Symantec™ Network Access Control 12.1.5 Getting Started Guide

For Symantec Network Access Control and Symantec Network Access Control Starter Edition

Symantec™

Symantec Network Access Control Getting Started Guide

Product version: 12.1.5

Documentation version: 1

This document was last updated on: September 19, 2014

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Getting Started with Symantec Network Access Control

This document includes the following topics:

- Setting up an Enforcer appliance
- Logging on to an Enforcer appliance
- Configuring an Enforcer appliance
- Where to get more information

What is 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 your protected network.

When enforcement controls are not in place, your organization's data is vulnerable to intended loss or inadvertent loss. Recovering the data can result in down time and the financial losses that are associated with lost productivity. To prevent these losses, Symantec Network Access Control controls on site and remote access to protected network resources. Symantec Network Access Control provides a complete end-to-end network access control solution.

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 quarantine server for remediation. The remediation server provides downloads of the necessary software, patches, virus definition updates, and so on, to make the client computer compliant. The Host Integrity policy on the client also continually monitors endpoints for changes in their 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 Network Access Control and Symantec Endpoint Protection clients.

See “About the types of enforcement in Symantec Network Access Control” on page 11.

What's new in Symantec Network Access Control 12.1.5

Symantec Network Access Control 12.1.5 includes new features for Symantec Endpoint Protection Manager and Host Integrity policies.

Table 1-1 New features in Symantec Network Access Control 12.1.5

Feature	Description
System requirements	You can now access Symantec Endpoint Protection Manager on the following browsers: ■ Microsoft Internet Explorer 10.2, 11 ■ Mozilla Firefox 5.x through 31.0 ■ Google Chrome through 37.0.2062.94 For the complete list of system requirements: See the knowledge base article: Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control
Management server updates	■ Symantec Protection Center 1 was removed in Symantec Network Access Control 12.1.4. You can still integrate Symantec Endpoint Protection Manager with Symantec Protection Center 2, but the feature is no longer tested. Protection Center lets you manage Symantec Network Access Control together with other Symantec products in a single environment. ■ Client password settings The client password protection settings now appear in a more accessible location in **Clients > Policies > Password Settings**. This dialog also provides a new option to enable password protection globally for all clients. You can also access the **Password Settings** dialog box when you log on to Symantec Endpoint Protection Manager. ■ You can no longer set to the console timeout to **Never**. For security reasons, the maximum timeout period is one hour. ■ After an administrator's failed logon attempts trigger an account lockout, the lockout interval now doubles with each subsequent lockout. Symantec Endpoint Protection Manager reverts to the original lockout interval after a successful logon, or after 24 hours since the first lockout.
Management server and client performance	The management server and the client include the following performance improvements: ■ Bandwidth control for client communication The management server now includes an Apache module that you can enable and configure to control network bandwidth. The module reduces the network load between Symantec Endpoint Protection Manager and the client computers, especially when the clients download content definitions or client installation packages. ■ The client startup time has improved by more than 10%. ■ The client service needs fewer processes to run.
Host Integrity policy changes	The Host Integrity policy is now included with both Symantec Endpoint Protection as well as Symantec Network Access Control. The Host Integrity policy evaluates the client computers and ensures that they meet the security policies you have modified and downloaded to those client computers.

Table 1-1 New features in Symantec Network Access Control 12.1.5 *(continued)*

Feature	Description
Documentation	Symantec Network Access Control provides the following documentation changes: ■ All main PDF files are now on the Technical Support site. You can now look for and download the most current PDF files from a single location: Product guides for all versions of Symantec Network Access Control (English) Symantec Network Access Control (other languages) The tools documents remain in the same folder as the associated tool. ■ The *Symantec Endpoint Protection Installation and Administration Guide* no longer includes Network Access Control topics. A new *Symantec Network Access Control Installation and Administration Guide* includes the Network Access Control topics. The documents for specific tools remain in the same folder as the associated tool.

System requirements for Symantec Network Access Control

In general, the system requirements for Symantec Endpoint Protection Manager and the Symantec Network Access Control clients are the same as those of the operating systems on which they are supported.

For the most current system requirements, see:

Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control

- System requirements for Symantec Endpoint Protection Manager
  See "System requirements for Symantec Endpoint Protection Manager" on page 7.
- System requirements for the Symantec Network Access Control client for Windows
  See "System requirements for the Symantec Network Access Control client for Windows" on page 9.
- System requirements for the Symantec Network Access Control On-Demand Client for Windows
  See "System requirements for the Symantec Network Access Control On-Demand Client for Windows" on page 9.
- System requirements for the Symantec Network Access Control On-Demand Client for Mac

See "System requirements for the Symantec Network Access Control On-Demand Client for Mac" on page 10.

See "Getting up and running on Symantec Endpoint Protection Manager for the first time" on page 15.

System requirements for Symantec Endpoint Protection Manager

Table 1-2 displays the minimum requirements for Symantec Endpoint Protection Manager.

