate all server groups and client groups at the same time. Also, you can migrate management servers and the clients that report to them one at a time.

Note: All computers that do not run MSI 3.1 are migrated to MSI 3.1 first, before client software is installed. Computers that are not restarted after client software is installed are protected with antivirus and antispyware features, but not with firewall features. To implement the firewall features, client computers must be restarted.

To migrate server and client group settings

1. If the Migration and Deployment Wizard is not already open, click **Start > Programs > Symantec Endpoint Protection Manager > Migration and Deployment Wizard**.
2. In the Welcome to the Migration and Deployment Wizard panel, click **Next**.
3. In the What would you like to do panel, click **Migrate from Symantec AntiVirus**.
4. In the next unnamed panel, check the radio buttons that indicate how you want your settings to be applied to your groups.

   See "About migrating groups and settings from Symantec System Center" on page 157.
5. Click **Next**.
6. In the next unnamed panel, do one of the following:
   - To import all settings from all management servers and clients, click **Auto-detect Servers**, type the IP address of a computer that runs the Symantec System Center, and then click **OK**.
   - To import settings from a single management server and the clients that it manages, click **Add Server**, type the IP address of a computer that runs a management server. Then click **OK**.
7. Click **Next**.
8. In the next unnamed panel, click **Next**.
9. In the next unnamed panel, configure the client installation packages that you want to export.
10. Click **Advanced Package Options**, uncheck the packages that you do not want to create, and then click **OK**.
11. Click **Browse**, browse to and select a directory in which to export the client installation packages, and then click **Open**.
12. In the unnamed panel, click **Next**.
13. In the next unnamed panel, do one of the following:
    - Check **Yes**, click **Finish** to export the packages, and then deploy the packages first to clients and then to servers with the Push Deployment Wizard.

      The exporting process can take ten minutes or more.
    - Check **No, just create them and I'll deploy them later**, click **Finish** to export the packages, and then manually deploy the packages first to clients

and then to servers by using ClientRemote.exe from the \Symantec Endpoint Protection\tomcat\bin\ directory.
See "Deploying client software on Windows computers with the Push Deployment Wizard" on page 106.

Migrating from Symantec AntiVirus for Macintosh

You can migrate your groups and your antivirus policy settings from Symantec Administration Console for Macintosh to Symantec Endpoint Protection Manager. You can migrate as part of the installation process, or you can run the Migration and Deployment Wizard after you install.

This procedure creates Mac client installation packages that contain the same group and policy settings that you deployed by using Symantec AntiVirus for Macintosh. You must deploy the client packages manually, however.

See "About deploying Mac client installation packages" on page 100.

See "Migrations that are supported and unsupported for the Mac client" on page 150.

Warning: Before you run the Migration and Deployment Wizard, you must manually grant access to the Mac MySql database to Symantec Endpoint Protection Manager. You can perform these steps before or after you install Symantec Endpoint Protection Manager.

To migrate from Symantec AntiVirus for Macintosh

1. On the server where you run Symantec Administration Console for Macintosh, start MySql.

   Note: You must log on to the server as the root user.

2. Run the following command:

   ```
   GRANT ALL ON sacm.* TO root@IP address of the server where you installed Symantec Endpoint Protection Manager IDENTIFIED BY password
   ```

   where *password* can be any password that you create.

3. Start the Migration and Deployment Wizard, and click **Next**.
4. Choose **Migrate from Symantec AntiVirus for Macintosh**, and click **Next**.

5 Enter the required data for the database for Symantec Administration Console for Macintosh. Enter the user name and password that you provided in step 2.

6 Follow the on-screen instructions to complete migration.

About verifying the updates to your migrated policies

After you migrate your clients and servers, you must verify that they appear in the appropriate groups in the Symantec Endpoint Protection Manager console. Then, you can update your LiveUpdate Settings Policy and Antivirus and Antispyware Policies to revert some or all of the changes that you made to settings with the Symantec System Center. For example, to start the migration process, you turned off scheduled scans. You may want to turn on scheduled scans when the migration is complete.

About migrating unmanaged clients

You have three options for migrating unmanaged clients.

- You can install Symantec Endpoint Protection with the installation files and setup.exe that are contained on the product disc.
  This option preserves client settings.
- You can export a package from the Symantec Endpoint Protection Manager console in unmanaged mode.
  This option does not preserve client settings.
- You can export a package from the Symantec Endpoint Protection Manager console in unmanaged mode for non-.exe files. You then replace serdef.dat in this installation package with a blank file of the same name.
  This option preserves client settings.

Note: Microsoft Internet Explorer 6.0 or later, and MSI 3.1 or later must be installed on client computers or they cannot be migrated.

About migrating unmanaged clients with the product disc

If you have unmanaged legacy clients, you can migrate them to Symantec Endpoint Protection and keep them unmanaged. Migrating unmanaged clients with the CD files also preserves the settings on each client. If you run Setup.exe, you also automatically upgrade the MSI on the clients to 3.1, a requirement.

When you run Setup.exe to install Symantec Endpoint Protection to legacy unmanaged clients, legacy settings are retained. For example, if a user creates a custom scan to run at midnight, that setting is retained.

You can use the following options to migrate the unmanaged clients:

- Insert the product disc in the drive on each client computer to migrate, and install Symantec Endpoint Protection from the installation user interface.
  See "Installing unmanaged client software on Windows computers by using the product disc" on page 101.
- Copy the files from the SEP folder on the product disc to a shared folder. Then have the users on the client computers connect to the shared folder and run Setup.exe.
  See "About deploying client software on Windows computers from a mapped drive " on page 106.
- Deploy the files that are contained in the SEP folder on the product disc using the Push Deployment Wizard.
  See "Deploying client software on Windows computers with the Push Deployment Wizard" on page 106.
- Deploy the files that are contained in the SEP folder on the product disc using third-party distribution tools.
  See "Third-party installation options" on page 110.

Migrating unmanaged clients with exported packages

You can create installation packages with the Symantec Endpoint Protection Manager console for unmanaged clients. This type of package creates unmanaged clients after migration, but by default deletes and resets legacy client settings to new defaults. You can override this default by creating a new Serdef.dat file that is blank in your exported files. You cannot modify the Serdef.dat file if you export to a single executable installation file.

To migrate unmanaged clients with exported packages and preserve legacy settings

1. In the Symantec Endpoint Protection Manager console, click **Admin**.
2. Under Tasks, click **Install Packages**.
3. Under Client Install Packages, right-click the package to create, and then click **Export Package**.
4. In the Export Package dialog box, uncheck **Create a single .EXE file for this package** (required).
5. Click **Browse**, and select the directory to contain your exported package.

6 Under Security Setting, check **Export an unmanaged client** and uncheck **Export packages with policies from the following groups:**.

7 Click **OK**.

8 Deploy the package to your legacy clients.

See "Deploying client software on Windows computers with the Push Deployment Wizard" on page 106.

To migrate unmanaged clients with exported packages and change legacy settings to defaults

1 In the Symantec Endpoint Protection Manager console, click **Admin**.

2 Under Tasks, click **Install Packages**.

3 Under Client Install Packages, right-click the package to create, and then click **Export Package**.

4 In the Export Package dialog box, check **Create a single .EXE file for this package** (recommended but not required).

5 Click **Browse**, and select the directory to contain your exported package.

6 Under Security Setting, check **Export an unmanaged client**.

7 Click **OK**.

8 Deploy the package to your legacy clients.

See "Deploying client software on Windows computers with the Push Deployment Wizard" on page 106.