Table 1-2 Symantec Endpoint Protection Manager system requirements

Component	Requirements
Processor	■ 32-bit processor: Intel Pentium 4 or equivalent (minimum dual core or hyper-threading recommended) ■ 64-bit processor: Intel Pentium 4 with x86-64 support or equivalent (minimum dual core or hyper-threading recommended) **Note:** Intel Itanium IA-64 processors are not supported.
Physical RAM	2 GB RAM available minimum; 4 GB or more available recommended. **Note:** Your Symantec Endpoint Protection Manager server may require additional RAM depending on the RAM requirements of other applications that are already installed.
Hard drive	16 GB available minimum (100 GB recommended) for the management server. 40 GB available minimum (200 GB recommended) for the management server and a locally installed database.
Display	1024 x 768

Table 1-2 Symantec Endpoint Protection Manager system requirements *(continued)*

Component	Requirements
Operating system	■ Windows XP (32-bit, SP2 or later; 64-bit, all SPs; all editions except Home) ■ Windows 7 (32-bit, 64-bit; RTM and SP1; all editions except Home) ■ Windows 8 (32-bit, 64-bit) ■ Windows 8.1 (32-bit, 64-bit) ■ Windows 8.1 Update 1 (32-bit, 64-bit) ■ Windows 8.1 Update 2 (32-bit, 64-bit) ■ Windows Server 2003 (32-bit, 64-bit; R2, SP1 or later) ■ Windows Server 2008 (32-bit, 64-bit; R2, RTM, SP1 and SP2) ■ Windows Server 2012 ■ Windows Server 2012 R2 ■ Windows Server 2012 R2 Update 1 ■ Windows Server 2012 R2 Update 2 ■ Windows Small Business Server 2003 (32-bit) ■ Windows Small Business Server 2008 (64-bit) ■ Windows Small Business Server 2011 (64-bit) ■ Windows Essential Business Server 2008 (64-bit)
Web browser	■ Microsoft Internet Explorer 8, 9, 10, 10.2, 11 ■ Mozilla Firefox 3.6 through 31.0 ■ Google Chrome, through 37.0.2062.94

Note: This Symantec Endpoint Protection Manager version manages clients earlier than version 12.1, regardless of the client operating system.

The Symantec Endpoint Protection Manager includes an embedded database. You may also choose to use one of the following versions of Microsoft SQL Server:

- SQL Server 2005, SP4
- SQL Server 2008, through SP3
- SQL Server 2008 R2, through SP2
- SQL Server 2012, through SP1
- SQL Server 2014

System requirements for the Symantec Network Access Control client for Windows

Table 1-3 displays the minimum requirements for the Symantec Network Access Control Windows client.

Table 1-3 Symantec Network Access Control client for Windows system requirements

Component	Requirement
Processor	■ 32-bit processor: 1 GHz Intel Pentium III or equivalent minimum (Intel Pentium 4 or equivalent recommended) ■ 64-bit processor: 2 GHz Pentium 4 with x86-64 support or equivalent minimum **Note:** Itanium processors are not supported.
Operating system	■ Windows XP (32-bit, SP2 or later; 64-bit, all SPs) ■ Windows XP Embedded ■ Windows Vista (32-bit, 64-bit) ■ Windows 7 (32-bit, 64-bit) ■ Windows 8 (32-bit, 64-bit) ■ Windows 8.1 (32-bit, 64-bit) ■ Windows 8.1 Update 1 (32-bit, 64-bit) ■ Windows Server 2003 (32-bit, 64-bit; R2, SP1 or later) ■ Windows Server 2008 (32-bit, 64-bit) ■ Windows Server 2012 ■ Windows Server 2012 R2 ■ Windows Server 2012 R2 Update 1 ■ Windows Small Business Server 2008 (64-bit) ■ Windows Essential Business Server 2008 (64-bit)
Physical RAM	512 MB of RAM, or higher if required by the operating system
Hard disk	32-bit: 300 MB; 64-bit: 400 MB
Display	800 x 600

System requirements for the Symantec Network Access Control On-Demand Client for Windows

Table 1-4 lists the minimum requirements for the computers on which the Symantec Network Access Control On-Demand Client needs to be installed.

Table 1-4 System requirements for the Symantec Network Access Control On-Demand Client for Windows

Component	Description
Processor	Intel Pentium II 550 MHz (1 GHz for Windows Vista) or faster
Operating System	The following operating systems are supported: ■ Windows XP Home or Professional (32-bit; SP2 and SP3) ■ Windows Vista (32-bit, 64-bit) ■ Windows 7 (32-bit, 64-bit) ■ Windows 8 (32-bit, 64-bit) ■ Windows 8.1 (32-bit, 64-bit) ■ Windows Server 2003 (32-bit, 64-bit; R2, SP1 or later) ■ Windows Server 2008 (32-bit, 64-bit; R2) ■ Windows Server 2012 ■ Windows Server 2012 R2 ■ Windows Small Business Server 2008 (64-bit) ■ Windows Essential Business Server 2008 (64-bit)
Memory	512 MB RAM
Hard disk	Download size: 9 MB The amount of free disk space that is needed to run the client: 100 MB
Display	Super VGA (1,024 x 768) or higher resolution video adapter and monitor
Browser	You can use one of the following browsers: ■ Microsoft Internet Explorer 6.0 or later ■ Mozilla Firefox 3.0 or later

System requirements for the Symantec Network Access Control On-Demand Client for Mac

You may want to check your system requirements before you try to connect to an organization's protected network.

Table 1-5 lists the minimum requirements for the computers on which the Symantec Network Access Control On-Demand Client installs.

Table 1-5 System requirements for Symantec Network Access Control On-Demand Downloader and Client on a Mac

Component	Description
Processor	Mac computer with an Intel CPU
Operating system	Mac OS X 10.6 or 10.7
Memory	512 MB of RAM
Hard disk	Download size: 9 MB The amount of free disk space that is needed to run the client: 100 MB
Display and connectivity	■ Super VGA (1,024 x 768) or higher resolution video adapter and monitor ■ At least one Ethernet adapter (with TCP/IP installed)
Browser	Apple Safari 4.0 and 5.0; Mozilla Firefox 3.0 or later.

About the types of enforcement in Symantec Network Access Control

Symantec Network Access Control provides different methods of enforcement to control access to your network.

Table 1-6 describes the differences between host-based enforcement and network-based enforcement.

Table 1-6 Types of enforcement

Type of enforcement	Description
Host-based enforcement	Allows the client computers to obtain and run the software they need to automatically remediate compliance failures. This is usually done through assigning the client computer to a quarantine server, where the client can download needed remediation files. When the client computer is remediated, it can safely access your protected network resources. Host-based enforcement can selectively allow or block access to the protected network, or can use the Symantec firewall to allow or block access. The firewall is included as part of the Symantec Endpoint Protection product. Host-based enforcement includes the following methods: ■ Host Integrity alone uses your Host Integrity policy to police network access, providing the easiest and fastest enforcement deployment option. You can implement Host Integrity more easily if the organization has already deployed the Symantec Endpoint Protection product. ■ Peer-to-peer authentication ensures that client-to-client communication occurs only between the company computers and Host Integrity-compliant computers outside the company. Compliant computers have passed their Host Integrity check. You must have Symantec Endpoint Protection installed with Symantec Network Access Control to use peer-to-peer enforcement.
Network-based enforcement	Uses the Symantec Enforcer appliances and integrated software Enforcers to enable you to control network access. Network-based enforcement authenticates and allows network access only to the clients that meet the requirements in the Host Integrity policy. Network-based enforcement also checks that the policy is current. Additionally, if your deployment includes a Gateway Enforcer appliance, you can allow guests without compliant software to access your network temporarily. These Enforcers enable guest access by installing On-Demand Clients on guest computers and dissolving them when guests log off. Guest access works with both Windows and Mac clients. This type of enforcement requires an Enforcer appliance. See "Deploying Symantec Network Access Control" on page 14.

See "Components of Symantec Network Access Control" on page 12.

Components of Symantec Network Access Control

Table 1-7 lists the product's components and describes their functions.

Table 1-7 Symantec Network Access Control 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 management server software provides secure communication to and from the client computers and the console. ■ The console is the interface to the management server. The console software coordinates and manages security policies, client computers, reports, logs, roles and access, administrative functions, and security. You can also install a remote console and use it to log on to the management server from any computer with a network connection. ■ The database stores security policies and events. You install the embedded database on the computer that hosts Symantec Endpoint Protection Manager. You can also separately install the Microsoft SQL Server database to use instead of the embedded database. See "Installing Symantec Endpoint Protection Manager" on page 20.
Symantec Network Access Control Windows client	The Host Integrity policy 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 the management server and a Symantec Enforcer. For more information about using the client, see the *Symantec Endpoint Protection and Symantec Network Access Control Client Guide*. See "What is Symantec Network Access Control?" on page 4.

For more information, see the *Symantec Network Access Control Installation and Administration Guide*.

See "Optional components for Symantec Network Access Control" on page 13.

Optional components for Symantec Network Access Control

Table 1-8 lists the additional components that you can download and use with Symantec Network Access Control.

Table 1-8 Symantec Network Access Control product subcomponents

Component	Description
Symantec Enforcer	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 Gateway Enforcer appliance provides in-line enforcement at network choke points. ■ The LAN 802.1X Enforcer appliance provides an out-of-band standards-based approach for LAN and wireless networks. ■ The DHCP Integrated Enforcer provides a DHCP-based approach for LAN and wireless networks over any infrastructure. ■ The Microsoft Network Access Protection Integrated Enforcer provides a Microsoft NAP-based approach for LAN and wireless networks.
Symantec Network Access Control On-Demand clients for Windows and Mac	On-Demand Clients are the temporary clients that you provide to users when they are unauthorized to access your network. Unauthorized client computers do not have the software that is compliant with your security policy. Once the Enforcer has installed an on-demand client, it temporarily connects to your enterprise network as a guest.
IT Analytics server	The IT Analytics tool expands upon the built-in reports in Symantec Endpoint Protection Manager by enabling you to create custom reports and custom queries. The tool also offloads the reporting burden from the management server to another server. IT Analytics keeps information for a longer period of time, enforces compliance, reduces costs, and provides summaries. The IT Analytics tool and documentation is located in the Tools\ITAnalytics folder.

Deploying Symantec Network Access Control

It is best to deploy Symantec Network Access Control in phases. This approach allows your organization to evolve an implementation that fits your needs. You build on each previous phase instead of completely redoing your entire security infrastructure to make changes or enhancements.