About new and updated features for legacy administrators

Several features have been updated from legacy protection products.

Table 8-5 New or updated features

Feature	Description
Server software does not provide Symantec AntiVirus protection	Symantec Endpoint Protection Manager does not include Symantec Endpoint Protection client software. To protect the management servers, you must install Symantec Endpoint Protection client software on the server. Legacy Symantec AntiVirus and Symantec Client Security servers included Symantec AntiVirus protection.

Table 8-5 New or updated features *(continued)*

Feature	Description
Client software user interface is redesigned	The client user interface has been redesigned.
Management console is redesigned	The Symantec System Center has been deprecated. The new management console is called the Symantec Endpoint Protection Manager console.
Secondary management servers are no longer used	Legacy management servers can be installed as secondary servers that report to a primary management server for a server group.
Group Update Providers	Symantec Endpoint Protection clients can be configured to provide signature and content updates to clients in a group. When clients are configured this way, they are called Group Update Providers. Group Update Providers do not have to be in the group or groups that they update.
Server groups can be thought of as sites	Legacy Symantec System Center operations revolved around server groups. Each group had a primary server and clients were ultimately managed by that primary server. Symantec Endpoint Protection uses the concept of a site. Multiple sites can be part of an installation instance. When you install additional sites in an installation instance, you do so by not specifying a secret key during installation. Every time you specify a secret key when you install a site, you create a new installation instance. Computers in different installation instances do not communicate with each other.
Location awareness is expanded	Legacy operations supported location awareness for firewall operations only. Symantec Endpoint Protection expands location awareness support to the group level. Each group can be divided into multiple locations, and when a client is in that location, policies can be applied to that location.
Policies now control most client settings	Legacy Symantec System Center operations let you apply a series of settings to groups of computers by using dialog boxes. Settings are now controlled with the policies that can be applied down to the location level. For example, two policies that affect LiveUpdate settings. One policy specifies how often LiveUpdate runs and controls user interaction. The other policy specifies the content that is allowed to be installed on client computers with LiveUpdate.
Grc.dat is no longer used	Legacy Symantec AntiVirus communications were governed by the presence of a Grc.dat file on client computers, which is deprecated.
Some settings are still set on groups	Some legacy Symantec System Center settings are still applied at the group level. For example, setting the client uninstall password applied to all computers in a group. Also, the new LiveUpdate Content Policy applies to the group.

Table 8-5 New or updated features *(continued)*

Feature	Description
NetWare servers are no longer supported	Legacy NetWare management servers are no longer supported. Do not migrate legacy NetWare management servers, but continue to manage them with legacy software.
Domains are now available for use	Domains let you create additional global groups if you want to use additional global groups. This feature is advanced and should be used only if necessary. The default domain is called Default.
Symantec Endpoint Protection now includes firewall support	Legacy products named Symantec Client Security included Symantec AntiVirus and Symantec Client Firewall. Symantec Endpoint Protection now includes a new, improved firewall and user interface.
Device blocking is now available	If you want to disable certain hardware devices on client computers, you can now configure policies to block user access to a list of hardware devices. These devices include items like USB ports and floppy disk drives, and modems. These devices also include items for which you should exercise caution. For example, you can disable network interface cards (NIC), which disable client computers from network communications, even with the Symantec Endpoint Protection Manager console. The only way to recover from this scenario is to uninstall Symantec Endpoint Protection and then enable the NIC with Windows Device Manager.
Symantec Client Firewall Administrator is no longer used	The Symantec Client Firewall Administrator was the tool that was used to create Symantec Client Firewall Policies. The new Symantec Endpoint Protection Manager console now integrates this functionality by default.
Failover and load balancing can be implemented for management servers	If you have a large network and need the ability to conserve bandwidth consumption, you can configure additional management servers in a load-balanced configuration. If you have a large network and need the ability to configure redundancy, you can configure additional management servers in a failover configuration.
Replication can be implemented between sites	If you have a large network and need replication, you can configure sites in an installation instance to replicate data. **Note:** When you install a site for replication, you do not specify a secret key. All sites that are installed with a secret key do not communicate with each other.
Alert Management Server is no longer used	Legacy product included an Alert Management Server that supported alerting. The new Symantec Endpoint Protection Manager now includes this functionality by default.
Client information is now stored in a database	Legacy products stored information in the Windows registry. Symantec Endpoint Protection Manager now stores all information about client computers in an SQL database (the embedded database or a Microsoft SQL database).

Table 8-5 New or updated features *(continued)*

Feature	Description
Enhanced LiveUpdate features	LiveUpdate now supports downloading and installation of a wide variety of content including definitions, signatures, white lists to prevent false positives, engines, and product updates.

Chapter 9

Migrating legacy Symantec Sygate software

This chapter includes the following topics:

About migrating to Symantec Endpoint Protection 11.x

You can migrate Symantec Sygate Enterprise Protection 5.1 and later and Symantec Network Access Control 5.1 and later to Symantec Endpoint Protection 11.x. No other legacy Sygate software is supported for this migration. To migrate older legacy Sygate software versions, you must first migrate them to Symantec Sygate Enterprise Protection 5.1.

Warning: When you migrate from version 5.1, you must select the option **Store client packages unzipped to provide better network performance for upgrades** for the upgrade to complete successfully.

About migrating Symantec Sygate server and management software

To migrate from a Sygate server to Symantec Endpoint Protection, install Symantec Endpoint Protection Manager for Symantec Endpoint Protection 11.x.

The legacy server and management software that you can migrate consists of the following products:

- Symantec Sygate Enterprise Protection 5.1 management server, console, and database

  The server components are called Symantec Policy Manager and Symantec Policy Management Console.
- Symantec Network Access Control 5.1 management server, console, and database

  The server components are also called Symantec Policy Manager and Symantec Policy Management Console.

The legacy product Symantec Sygate Enterprise Protection 5.1 includes all of the functionality that the legacy product Symantec Network Access Control 5.1 provides. The functionality subset that Symantec Network Access Control provides is Host Integrity Policies and Enforcer capabilities.

Note: Timestamp values in Host Integrity Policies may not properly migrate. After the migration, you must inspect all Host Integrity settings that are configured for time values and change them if necessary.

Symantec Endpoint Protection 11.x is similar to Symantec Sygate Enterprise Protection 5.1 with one exception. The exception is that Symantec Endpoint Protection does not include Host Integrity or Enforcer capabilities. If you migrate version 5.1 servers that provide Host Integrity or Enforcer capabilities, you must also purchase and install the Symantec Endpoint Protection Manager for Symantec Network Access Control 11.x. Install the Symantec Endpoint Protection Manager on the migrated servers to regain access to that functionality.

Note: Server migration migrates all existing policies and settings that are configured for the servers and site.