Table 1-9 Phases for deploying Symantec Network Access Control

Phase	Action	Description
Phase 1	Install Symantec Endpoint Protection Manager and Symantec Network Access Control clients, and configure Host Integrity policies	You can control access for the laptops, desktops, and servers in your organization with Host Integrity and elf-enforcement. With self-enforcement, computers can obtain the software they need to comply with your security policy. Use Symantec Endpoint Protection Manager to configure Host Integrity policies. See "Getting up and running on Symantec Endpoint Protection Manager for the first time" on page 15.
Phase 2	Install and configure a Gateway Enforcer appliance	For partial network protection, control wired and wireless access to the network for managed clients and for guest computers. ■ Managed clients are those that run the Symantec Network Access Control client. ■ Guest clients are the laptops, desktops, and servers that do not meet your security requirements for items such as installed software and secure passwords. These are devices owned by guests such as contractors, consultants, and partners. You can allow these guest clients to safely and temporarily connect to your network with On-Demand clients. See "Installing an Enforcer appliance" on page 29.
Phase 3	Install and configure a LAN Enforcer appliance	For complete network protection, you can control LAN access for client computers and guest computers. See "Installing an Enforcer appliance" on page 29.

See "About the types of enforcement in Symantec Network Access Control" on page 11.

Getting up and running on Symantec Endpoint Protection Manager for the first time

Table 1-10 lists the tasks that you should perform to install and protect the computers in your network immediately.

Table 1-10 Tasks to install and configure Symantec Endpoint Protection Manager

Action	Description
Plan your installation architecture	Before you install the product, consider the size and geographical distribution of your network to determine the installation architecture. To ensure good network and database performance, you need to evaluate several factors. These factors include how many computers need protection, whether any of those computers connect over a wide-area network, or how often to schedule content updates. ■ If your network is small, is located in one geographic location, and has fewer than 500 clients, you need to install only one Symantec Endpoint Protection Manager. ■ If the 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 or load balancing support. Failover and load balancing can only be used with Microsoft SQL Server databases. ■ If your network is geographically dispersed, you may need to install additional management servers for load balancing and bandwidth distribution purposes. To help you plan medium to large-scale installations, see: Symantec Endpoint Protection Sizing and Scalability Best Practices White Paper.

Table 1-10 Tasks to install and configure Symantec Endpoint Protection Manager *(continued)*

Action	Description
Prepare for and then install Symantec Endpoint Protection Manager	**1** Make sure the computer on which you install the management server meets the minimum system requirements. See: Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control **2** Decide on whether to install the embedded database or use a Microsoft SQL Server database. If you use a Microsoft SQL Server database, the installation requires additional steps. These include, but are not limited to, configuring or creating a database instance that is configured to use mixed mode or Windows authentication mode. You also need to provide database server administration credentials to create the database and the database user. These are specifically for use with the management server. **3** You install Symantec Endpoint Protection Manager first. After you install, you immediately configure the installation with the Management Server Configuration Wizard. Decide on the following items when you configure the management server: ■ A password for your login to the management console ■ An email address where you can receive important notifications and reports ■ An encryption password, which may be needed depending on the options that you select during installation See “Installing Symantec Endpoint Protection Manager” on page 20. See “Configuring Symantec Endpoint Protection Manager during installation” on page 21.

Table 1-10 Tasks to install and configure Symantec Endpoint Protection Manager *(continued)*

Action	Description
Add groups, locations, and policies	1 You use groups to organize the client computers, and apply a different level of security to each group. You can use the default groups, import groups if your network uses Active Directory or an LDAP server, or add new groups. If you add new groups, you can use the following group structure as a basis: ■ Desktops ■ Laptops ■ Servers 2 You use locations to apply different policies and settings to computers based on specific criteria. For example, you can apply different security policies to the computers based on whether they are inside or outside the company network. In general, the computers that connect to your network from outside of your firewall need stronger security than those that are inside your firewall. You can set up a location that allows the mobile computers that are not in the office to update their definitions automatically from Symantec's LiveUpdate servers. See Best Practices for Symantec Endpoint Protection Location Awareness. 3 Disable inheritance for the groups or locations for which you want to use different policies or settings. By default, groups inherit their policies and settings from the default parent group, **My Company**. If you want to assign a different policy to child groups, or want to add a location, you must first disable inheritance. Then you can change the policies for the child groups, or you can add a location. 4 For the default Host Integrity policy, you must add requirements for the Host Integrity check to have an effect on the client computer. Before you deploy the policy to client computers, test that the policy works the way that it should.
Change communication settings to increase performance	You can improve network performance by modifying the following client-server communication settings in each group: ■ Use pull mode instead of push mode to control when clients use network resources to download policies and content updates. ■ Increase the heartbeat interval. For fewer than 100 clients per server, increase the heartbeat to 15-30 minutes. For 100 to 1,000 clients, increase the heartbeat to 30-60 minutes. Larger environments might need a longer heartbeat interval. Symantec recommends that you leave **Let clients upload critical events immediately** checked. ■ Increase the download randomization to between one and three times the heartbeat interval.