Supported server migration paths

The following software is supported for migration to Symantec Endpoint Protection Manager and Management Console for Symantec Endpoint Protection:

- Symantec Policy Manager and Management Console 5.1
  To gain access to the Host Integrity and Enforcer features, you must also install Symantec Endpoint Protection Manager for Symantec Network Access Control 11.x.
  If you migrate from Symantec Policy Manager 5.1 MR7 or MR8, AntiVirus policies are removed and not migrated.
- Symantec Network Access Control Manager and Console 5.1
  You can migrate this software to Symantec Endpoint Protection 11.x. However, to gain access to the legacy Host Integrity and Enforcer features, you must also install the Symantec Endpoint Protection Manager for Symantec Network Access Control 11.x.

Unsupported server migration paths

Symantec Endpoint Protection Manager for Symantec Endpoint Protection migration is blocked when any of the following software is detected:

- Sygate Policy Manager 5.0
- Sygate Management Server 3.x and 4.x
- Whole Security Management Server, all versions

Before you can install Symantec Endpoint Protection Manager for Symantec Endpoint Protection, you must uninstall this software.

Note: If you try to migrate Symantec Endpoint Protection Manager 5.1, and if any of the unsupported software is detected, the migration is also blocked.

About migrating legacy Symantec Sygate client software

The migration goal is to install Symantec Endpoint Protection 11.x.

The legacy agent software that you can migrate consists of the following two products:

- Symantec Protection Agent 5.1
- Symantec Enforcement Agent 5.1

Symantec Protection Agent includes all of the functionality that Symantec Enforcement Agent provides. The Symantec Enforcement Agent includes Host Integrity only.

When you migrate the clients that run Symantec Protection Agent or Symantec Enforcement Agent, install Symantec Endpoint Protection to complete the migration.

The Symantec Endpoint Protection 11.x client software includes all functionality that the Symantec Protection Agent and Symantec Enforcement Agent provide and more. If you have Sygate Protection Agents that provide Host Integrity, you do not need to also install the Symantec Endpoint Protection 11.x client on those computers. You do, however, need to install the Symantec Endpoint Protection Manager for Symantec Network Access Control 11.x on the management servers to regain access to that client functionality.

Note: Agent migration migrates all existing settings that are configured for the clients if you export the client installation package for your existing groups. You can then perform automatic upgrades for the clients that belong to those groups.

Supported client migration paths

The following software is supported for migration to Symantec Endpoint Protection:

- Symantec Protection Agent 5.1
- Symantec Protection Agent 5.1 with Symantec AntiVirus 9.x and greater
- Symantec Protection Agent 5.1 with Symantec Client Security 2.x and greater
- Symantec Enforcement Agent 5.1
- Symantec Enforcement Agent 5.1 with Symantec AntiVirus 9.x and greater
- Symantec Enforcement Agent 5.1 with Symantec Client Security 2.x and greater

Unsupported client migration paths

Symantec Endpoint Protection 11.x client migration is blocked when any of the following software is detected:

- Sygate Protection Agent 5.0
- Sygate Enforcement Agent 5.0
- Sygate Security Agent 3.x and 4.x
- Whole Security Confidence Online Enterprise Edition all versions
- Symantec Protection Agent 5.1 and Symantec AntiVirus 7.x and 8.x
- Symantec Protection Agent 5.1 and Symantec Client Security 1.x

- Symantec Enforcement Agent 5.1 and Symantec AntiVirus 7.x and 8.x
- Symantec Enforcement Agent 5.1 and Symantec Client Security 1.x

About migrating to Symantec Network Access Control 11.x

You can migrate Symantec Network Access Control 5.1 to Symantec Network Access Control 11.x. No other legacy Sygate software is supported for this migration. To migrate other versions, first migrate them to Symantec Sygate Enterprise Protection 5.1.

About migrating legacy Symantec Sygate server software

Symantec Network Access Control Manager and Management Console 5.1 is the only software that is supported for migration to Symantec Endpoint Protection Manager and Management Console for Symantec Network Access Control 11.x.

Symantec Endpoint Protection Manager for Symantec Network Access Control migration is blocked when any of the following software is detected:

- Sygate Policy Manager 5.0
- Sygate Management Server 3.x and 4.x
- Whole Security Management Server, all versions

About migrating legacy Symantec Sygate client software

Symantec Enforcement Agent 5.1 is the only software that is supported for migration to Symantec Network Access Control 11.x.

Note: Agent migration migrates all existing settings that are configured for the clients as long as you export the client installation package for your existing groups. Then you perform an automatic upgrade for those groups.

Symantec Network Access Control 11.x client migration is blocked when any of the following software is detected:

- Sygate Enforcement Agent 5.0
- Sygate Protection Agent 5.0 and greater
- Sygate Security Agent 3.x and 4.x
- Whole Security Confidence Online Enterprise Edition all versions

- Symantec Enforcement Agent 5.1 and Symantec AntiVirus all versions
- Symantec Enforcement Agent 5.1 and Symantec Client Security all versions

About Enforcer upgrades

Symantec Endpoint Protection Manager supports Symantec Gateway, DHCP, and LAN Enforcers that run on version 6100 hardware appliances only. These appliances support software versions 5.1, 5.1.5, and 11.x. Symantec Endpoint Protection Manager supports software versions 5.1.5 and 11.x only. Symantec Endpoint Protection Manager does not support software version 5.1. Earlier versions of Symantec Enforcer that were provided as software only are also not supported.

If your 6100 Enforcer appliance is running software version 5.1, you must upgrade the software image to version 5.1.5 or 11.x. Symantec recommends that you flash the legacy software image to version 11.x to use the latest version. All Enforcer settings are stored in Symantec Endpoint Protection Server, so Enforcer settings are migrated during server migration.

Server migration scenarios

Migrating legacy Symantec Sygate Enterprise Protection software is as complex as your network architecture. If you have one legacy management server that manages clients, install the Management components on the computer that runs Symantec Policy Manager 5.1. If additional legacy servers run replication, turn off replication before migration and then turn on replication after migration.

If additional legacy servers run failover or load balancing, you must disable the Symantec Policy Manager service on those computers. Then you migrate the servers one by one. Begin with the server that you first installed with the license file and preshared secret. After the servers are migrated, they automatically manage legacy clients. Then you use the **Upgrade Groups Wizard** to migrate the client computers to the latest version, which is the easiest way to migrate the clients.

Note: The server scenarios support both Symantec Endpoint Protection and Symantec Network Access Control migrations.

Migrating an installation instance that uses one management server

Migrating an installation instance that uses one management server is straightforward because you only migrate one site. You install Symantec Endpoint

Protection Manager on the computer that runs Symantec Sygate Enterprise Protection. Then proceed to update your client software. The database is also migrated. It does not matter if the embedded database server, a local Microsoft SQL Server, or a remote Microsoft SQL Server maintains the database.

To migrate a site that uses one Management server

- Migrate your management server.

  See "Migrating a management server" on page 182.

Migrating an installation instance that uses one Microsoft SQL database and multiple management servers

Migrating an installation instance that uses one database and multiple management servers has the following implications:

- The management servers are configured for load balancing or failover.
- The database runs on Microsoft SQL server because failover and load balancing is supported on Microsoft SQL Server only.
- Replication is not performed because there is only one database.

All installation instances have a site in which you first installed the management server. Only one of these management servers was installed with a license and a preshared secret. You should migrate this management server first. You then migrate the other management servers that were installed for load balancing and failover.