Table 1-10 Tasks to install and configure Symantec Endpoint Protection Manager *(continued)*

Action	Description
Activate the product license	Purchase and activate a license within 60 days of product installation. See "Activating or importing your Symantec Network Access Control 12.1.x product license" on page 22.
Decide on a client deployment method	Determine which client deployment method would work best to install the client software on your computers in your environment. See "Installing clients with Web Link and Email" on page 25. See "Installing clients with Remote Push" on page 27. See "Installing clients with Save Package" on page 26. If you use Remote Push, you may need to do the following task: If the client computers are part of an Active Directory domain, you must be logged on to the computer that hosts Symantec Endpoint Protection Manager with an account that grants local administrator access to the client computers. You should have administrator credentials available for each client computer that is not part of an Active Directory domain.
Prepare and deploy the client software for installation	1 Make sure that the computers on which you install the client software meet the minimum system requirements. See: Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control 2 Do the following tasks: ■ Make sure that you keep computer mode and not user mode. ■ Update custom client install settings to determine installation options on the client computer. These options include the target installation folder and the restart behavior after installation completes. You can also use the default client install settings. 3 With the Client Deployment Wizard, create a client installation package with selections from the available options, and then deploy it to your client computers.

Table 1-10 Tasks to install and configure Symantec Endpoint Protection Manager *(continued)*

Action	Description
Check that the computers are listed in the groups that you expected and that the client communicates with the management server	In the management console, on the **Clients** > **Clients** page: 1 Change the view to **Client status** to make sure that the client computers in each group communicate with the management server. Look at the information in the following columns: ■ The **Name** column displays a green dot for the clients that are connected to the management server. ■ The **Last Time Status Changed** column displays the time that each client last communicated with the management server. ■ The **Restart Required** column displays the client computers you need to restart to enable protection. ■ The **Policy Serial Number** column displays the most current policy serial number. The policy might not update for one to two heartbeats. You can manually update the policy on the client if the policy does not update immediately. 2 On the client, check that the client is connected to a server, and check that the policy serial number is the most current one.

For information on how to perform these tasks, see the *Symantec Network Access Control Installation and Administration Guide*.

Installing Symantec Endpoint Protection Manager

You perform several tasks to install the management server and the console. In the installation wizard, a green check mark appears next to each completed task.

Note: Symantec Endpoint Protection Manager requires full access to the system registry for installation and normal operation. To prepare a Windows Server 2003 computer on which you plan to remotely install Symantec Endpoint Protection Manager, you must first allow remote control on the computer. When you connect with Remote Desktop, you must also use a console session or shadow the console session in Remote Desktop.

For the most current system requirements, see: Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control

To install Symantec Endpoint Protection Manager

1. If you downloaded the product, extract the entire installation file to a physical disk, such as a hard disk. Run **Setup.exe** from the physical disk.

   If you have a product disc, insert it into the optical drive. The installation should start automatically. If it does not start, open the disc, and then double-click **Setup.exe**.

2. On the **Symantec Endpoint Protection Installation Program** dialog box, click **Install Symantec Network Access Control**.
3. Click **Install Symantec Endpoint Protection Manager.**
4. In the **Welcome** panel, click **Next**.
5. Review the sequence of installation events, and then click **Next**.
6. In the **License Agreement** panel, click **I accept the terms in the license agreement**, and then click **Next**.
7. In the **Destination Folder** panel, accept the default destination folder or specify another destination folder, and then click **Next**.
8. Click **Install**.

   The installation process begins with the installation of the Symantec Endpoint Protection Manager management server and console.

9. Follow the prompts that are provided in the installation wizard.
10. After the initial installation completes, you configure the server and database.

    The **Management Server Configuration Wizard** starts automatically.

    See "Configuring Symantec Endpoint Protection Manager during installation" on page 21.

Configuring Symantec Endpoint Protection Manager during installation

The Management Server Configuration Wizard automatically starts after the Symantec Endpoint Protection Manager installation.

See "Installing Symantec Endpoint Protection Manager" on page 20.

You can also start the Management Server Configuration Wizard at any time after installation from **Start > All Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager Tools**.

To configure the server, you specify the following information:

- The configuration type, which is **Default configuration** or **Custom configuration**. The wizard provides information about each type.
- Whether you want to use a recovery file.

  Note: If this installation is the first installation of Symantec Endpoint Protection Manager, there is no recovery file.

- The password for the default administrator account.
- The email address that receives important notifications and reports.
- The mail server name and port number.
- The Symantec Sales Partner information, if a partner manages your Symantec licenses.

Each configuration type has a separate configuration process. Follow the instructions that are provided in the Management Server Configuration Wizard to complete the configuration.

Activating or importing your Symantec Network Access Control 12.1.x product license

You can use the License Activation Wizard workflow to perform the following tasks:

- Activating a new paid license.
- Converting a trial license to a paid license.
- Renewing a license.
- Activating an additional paid license in response to an over-deployment status.
- Activating a license after you upgrade from a previous version, such as 11.0.

You can import and activate a license file that you received from the following sources:

- Symantec Licensing Portal
- Symantec partner or preferred reseller
- Symantec sales team
- Symantec Business Store

Note: You can only import your Symantec Network Access Control 12.1.x license into a Symantec Network Access Control-enabled management server.

You can start the License Activation Wizard in the following ways:

- The Welcome screen that appears after you install the product.
- From the **Common Tasks** menu on the **Home** page.
- The **Admin** page of the Symantec Endpoint Protection Manager console.

If you activate or import your license from the Welcome screen or the **Common Tasks** menu, you can skip to step 3.