To migrate an installation instance that uses one SQL Server database and multiple management servers

1. On all management servers that were not installed with the license and preshared secret, disable the Symantec Policy Manager service with Windows Administrative Tools.

   See "Stopping the servers before load balancing and failover migration" on page 183.

2. Authenticate to and log on to the computer that contains the Symantec Policy Manager that was installed with the license and preshared secret.

   Do not log on to the Symantec Policy Manager.

3. Migrate the management server.

   See "Migrating a management server" on page 182.

4. Migrate all additional management servers one by one.

Migrating an installation instance that uses multiple embedded databases and management servers

Migrating an installation instance that uses multiple embedded database and management servers has the following implications:

- No failover or load balancing is performed because the embedded database does not support failover or load balanced servers.
- The Management servers are configured for replication only because you cannot install multiple embedded database servers without installing them as replicating servers.

All sites have a computer on which you first installed the management server. Only one of these management servers was installed with a license and a preshared secret. You must migrate this management server first. You then migrate the other management servers that were installed for replication.

To migrate an installation instance that uses multiple embedded databases and management servers

1. On all management servers, disable replication.

   See "Turning off replication before migration" on page 183.

2. Authenticate to and log on to the computer that contains the Symantec Policy Manager that was installed with the license and preshared secret.

   Do not log on to the Symantec Policy Manager.

3. Migrate the management server.

   See "Migrating a management server" on page 182.

4. Migrate all additional management servers one by one.
5. After you migrate the servers, enable replication on each server.

   See "Enabling replication after migration" on page 184.

Migrating an installation instance that uses multiple SQL database and management servers

Migrating a site that uses multiple SQL database and management servers has the following implications:

- Replication is configured because it uses multiple Microsoft SQL 2000 databases.
- The management servers may be configured for load balancing or failover.

All sites have a computer on which you first installed the management server. Only one of these management servers was installed with a license and a preshared secret. You should migrate this management server first. You then migrate the other management servers that were installed for replication, failover, and load balancing.

Note: You can have an embedded database that replicates with Microsoft SQL database. The embedded database, however, does not support failover and load balanced servers.

To migrate an installation instance that uses multiple SQL database and management servers

1. On all management servers that perform replication to a database, disable replication.

   See "Turning off replication before migration" on page 183.

2. Disable the Symantec Policy Manager service on all management servers that perform load balancing and failover.

   Do so on all management servers that were not installed with the license and preshared secret.

   See "Stopping the servers before load balancing and failover migration" on page 183.

3. Log on to the Symantec Policy Manager computer that was installed with the license and preshared secret. Do not log on to the Symantec Policy Manager.

4. Migrate the management server.

   See "Migrating a management server" on page 182.

5. Migrate all additional management servers that perform failover and load balancing one by one.

6. Repeat the previous steps until you have migrated all sites.

7. Turn on replication one site at a time until all sites replicate again.

   See "Enabling replication after migration" on page 184.

About scenarios for migrating management servers

You can migrate the management servers, the management consoles, and the management databases. You migrate the components according to the scenarios that fit your environments and sites. The order in which you migrate your components depends on the migration scenario that you use.

See "Server migration scenarios" on page 178.

Migrating a management server

You must migrate all management servers before you migrate any clients. If you migrate management servers in an environment that supports load balancing, failover, or replication, you must prepare and migrate the management servers in a specific order.

See "Server migration scenarios" on page 178.

Warning: You must identify and follow your migration scenario, or your migration fails.

To migrate Symantec Sygate Enterprise Protection servers that use Host Integrity Policies or Enforcer protection, install the Symantec Endpoint Protection Manager for Symantec Endpoint Protection first. Then, you repeat the installation procedure and you install Symantec Endpoint Protection Manager for Symantec Network Access Control to gain access to the Host Integrity and Enforcer functionality.

To migrate a management server

1. In the server to migrate, insert the product disc for one of the following:
   - Symantec Endpoint Protection
   - Symantec Network Access Control
2. Start the setup program, and then do one of the following actions:
   - To install for Symantec Endpoint Protection, click **Install Symantec Endpoint Protection Manager**.
   - To install for Symantec Network Access Control, click **Install Symantec Network Access Control**, and then click **Install Symantec Endpoint Protection Manager**.
3. In the Welcome panel, click **Next**.
4. Click through the installation prompts until the installation begins.

   Initial file installation takes a few minutes.
5. In the Install Wizard Completed panel, click **Finish**.
6. In the Welcome to the Management Server Upgrade Wizard panel, click **Next**.
7. In the Information prompt, click **Continue**.
8. When the Server Upgrade Status succeeds, click **Next**.

9 In the Upgrade Succeeded panel, click **Finish**.

10 When the Symantec Endpoint Protection Manager logon panel appears, log on to the console by using your legacy logon credentials.

11 (Optional) If you need to install the Symantec Endpoint Protection Manager for Symantec Network Access Control, log off the Symantec Endpoint Protection Manager. Then repeat this procedure and install Symantec Endpoint Protection Manager for Symantec Network Access Control from the Symantec Network Access Control installation CD.

You are not required to restart the computer, but you may notice performance improvements if you restart the computer and log on.

Stopping the servers before load balancing and failover migration

If you have legacy Symantec servers that perform load balancing and failover, you must stop the Symantec Policy Manager service on all legacy servers. When you stop this service, you stop legacy servers that try to update the database during migration. Legacy servers should not try to update the database until migration is complete.

To stop the servers before load balancing and failover migration

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

2 In the Services window, under Name, scroll to and right-click **Symantec Policy Manager**.

3 Click **Stop**.

Turning off replication before migration

If you have legacy Symantec sites that are configured for replication, you must turn off replication before migration. You do not want sites trying to replicate data between legacy and updated databases during or after migration. You must turn off replication at each site that replicates, which means that you must log on to and turn off replication at a minimum of two sites.

To disable replication before migration

1 Log on to the Symantec Policy Management Console if you are not logged on.

2 On the Servers tab, in the left pane, expand Local Site, and then expand Replication Partners.

3 For each site that is listed under Replication Partners, right-click the site, and then click **Delete**.

4 In the Delete Partner prompt, click **Yes**.

5 Log off the console, and then repeat this procedure at all sites that replicate data.

Enabling replication after migration

After you migrate all the servers that are used replication, failover, and load balancing, you must turn on replication. After migration, you add a replication partner to enable replication. You must add replication partners only on the computer on which you first installed the management server. Replication partners automatically appear on the other management servers.

To enable replication after migration

1 Log on to the Symantec Policy Management Console if you are not logged on.

2 On the Servers tab, in the left pane, expand Local Site, and then expand Replication Partners.

3 For each site that is listed under Replication Partners, right-click the site, and then click **Add Partner**.

4 In the Add Replication Partner panel, click **Next**.

5 In the Remote Site Information panel, enter the identifying information about the replication partner, enter the authentication information, and then click **Next**.

6 In the Schedule Replication panel, set the schedule for when replication occurs automatically, and then click **Next**.

7 In the Replication of Log Files and Client Packages panel, check the items to replicate, and then click **Next**.

Package replication generally involves large amounts of traffic and storage requirements.