To activate or import your Symantec Network Access Control 12.1.x product license

1. In Symantec Endpoint Protection Manager, click **Admin > Licenses**.
2. Under **Tasks**, click **Activate license**.
3. Click **Activate a new license**, and then click **Next**. If you do not see this panel, continue to the next step.

4 On the **License Activation** panel, select the option that matches your situation, and then click **Next**.

The following table describes each option:

Option	Description
I have a serial number	You may receive a license serial number when you or your Symantec Partner purchased the license. If you have a license serial number, select this option. If you are an eFlex (Symantec Enterprise Options) customer and have an eFlex-generated serial number, select **I have a Symantec License File**.
I have a Symantec License File (.slf)	In most cases, you receive a Symantec license file (.slf file) in an email from Symantec shortly after you complete the purchase process. The file arrives attached to the notification email as a .zip file. If you have received a .slf file, select this option. **Note:** You must extract the .slf file from the .zip file before you can use it to activate your product license. **Warning:** The .slf file contains the information that is unique to your license. To avoid corrupting the license file, do not alter its contents. You may copy the file for your records.

You can find information about eFlex at the following webpage:

Enterprise Options

5 Do one of the following tasks based on the selection that you made in the previous step:

- If you selected **I have a serial number**, enter the serial number, and then click **Submit**. Review the information about the license you added, and then click **Next**.
- If you selected **I have a Symantec License File (.slf)**, click **Add File**. Browse to and select the .slf file you extracted from the .zip file that came with your Symantec notification email. Click **Open**, and then click **Next**.

6 Enter information about your technical contacts and primary contacts, and about your company. Click to acknowledge the disclosure statement, and then click **Submit**.

   If you provided this information when you purchased your license, this panel does not display.

7 Click **Finish**.

Installing clients with Web Link and Email

The Web Link and Email option creates the installation package and the URL for the installation package, and then sends the link to users in an email. The users download the package and install the Symantec Network Access Control client. Users must have administrator privileges to install the package.

Web Link and Email comprises the following tasks:

- You select, configure, and then create the client installation package.
  You choose the options that appear for the configuration of the client installation package. All client installation packages are stored on the computer that runs Symantec Endpoint Protection Manager.
- Email from Symantec Endpoint Protection Manager notifies the computer users that they can download the client installation package.
  You provide a list of users to receive an email message, which contains instructions to download and install the client installation package. Users follow the instructions to install the client software.

Before you begin the client installation with Web Link and Email, make sure that you correctly configure the connection from the management server to the mail server.

To install clients with Web Link and Email

1 In the console, on the **Home** page, in the **Common Tasks** menu, select **Install protection client to computers**.

2 In the **Client Deployment Wizard**, click **New Package Deployment**, and then click **Next**. Web Link and Email only sends a new installation package.

3 Make selections from the available options, which vary depending on the installation package type, and then click **Next**.

4 Click **Web Link and Email**, and then click **Next**.

5 In the **Email Recipients and Message** panel, specify the email recipients and the subject.

   To specify multiple email recipients, type a comma after each email address. A management console System Administrator automatically receives a copy of the message.

   You can accept the default email subject and body, or edit the text. You can also copy the URL and post it to a convenient and secure online location, like an intranet page.

6 To create the package and deliver the link by email, click **Next**, and then click **Finish**.

7 Confirm that the computer users received the email message and installed the client software.

   Client computers may not appear within the management console until after they restart. Depending on the client restart settings of the installed client, you or the computer users may need to restart the client computers.

Installing clients with Save Package

Save Package creates the installation packages that you can install either manually, with third-party deployment software, or with a login script.

Save Package comprises the following tasks:

- You make your configuration selections and then create the client installation packages.
- You save the installation package to a folder on the computer that runs Symantec Endpoint Protection Manager.
  For Windows, the installation package can be for 32- or 64-bit operating systems. The installation package comprises one setup.exe file or a collection of files that includes a setup.exe file. Computer users often find one setup.exe file easier to use.

Either you or the end user can install the installation package on the client computer. Alternately, you can use third-party deployment software to perform the installation.

To install clients with Save Package

1 In the console, on the **Home** page, in the **Common Tasks** menu, click **Install protection client to computers**.

2 In the **Client Deployment Wizard**, do one of the following tasks:

   - Click **New Package Deployment**, and then click **Next**. Save Package only installs a new installation package.

- Click **Communication Update Package Deployment** if you want to update Windows client communication settings on the computers that already have the Symantec Network Access Control client installed. Follow the on-screen instructions, and then go to step 4.

  Note: While the Communication Update Package option appears for Mac, there is no Mac client for Symantec Network Access Control.

3. Make selections from the available options, which vary depending on the installation package type, and then click **Next**.
4. Click **Save Package**, and then click **Next**.
5. Click **Browse** and specify the folder to receive the package.

   For Communication Update Package Deployment, go to step 6.

   For new Windows packages, check **Single .exe file (default)** or **Separate files (required for .MSI)**.

   Note: Use **Single .exe file** unless you require separate files for a third-party deployment program.

6. Click **Next**.
7. Review the settings summary, click **Next**, and then click **Finish**.
8. Provide the exported package to the computer users.

   For example, you can save the package to a secure shared network location, or email the package to the computer users. You can also use a third-party program to install the package.

9. Confirm that the user downloads and installs the client software, and confirm the installation status of the clients.

   Client computers may not appear within the management console until after they restart. Depending on the client restart settings of the installed client, you or the computer users may need to restart the client computers.

Installing clients with Remote Push

Remote Push pushes the client software to the computers that you specify. Using Remote Push requires knowledge of how to search networks to locate computers by IP address or computer names. Once the package copies to the target computer,

the package installs automatically. The computer user does not need to begin the installation or to have administrator privileges.

Remote Push comprises the following tasks:

- You select an existing client installation package, create a new installation package, or create a package to update communication settings.
- For new installation packages, you configure and create the installation package.
- You specify the computers on your network to which Symantec Endpoint Protection Manager sends a package.
  Remote Push locates either specific computers for which you provide an IP number or range, or all computers that are visible by browsing the network.
- Symantec Endpoint Protection Manager pushes the client software to the specified computers.
  The installation automatically begins on the computers once the package successfully copies to the target computer.

To install clients with Remote Push

1. In the console, on the **Home** page, in the **Common Tasks** menu, click **Install protection client to computers**.
2. In the **Client Deployment Wizard**, do one of the following tasks:
   - Click **New Package Deployment** to create a new installation package, and then click **Next**.
   - Click **Existing Package Deployment** to use a package that was previously created, and then click **Browse** to locate the package to install.
     The Client Deployment Wizard uploads the package and directs you to the **Computer Selection** panel (step 5).
   - Click **Communication Update Package Deployment** if you want to update Windows client communication settings on the computers that already have the Symantec Network Access Control client installed. Follow the on-screen instructions, and then go to step 4.

     Note: While the Communication Update Package option appears for Mac, there is no Mac client for Symantec Network Access Control.

3. For a new package, in the **Select Group and Install Feature Sets** panel, make selections from the available options, which vary depending on the installation package type. Click **Next**.
4. Click **Remote Push**, and then click **Next**.

5 In the **Computer Selection** panel, locate the computers to receive the software using one of the following methods:

- To browse the network for computers, click **Browse Network**.
- To find computers by IP address or computer name, click **Search Network**, and then click **Find Computers**.

You can set a timeout value to constrain the amount of time that the server applies to a search.

6 Click **> >** to add the computers to the list, and authenticate with the domain or workgroup if the wizard prompts you.

The remote push installation requires elevated privileges. If the client computer is part of an Active Directory domain, you should use a domain administrator account.

7 Click **Next**, and then click **Send** to push the client software to the selected computers.

Once the **Deployment Summary** panel indicates a successful deployment, the installation starts automatically on the client computers.

The installation takes several minutes to complete.

8 Click **Next**, and then click **Finish**.

9 Confirm the status of the installed clients on the **Clients** page.

For new Symantec Network Access Control installations, the client computers may not appear within the management console until after they are restarted. Depending on the client restart settings of the client, you or the computer users may need to restart the client computers.

Installing an Enforcer appliance

Table 1-11 lists the steps to install all types of Enforcer appliances.

Table 1-11 Installation summary for an Enforcer appliance

Step	Action	Description
Step 1	Learn where to place Enforcers in your network.	Enforcers need to be placed in specific locations on your network to ensure that all endpoints comply with your security policy.

Table 1-11 Installation summary for an Enforcer appliance *(continued)*

Step	Action	Description
Step 2	Set up the appliance.	Connect the Enforcer appliance to your network. See "About the Enforcer appliance indicators and controls" on page 30. See "Setting up an Enforcer appliance" on page 30.
Step 3	Configure the appliance.	Log on and configure the Enforcer appliance from the Enforcer command line. See "Logging on to an Enforcer appliance" on page 31. See "Configuring an Enforcer appliance" on page 32.

About the Enforcer appliance indicators and controls

The Enforcer appliance is installed on a 1U rack-mountable chassis with support for static rails.

You can use the provided serial port and the serial cable to connect to another system that is hooked up to a monitor and keyboard. Alternatively, you can connect a monitor or keyboard directly. If you connect by using the serial port, the default baud rate that is set on the Enforcer is 9600 bps. You must configure the connection on the other system to match. Connecting by the serial port is the preferred method. It lets you transfer files, such as debugging information, to the connected computer for troubleshooting.

See "Installing an Enforcer appliance" on page 29.

See "Setting up an Enforcer appliance" on page 30.

Setting up an Enforcer appliance

Set up the Enforcer appliance hardware by connecting it to your network, switching it on, and logging on at the command line.

See "Installing an Enforcer appliance" on page 29.

See "About the Enforcer appliance indicators and controls" on page 30.

To set up an Enforcer appliance

1. Unpack the Enforcer appliance.
2. Mount the Enforcer appliance in a rack or place it on a level surface.

   See the rack mounting instructions that are included with the Enforcer appliance.

3 Plug it into an electrical outlet.

4 Connect the Enforcer appliance by using one of the following methods:

- Connect another computer to the Enforcer appliance by using a serial port. Use a null modem cable with a DB9 connector (female). You must use terminal software, such as HyperTerminal, CRT, or NetTerm, to access the Enforcer console. Set your terminal software to 9600 bps, data bits 8, no parity, 1 stop bit, no flow control.
- Connect a keyboard and VGA monitor directly to the Enforcer appliance.