8 In the Completing the Add Replication Partner Wizard panel, click **Finish**.

9 Repeat this procedure for all management servers that replicate data with this management server.

About console user interface and functionality changes post migration

The following user interfaces changes appear after migration:

- The Start Program menu for Symantec Policy Manager is changed to Symantec Endpoint Protection Manager console.
- The installation directory and service name retain the legacy name of Symantec Policy Manager and are not renamed.
- Legacy OS Protection Policies appear as Hardware Device Protection policies.
- Several new policy types are available for LiveUpdate Settings, AntiVirus and Antispyware, and so forth. You cannot use the new policies until you migrate your clients.
- Legacy client installation packages are removed from the database so that they do not appear in the migrated console. However, these packages remain in your legacy package directory. You should export your new client installation packages to a different directory.
- Report Scheduler is now available from the Reports tab instead of the legacy Server Site Properties dialog box.
- License Management has been deprecated and is no longer required.
- Package management is now available from the Servers pane instead of the legacy Client Manager pane.
- Policy Library components such as Management Server Lists and Network Services are now available on the Policies pane, under the lists of Policies and are identified as Policy Components.
- The Servers and Administrators tab functionality have been consolidated into the Admin pane.
- The server migration purges all client installation packages from the database. These packages are no longer supported and package removal does not affect the connected clients. This prevents new deployments of the legacy client packages.

Migrating remote management consoles

You migrate legacy remote management consoles by installing the latest remote management consoles on the computers that run the legacy consoles. The legacy Symantec Policy Manager icons and Program start menu are not migrated. When you click the icon or the menu item, however, they display the new Symantec Endpoint Protection Manager logon prompt.

When a legacy remote management console was installed, Sun Java 1.4 runtime may have been installed on the computer if it was not already installed. This new version of the remote management console downloads and installs Sun Java 1.5

to the remote computer. If you do not need Sun Java 1.4 runtime for any other applications, you can remove it with the Windows Add/Remove program utility.

To migrate remote management consoles

1. On the computer on which to install the management console, start a Web browser.
2. In the URL box, type one of the following identifiers for the computer that runs the policy manager:
   - **http://*computer_name*:9090**
   - **http://*computer_IP_address*:9090**

   The default port number for the Web console port is 9090. If you specified a different port during installation, replace 9090 with the port that you specified. You can change the port number by using the Management Server Configuration Wizard.
3. In the Symantec Policy Management Console window, click **Here** to download and install JRE 1.5.
4. Respond to and follow the prompts and log on to the Symantec Endpoint Protection Manager console.

About configuring migrated and new policies

If you migrated to Symantec Endpoint Protection, the migrated Firewall and Intrusion Prevention Policies contain your legacy settings. There are also additional Symantec Endpoint Protection default policies assigned. You should review the new policies to determine if the settings are appropriate for your environment. If you want to modify the settings, make any changes you that affect your groups before you migrate legacy clients.

For example, if you decide to add Antivirus and Antispyware Protection to your clients during migration, you should become familiar with the Antivirus and Antispyware Policy settings. LiveUpdate Settings and LiveUpdate Content Policies affect both Symantec Endpoint Protection and Symantec Network Access Control. As a result, you should become very familiar with these policies and how they affect your groups and locations before client migration.

For more information about policies, see the *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control*.

About removing the client password protections from group settings

Group settings are migrated and include the group client password protection settings. If you have group settings that enable one or more passwords such as for uninstallation, client migration fails for certain maintenance releases. As a best practice, you must disable these passwords in your migrated groups with the Symantec Endpoint Protection Manager console before you migrate legacy client software. The password protection settings appear in the General Settings for each group. You can turn on these passwords after migration.

Warning: If you do not disable the uninstallation password, you may have to enter this password on each client computer. If you deploy to 100 or more clients, you may have to email the password to end users.

For more information on password protecting the client, see the *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control*.

Migrating legacy Symantec Sygate client software

The easiest way to migrate both Symantec Protection Agent and Symantec Enforcement Agent software is by using the Auto Upgrade feature. All other client software deployment methods are supported, but the Auto Upgrade approach is the easiest way. The migration can take up to 30 minutes. Therefore, you should migrate when most users are logged off of their computers.

Note: You must test this migration approach before you roll out the migration to a large number of computers. You can create a new group and place a small number of client computers in that group.

To migrate legacy Symantec Sygate client software

1. Log on to the newly migrated Symantec Endpoint Protection Manager console if you are not logged on.
2. Click **Admin > Install Packages**.
3. In the lower-left pane, under Tasks, click **Upgrade Groups with Package**.
4. In the Welcome to the Upgrade Groups Wizard panel, click **Next**.
5. In the Select Client Install Package panel, in the Select the new client installation package drop-down menu, do one of the following actions:

- Click **Symantec Endpoint Protection <appropriate version>**.
- Click **Symantec Network Access Control <appropriate version>**.

6 In the Specify Groups panel, check one or more groups that contains the client computers that you want to migrate, and then click **Next**.

7 In the Package Upgrade Settings panel, check **Download from the management server**.

You can optionally stage and select a package on a Web server.

8 Click **Upgrade Settings**.

9 In the Add Client Install Package dialog box, do the following actions:

- On the General tab, specify a schedule for when to migrate the client computers.
- On the Notification tab, specify a message to display to users during the upgrade.
  For details about settings on these tabs, click **Help**.

10 Click **OK**.

11 In the Package Upgrade Settings panel, click **Next**.

12 In the Completing the Client Upgrade Wizard panel, click **Finish**.

Section 4

Appendices

Appendix A

Symantec Endpoint Protection installation features and properties

This appendix includes the following topics:

About installation features and properties

Installation features and properties appear as strings in text files and command lines. Text files and command lines are processed during all client software installations. Installation features control what components get installed. Installation properties control what subcomponents are enabled or disabled after installation. Installation features and properties are available for Symantec Endpoint Protection client software only and are also available for the Windows operating system. Installation features and properties are not available for

Symantec Network Access Control client software or for Symantec Endpoint Protection Manager installations.

Installation features and properties are specified in two ways: as lines in the Setaid.ini file and as values in Windows Installer (msi) commands. Msi commands can be specified in Windows Installer strings and in vpremote.dat for customized Push Deployment Wizard deployment. Windows Installer commands and Setaid.ini are always processed for all managed client software installations. If different values are specified, the values in Setaid.ini always take precedence.

About configuring Setaid.ini

Setaid.ini appears in all installation packages. Setaid.ini always takes precedence over any setting that may appear in an msi command string that is used to start the installation. Setaid.ini appears in the same directory as setup.exe. If you export to a single .exe file, you cannot configure Setaid.ini. However, the file is automatically configured when you export Symantec Endpoint Protection client installation files from the console.

The following lines show some of the options that you can configure in Setaid.ini. Value 1 enables a feature and value 0 disables a feature.

```
[CUSTOM_SMC_CONFIG]
InstallationLogDir=
DestinationDirectory=

[FEATURE_SELECTION]
Core=1

SAVMain=1
 EMailTools=1
 OutlookSnapin=1
 Pop3Smtp=0
 NotesSnapin=0

PTPMain=1
 DCMain=1
 COHMain=1

ITPMain=1
 Firewall=1
```

Note: The features are indented to show hierarchy. The features are not indented inside the Setaid.ini file. Feature names in Setaid.ini are case sensitive.