5 Connect the Ethernet cables to the network interface ports as follows:

Gateway Enforcer appliance	Connect two Ethernet cables. One cable connects to the eth0 port (internal NIC). The other cable connects to the eth1 port (external NIC) on the rear of the Enforcer appliance. The internal NIC connects to the protected network and the Symantec Endpoint Protection Manager. The external NIC connects to the endpoints.
LAN Enforcer appliance	Connect one Ethernet cable to the eth0 port on the rear of the Enforcer appliance. This cable connects to the internal network. The internal network connects to an 802.1x-enabled switch and to any additional 802.1x-enabled switches in your network.

6 Switch on the power.

The Enforcer appliance starts.

See “Logging on to an Enforcer appliance” on page 31.

See “Configuring an Enforcer appliance” on page 32.

Logging on to an Enforcer appliance

When you turn on or restart the Enforcer appliance, the logon prompt for the Enforcer appliance console appears:

```
Enforcer Login
```

The following levels of access are available:

Superuser	Access to all commands

Normal	Access only to the `clear`, `exit`, `help`, and `show` commands for each level of the command hierarchy

Note: The Enforcer appliance automatically logs users off after 90 seconds of inactivity.

See "Setting up an Enforcer appliance" on page 30.

To log on to an Enforcer appliance with access to all commands

1. On the command line, log on to an Enforcer appliance with access to all commands by typing the following command:

   `root`

2. Type the password that you created during the initial installation.

   The default password is `symantec`.

   The console command prompt for root is `Enforcer#`.

To log on to an Enforcer appliance with limited access to commands

1. If you want to log on to an Enforcer appliance with limited access to commands, type the following command on the command line:

   `admin`

2. Type the password on the command line.

   The default password is `symantec`.

   The console command prompt for admin is `Enforcer$`.

See "Configuring an Enforcer appliance" on page 32.

Configuring an Enforcer appliance

After you log on to the Enforcer appliance, you can configure the appliance from the Enforcer command-line interface.

To configure an Enforcer appliance

1. Specify the type of Enforcer appliance as follows, responding to the prompts from the Enforcer:

   ```
   1. Select Enforcer mode
   [G] Gateway  [L] LAN
   ```

   Where:

G	Gateway Enforcer appliance
L	LAN Enforcer appliance

2. Change the host name of the Enforcer appliance, or press **Enter** to leave the host name of the Enforcer appliance unchanged.

   The default host name of the Enforcer appliance is Enforcer. The name of the Enforcer appliance automatically registers on the Symantec Endpoint Protection Manager during the next heartbeat.

   At the prompt, type the following command if you want to change the host name of the Enforcer appliance:

   ```
   2. Set the host name
   Note:
   1) Input new hostname or press "Enter" for no change. [Enforcer]:
   ```

   `hostname` *hostname*

   where *hostname* is the new host name for the Enforcer appliance.

   Be sure to register the host name of the Enforcer appliance on the Domain Name Server itself.

3. Type the following command to confirm the new host name of the Enforcer appliance:

   ```
   show hostname
   ```

4. Type the IP address of the DNS server and press **Enter**.

5 Type the new root password at the prompt by first typing the following command:

```
password
Old password: new password
```

You must change the root password that you used to log on to the Enforcer appliance. Remote access is not enabled until you change the password. The new password must be at least nine characters long, and contain one lowercase letter, one uppercase letter, one digit, and one symbol.

6 Type the new admin password.

7 Set the time zone by following these prompts.

```
Set the time zone
Current time zone is [+0000]. Change it? [Y/n]
If you click 'Y', follow the steps below:
1) Select a continent or ocean
2) Select a country
3) Select one of the time zone regions
4) Set the date and time
Enable the NTP feature [Y/n]
Set the NTP server:
Note: We set up the NTP server as an IP address
```

8 Set the date and time.

9 Configure the network settings and complete the installation, following the Enforcer prompts.

```
Enter network settings

Configure eth0:
Note: Input new settings.
IP address []:
Subnet mask []:
Set Gateway? [Y/n]
   Gateway IP[]:

   Apply all settings [Y/N]:
```

See "Logging on to an Enforcer appliance" on page 31.

Where to get more information

Table 1-12 displays the websites where you can get best practices, troubleshooting information, and other resources to help you use the product.

Table 1-12 Symantec websites

Types of information	Web address
Trial versions	Trialware
Manuals and documentation updates	■ Product guides for all versions of Symantec Endpoint Protection and Symantec Endpoint Protection Small Business Edition (English) ■ Symantec Endpoint Protection (other languages) ■ Symantec Endpoint Protection Small Business Edition (other languages) ■ Product guides for all versions of Symantec Network Access Control (English) ■ Symantec Network Access Control (other languages)
Technical Support	Includes the public knowledge base, product release details, updates and patches, and contact options for support. Endpoint Protection Technical Support Endpoint Protection Small Business Edition Symantec Network Access Control
Virus and other threat information and updates	Security Response
Free online technical training	SymantecTV
Symantec Educational Services	Symantec Endpoint Security Training Courses
Symantec Connect forums	Endpoint Protection (AntiVirus) Endpoint Protection Small Business Edition 12.x Network Access Control