Feature values that are set to 1 install the features. Feature values that are set to 0 do not install the features. You must specify and install the parent features to successfully install the client features as shown in the feature tree.

See "Symantec Endpoint Protection client features" on page 193.

The only time that Setaid.ini is not processed is when you install the client software with the files in the SAV installation CD directory. You can install these files with third-party distribution tools like SMS.

Be aware of the following additional setaid.ini settings that map to msi properties for Symantec Endpoint Protection client installation:

- DestinationDirectory maps to INSTALLDIR
- KeepPreviousSetting maps to MIGRATESETTINGS
- AddProgramIntoStartMenu maps to ADDSTARTMENUICON

About configuring msi command strings

Symantec Endpoint Protection installation software uses Windows Installer (msi) 3.1 packages for installation and deployment. If you use the command line to deploy a package, you can customize the installation. You can use the standard Windows Installer parameters and the Symantec-specific features and properties.

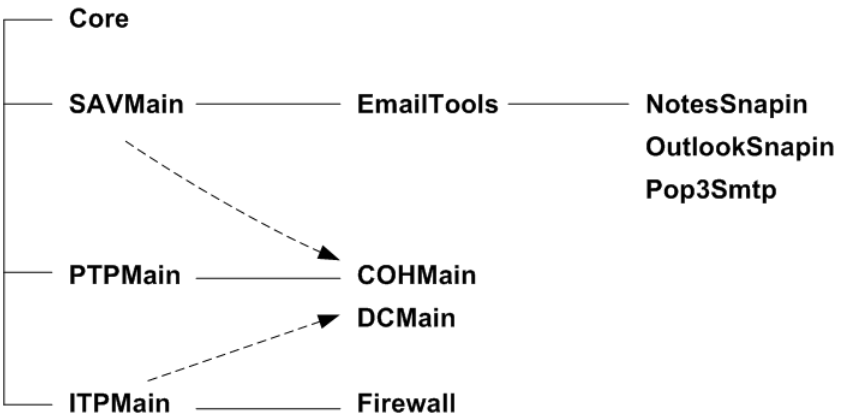
To use the Windows Installer, elevated privileges are required. If you try the installation without elevated privileges, the installation may fail without notice. For the most up-to-date list of Symantec installation commands and parameters, see the Symantec Support Knowledge Base article, MSI command line reference for Symantec Endpoint Protection 11.0

Note: The Microsoft Installer advertise function is unsupported. Setaid.ini-specified features and properties take precedence over MSI-specified features and properties. Feature and property names in msi commands are case sensitive.

Symantec Endpoint Protection client features

Symantec Endpoint Protection features can be installed by specifying them in Setaid.ini files and in msi commands. Most features have a parent-child relationship. If you want to install a child feature that has a parent feature, you must also install the parent feature.

Figure A-1 Client feature tree parent-child relationships



The feature tree shows four primary features as listed on the left. The Core feature must always be specified for installation. It contains the core client communications functionality. The other three features can be installed as stand-alone features. SAVMain installs antivirus and antispyware protection, PTPMain installs TruScan proactive threat scanning technology, and ITPMain installs network threat protection.

Note: COHMain and DCMain require two parents. COHMain is Proactive Threat Scan and requires PTPMain and SAVMain. DCMain, which is Application and Device Control, requires PTPMain and ITPMain.

For both setaid.ini and msi, if you specify a child feature but do not specify its parent feature, the child feature is installed. However, the feature does not work because the parent feature is not installed. For example, if you specify to install the Firewall feature but do not specify to install ITPMain, the Firewall, is not installed.

Table A-1 Symantec Endpoint Protection client features

Feature	Description	Required parent features
Core	Install the files that are used for communications between clients and the Symantec Endpoint Protection Manager. This feature is required.	none

Table A-1 Symantec Endpoint Protection client features *(continued)*

Feature	Description	Required parent features
SAVMain	Install the basis antivirus and antispyware feature files.	none
SymProtectManifest	Install the Tamper Protection feature.	none
EMailTools	Install the basic email Auto-Protect feature files.	SAVMain
NotesSnapin	Install the Lotus Notes Auto-Protect email feature.	SAVMain, EMailTools
OutlookSnapin	Install the Microsoft Exchange Auto-Protect email feature.	SAVMain, EMailTools
Pop3Smtp	Install the Internet Email Auto-Protect feature.	SAVMain, EMailTools
PTPMain	Install the basic TruScan proactive threat scan feature files.	none
COHMain	Install the proactive threat scan feature.	PTPMain, SAVMain
DCMain	Install the Application Control and Device Control feature.	PTPMain, ITPMain
ITPMain	Install the basic Network Threat Protection feature files.	none
Firewall	Install the firewall feature.	IPTMain

Symantec Endpoint Protection client installation properties

Table A-2 Symantec Endpoint Protection client installation properties

Property	Description
RUNLIVEUPDATE=*val*	Determines whether LiveUpdate is run as part of the installation, where *val* is one of the following values: ■ 1: Runs LiveUpdate during installation (default). ■ 0: Does not run LiveUpdate during installation. By default, all Symantec Endpoint Protection clients in a group receive the latest versions of all content and all product updates. If configured to get updates from a management server, the clients receive only the updates that the server downloads. If the LiveUpdate content policy allows all updates, but the management server does not download all updates, the clients receive only what the server downloads.
ENABLEAUTOPROTECT=*val*	Determines whether File System Auto-Protect is enabled after the installation is complete, where *val* is one of the following values: ■ 1: Enables Auto-Protect after installation (default). ■ 0: Disables Auto-Protect after installation.
SYMPROTECTDISABLED=*val*	Determines whether Tamper Protection is enabled as part of the installation, where *val* is one of the following values: ■ 1: Disables Tamper Protection after installation. ■ 0: Enables Tamper Protection after installation. (default)

Windows Installer parameters

Symantec Endpoint Protection Manager client installation packages use the standard Windows Installer parameters, as well as a set of extensions for command-line installation and deployment.

See the Windows Installer documentation for further information about the usage of standard Windows Installer parameters. You can also execute msiexec.exe from a command line to see the complete list of parameters.

Table A-3 Windows Installer parameters

Parameter	Description
Symantec AntiVirus.msi	Symantec AntiVirus.msi installation file for the Symantec Endpoint Protection Manager client. If any .msi file contains spaces, enclose the file name in quotations when used with /I and /x. Required
Msiexec	Windows Installer executable. Required
/I "*msi file name*"	Install the specified .msi file. If the file name contains spaces, enclose the file name in quotations. If the .msi file is not in the same directory from which you execute Msiexec, specify the path name. If the path name contains spaces, enclose the path name in quotations. For example, msiexec.exe /I "C:*path to* Symantec AntiVirus .msi" Required
/qn	Install silently. **Note:** When a silent deployment is used, the applications that plug into Symantec Endpoint Protection, such as Microsoft Outlook and Lotus Notes, must be restarted after installation.
/x "*msi file name*"	Uninstall the specified components. Optional
/qb	Install with a basic user interface that shows the installation progress. Optional
/l*v *logfilename*	Create a verbose log file, where *logfilename* is the name of the log file you want to create. Optional
INSTALLDIR=*path*	Designate a custom path on the target computer where *path* is the specified target directory. If the path includes spaces, use quotation marks. **Note:** The default directory is C:\Program Files\Symantec Endpoint Protection Manager Optional

Table A-3 Windows Installer parameters *(continued)*

Parameter	Description
REBOOT=*value*	Controls a computer restart after installation, where *value* is a valid argument. The valid arguments include the following: ■ Force: Requires that the computer is restarted. Required for uninstallation. ■ Suppress: Prevents most restarts. ■ ReallySuppress: Prevents all restarts as part of the installation process, even a silent installation. Optional **Note:** Use ReallySuppress to suppress a restart when you perform a silent uninstallation of Symantec Endpoint Protection client.
ADDLOCAL= *feature*	Select the custom features to be installed, where *feature* is a specified component or list of components. If this property is not used, all applicable features are installed by default, and Auto-Protect email clients are installed only for detected email programs. To add all appropriate features for the client installations, use the ALL command as in ADDLOCAL=ALL. See "Symantec Endpoint Protection client features" on page 193. **Note:** When you specify a new feature to install, you must include the names of the features that are already installed that you want to keep. If you do not specify the features that you want to keep, Windows Installer removes them. By specifying existing features, you do not overwrite the installed features. To uninstall an existing feature, use the REMOVE command. Optional
REMOVE=*feature*	Uninstall the previously installed program or a specific feature from the installed program, where *feature* is one of the following: ■ *Feature*: Uninstalls the feature or list of features from the target computer. ■ ALL: Uninstalls the program and all of the installed features. All is the default if a feature is not specified. Optional

Windows Security Center properties

You can customize Windows Security Center (WSC) properties during Symantec Endpoint Protection client installation. These properties apply to unmanaged clients only. Symantec Endpoint Protection Manager controls these properties for the managed clients.

Table A-4 Windows Security Center properties

Property	Description
WSCCONTROL=*val*	Controls WSC where *val* is one of the following values: ■ 0: Do not control (default). ■ 1: Disable one time, the first time it is detected. ■ 2: Disable always. ■ 3: Restore if disabled.
WSCAVALERT=*val*	Configures the antivirus alerts for WSC where *val* is one of the following values: ■ 0: Enable. ■ 1: Disable (default). ■ 2: Do not control.
WSCFWALERT=*val*	Configures the firewall alerts for WSC where *val* is one of the following values: ■ 0: Enable. ■ 1: Disable (default). ■ 2: Do not control.
WSCAVUPTODATE=*val*	Configures the WSC out-of-date time for antivirus definitions where *val* is one of the following values: 1 - 90: Number of days (default is 30).
DISABLEDEFENDER=*val*	Determines whether to disable Windows Defender during installation, where *val* is one of the following values: ■ 1: Disables Windows Defender (default). ■ 0: Does not disable Windows Defender.

About using the log file to check for errors

The Windows Installer and Push Deployment Wizard create log files that can be used to verify whether or not an installation was successful. The log files list the components that were successfully installed and provide a variety of details that are related to the installation package. The log files can be used as an effective tool to troubleshoot a failed installation.

If the installation is successful, the log files include a success entry near the end. If the installation is not successful, an entry indicates that the installation failed. Typically, look for Value 3 to find failures. You specify the log file and location with the parameter named /l*v <*log filename*>. The log file (vpremote.log) that is

created when you use the Push Deployment Wizard is located in the \\Windows\temp directory.

Note: Each time the installation package is executed, the log file is overwritten.

Identifying the point of failure of an installation

You can use the log file to help identify the component or the action that caused an installation to fail. If you cannot determine the reason for the failed installation, you should retain the log file. Provide the file to Symantec Technical Support if it is requested.

To identify the point of failure of an installation

1. In a text editor, open the log file that the installation generated.
2. Search for the following:

   ```
   Value 3
   ```

   The action that occurred before the line that contains this entry is most likely the action that caused the failure. The lines that appear after this entry are the installation components that have been rolled back because the installation was unsuccessful.

Command-line examples for installing the client

Table A-5 Command-line examples

Task	Command line
Silently install all of the Symantec Endpoint Protection client components with default settings to the directory C:\SFN. Suppress a computer restart, and create a verbose log file.	msiexec /I "Symantec AntiVirus.msi" INSTALLDIR=C:\SFN REBOOT=ReallySuppress /qn /l*v c:\temp\msi.log
Silently install the Symantec Endpoint Protection client with Antivirus and Antispyware Protection, and with Network Threat Protection. Create a verbose log file. The computer must be restarted to implement Network Threat Protection.	msiexec /I "Symantec AntiVirus.msi" ADDLOCAL=Core,SAVMain,EMailTools,OutlookSnapin, Pop3Smtp,ITPMain,Firewall /qn /l*v c:\temp\msi.log

Appendix B

Disaster recovery

This appendix includes the following topics:

Preparing for disaster recovery

You prepare for disaster recovery by collecting files and information during and after Symantec Endpoint Protection Manager installation. For example, you must document your encryption password during the installation. You must locate and move your keystore file to a secure location.

See "Performing disaster recovery" on page 203.

Table B-1 High-level steps to prepare for disaster recovery

Step	Action	Description
Step 1	Back up your database on a regular basis, preferably weekly, and store the backups off site.	The database backup directory is located in \\Program Files\Symantec\ Symantec Endpoint Protection Manager\data\backup. The backup file is named *date_timestamp*.zip.

Table B-1 High-level steps to prepare for disaster recovery *(continued)*

Step	Action	Description
Step 2	Locate your keystore file and your server.xml file.	During the installation, these files were backed up to the directory that is named \\Program Files\Symantec\ Symantec Endpoint Protection Manager\Server Private Key Backup. The keystore file name is keystore_*timestamp*.jks. The keystore contains the private-public key pair and the self-signed certificate. The server.xml file name is server_*timestamp*.xml. You can also back up these files from the Admin panel in the management server console.
Step 3	Create and open a text file with a text editor. Name the file Backup.txt, or a similar name. Open server.xml, locate the keypass and storepass password, and copy and paste it into the text file. Leave the text file open.	The password is used for both storepass and keypass. Storepass protects the JKS file. Keypass protects the private key. You enter these passwords to restore the certificate. The password string looks like keystorePass="WjCUZx7kmX$qA1u1". Copy and paste the string that is between the quotation marks. Do not include the quotation marks.
Step 4	Copy and paste the sylink.xml file.	If you have one domain only, find and copy the sylink.xml file from a directory in \\Program Files\Symantec\Symantec Endpoint Protection Manager\data\outbox\agent\. Then, paste it to \\Program Files\Symantec\ Symantec Endpoint Protection Manager\Server Private Key Backup\. If you have multiple domains, locate and copy a sylink.xml file on a client computer in each domain. Then paste it into the following location: \\Program Files\Symantec\ Symantec Endpoint Protection Manager\Server Private Key Backup. The domain IDs are required if you do not have a backup of the database. This ID is in the sylink.xml file on the clients computers in each domain.
Step 5	Open each sylink.xml file, locate the DomainId, and copy and paste it into the Backup.txt file.	You add this ID to a new domain that you create to contain your existing clients. The string in the sylink.xml file looks like DomainId="B44AC676C08A165009ED819B746F1". Copy and paste the string that is between the quotation marks. Do not include the quotation marks.

Table B-1 High-level steps to prepare for disaster recovery *(continued)*

Step	Action	Description
Step 6	In the Backup.txt file, type the encryption password that you used during the installation of the first site in your network.	You retype this key when you reinstall the management server. You must retype the identical key if you do not have a backed up database to restore. It is not required if you have a backed up database to restore, but it is a best practice.
Step 7	In the Backup.txt text file, type the IP address and host name of the computer that runs the management server.	If you have a catastrophic hardware failure, you must reinstall the management server on a computer that has the same IP address and host name.
Step 8	In the Backup.txt file, type the site name that identifies the management server. Save and close the Backup.txt file, which now contains the essential information that is required for disaster recovery.	While the site name is not strictly required for reinstallation, it helps to create a consistent restoration.
Step 9	Copy these files to removable media, and store the media in a secure location, preferably in a safe.	After you secure the files, you should remove these files from the computer that runs the management server.

Performing disaster recovery

After you prepare for disaster recover, use the following steps to perform disaster recovery.

See "Preparing for disaster recovery" on page 201.

Table B-2 Process for performing disaster recovery

Step	Action
Step 1	Restore Symantec Endpoint Protection Manager See "Restoring the Symantec Endpoint Protection Manager" on page 204.
Step 2	Restore the server certificate See "Restoring the server certificate" on page 204.
Step 3	Restore client communications How you restore client communications depends on whether or not you have access to a database backup. See "Restoring client communications" on page 205.

Restoring the Symantec Endpoint Protection Manager

If you have a disaster, recover the files that were secured after initial installation. Then open the Backup.txt file that contains the passwords, domain IDs, and so forth.

If you had a catastrophic hardware failure, you may need to rebuild the computer. If you rebuild the computer, you must assign it the original IP address and host name. This information should be in the Backup.txt file.

When you reinstall the software, use the same encryption password and other settings you specified during the first installation on the server that failed.

Restoring the server certificate

The server certificate is a Java keystore that contains the public certificate and the private-public key pairs. You must enter the password that is contained in the Backup.txt file. This password is also in the original server_*timestamp*.xml file.

To restore the server certificate

1. Log on to the Console, and then click **Admin**.
2. In the Admin pane, under Tasks, click **Servers**.
3. Under View Servers, expand Local Site, and then click the computer name that identifies the local site.
4. Under Tasks, click **Manage Server Certificate**.
5. In the Welcome panel, click **Next**.
6. In the Manage Server Certificate panel, check **Update the Server Certificate**, and then click **Next**.
7. Under Select the type of certificate to import, check **JKS keystore**, and then click **Next**.

   If you have implemented one of the other certificate types, select that type.
8. In the JKS Keystore panel, click **Browse**, locate and select your backed up keystore_*timestamp*.jks keystore file, and then click **OK**.
9. Open your disaster recovery text file, and then select and copy the keystore password.
10. Activate the JKS Keystore dialog box, and then paste the keystore password into the Keystore and Key boxes.

    The only supported paste mechanism is Ctrl + V.

11 Click **Next**.

If you get an error message that says you have an invalid keystore file, it is likely you entered invalid passwords. Retry the password copy and paste. This error message is misleading.

12 In the Complete panel, click **Finish**.

13 Log off the Console.

14 Click **Start > Settings > Control Panel > Administrative Tools > Services**.

15 In the Services window, right-click **Symantec Endpoint Protection Manager**, and then click **Stop**.

Do not close the Services window until you are finished with disaster recovery and reestablish client communications.

16 Right-click **Symantec Endpoint Protection Manager**, and then click **Start**.

By stopping and starting Symantec Endpoint Protection Manager, you fully restore the certificate.

Restoring client communications

If you have access to a database backup, you can restore this database and then resume client communications. The advantage to restoring with a database backup is that your clients reappear in their groups and they are subject to the original policies. If you do not have access to a database backup, you can still recover communications with your clients, but they appear in the Temporary group. You can then re-create your group and your policy structure.

See "Restoring client communications with a database backup" on page 205.

See "Restoring client communications without a database backup" on page 207.

Restoring client communications with a database backup

You cannot restore a database on a computer that runs an active Symantec Endpoint Protection Manager service. You must stop and start it a few times.

Warning: When you restore a database backup, you must use the same version of the management server that you used to create the backup.

To restore client communications with a database backup

1. If you closed the Services window, click **Start > Settings > Control Panel > Administrative Tools > Services**.
2. In the Services window, right-click **Symantec Endpoint Protection Manager**, and then click **Stop**.

   Do not close the Services window until you are finished with this procedure.
3. Create the following directory:

   \\Program Files\Symantec\Symantec Endpoint Protection Manager\data\backup
4. Copy your database backup file to the directory.

   By default, the database backup file is named *date_timestamp*.zip.
5. Click **Start > Programs > Symantec Endpoint Protection Manager > Database Back Up and Restore**.
6. In the Database Back Up and Restore dialog box, click **Restore**.
7. In the Restore Site dialog box, select the backup file that you copied to the backup directory, and then click **OK**.

   The database restoration time varies and depends on the size of your database.
8. When the Message prompt appears, click **OK**.
9. Click **Exit**.
10. Click **Start > Programs > Symantec Endpoint Protection Manager > Management Server Configuration Wizard**.
11. In the Welcome panel, check **Reconfigure the Management Server**, and then click **Next**.
12. In the Server Information panel, modify input values if necessary to match previous inputs, and then click **Next**.
13. In the Database Server Choice panel, check the database type to match the previous type, and then click **Next**.
14. In the Database Information panel, modify and insert input values to match previous inputs, and then click **Next**.

    The configuration takes a few minutes.
15. In the Configuration Completed dialog box, click **Finish**.

16 Log on to the console.

17 Right-click your groups, and then click **Run Command on Group > Update Content**.

If the clients do not respond after about one half hour, restart the clients.

Restoring client communications without a database backup

For each domain that you use, you must create a new domain and re-insert the same domain ID into the database. These domain IDs are in the disaster recovery text file if someone typed them in this file. The default domain is the Default domain.

A best practice is to create a domain name that is identical to the previous domain name. To re-create the Default (default) domain, append some value such as _2 (Default_2). After you restore domains, you can then delete the old default domain. Then rename the new domain back to Default.

To restore client communications without a database backup

1 Log on to the console.

2 In the console, click **Admin**.

3 In the System Administrator pane, click **Domains**.

4 Under Tasks, click **Add Domain**.

5 Click **Advanced**.

6 Open the disaster recovery text file, select and copy the domain ID, and then paste the domain ID into the Domain ID box.

7 Click **OK**.

8 (Optional) Repeat this procedure for each domain to recover.

9 Under Tasks, click **Administer Domain**.

10 Click **Yes** on the Administer Domain dialog box.

11 Click **OK**.

12 Restart all of the client computers.

The computers appear in the Temporary group.

13 (Optional) If you use one domain only, delete the unused Default domain, and rename the newly created domain to Default.

Index

K

L

M

V

W