Symantec™ Network Access Control 12.1.2 Getting Started Guide

For Symantec Network Access Control and Symantec Network Access Control Starter Edition
Getting Started with Symantec Network Access Control

This document includes the following topics:

- About Symantec Network Access Control
- What’s new in Symantec Network Access Control 12.1.2
- About the types of enforcement in Symantec Network Access Control
- Components of Symantec Network Access Control
- Deploying Symantec Network Access Control
- Getting up and running on Symantec Endpoint Protection Manager for the first time
- System requirements for Symantec Network Access Control
- Installing Symantec Endpoint Protection Manager
- Activating or importing your Symantec Endpoint Protection or Symantec Network Access Control 12.1 product license
- Deploying clients using a Web link and email
- Installing an Enforcer appliance
- About the Enforcer appliance indicators and controls
- Setting up an Enforcer appliance
- Logging on to an Enforcer appliance
Configuring an Enforcer appliance

Where to get more information about Symantec Network Access Control

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.

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 financial losses that are associated with lost productivity. To prevent these losses, Symantec Network Access Control controls on site and remote access to corporate 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 remediation server. The remediation server downloads the necessary software, patches, virus definition updates, and so on, to make the client computer compliant. Symantec Network Access Control 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 7.

What's new in Symantec Network Access Control 12.1.2

Symantec Network Access Control 12.1.2 includes new features for Symantec Endpoint Protection Manager, Host Integrity policies, and the Enforcers.

Table 1-1 displays the new features for the management server.
Table 1-1: New features in Symantec Endpoint Protection Manager 12.1.2

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| System requirements | Symantec Network Access Control now includes the following additional system requirements:  
|                   | ■ Symantec Endpoint Protection Manager is supported on Windows 8/Windows Server 2012.  
|                   | ■ The Windows client is supported on Windows 8.  
|                   | ■ Symantec Endpoint Protection Manager is supported on the Microsoft Internet Explorer 10 and Google Chrome Web browsers.  
|                   | For the complete list of system requirements:  
|                   | See “System requirements for Symantec Network Access Control” on page 14.  
|                   | See the knowledge base article: Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control |
| Installation     | The Client Deployment Wizard includes the following changes:  
|                   | ■ The Client Deployment Wizard includes the Communication Update Package Deployment option to push the communications file (Sylink.xml) to the client in a client installation package. You use the Sylink.xml file to convert an unmanaged client to a managed client, or to manage a previously orphaned client. In previous releases, you needed to export the Sylink.xml file from the management server, and import Sylink.xml to each client.  
|                   | ■ Client Deployment Wizard searches the network faster to find computers without the client software installed.  
|                   | You can download and run a new diagnostic tool on the management server and client to help you diagnose common issues before and after installation. The Symantec Help tool enables you to resolve product issues yourself instead of having to call Support.  
|                   | For more information, see the knowledge base article: Symantec Help (SymHelp) |
| Protection features | You can export all the policies, locations, and server settings for a domain. If you then import these policies and settings into a new domain, you do not need to recreate them. |
| LiveUpdate       | The LiveUpdate Settings policy includes an additional type of Group Update Provider (GUP) that allows clients to connect to Group Update Providers in a different subnet. This new type of GUP lets you explicitly define which networks each client may connect to. You can configure a single LiveUpdate policy to meet all your requirements. |

Table 1-2 displays the new features for Host Integrity policies and the Enforcers.
### Table 1-2

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Integrity policies</td>
<td>The Symantec Endpoint Protection Manager Host Integrity policy includes the following new templates that you can import into a Host Integrity requirement. The Symantec Network Access Control client checks whether the client computer meets the requirements of the Host Integrity policy. To save time, you can create a Host Integrity requirement based on an existing template instead of creating a custom requirement.</td>
</tr>
</tbody>
</table>
|                          | - **Removable Drive Scanning**  
  The client scans USB drives after the drives are plugged in. The client then automatically scans the autorun.inf file and any file that is referenced in the autorun.inf file. |
|                          | - **Dual NIC Detection**  
  The client checks whether the computer has dual NICs. If the computer has dual NICs, the client sets a registry key to use as a location switching criterion. The client can switch to a location to block the traffic, log the event, and send the end user a notification. |
|                          | - **Local GUP Status Detection**  
  The client detects whether the local client is a Group Update Provider (GUP) client and checks whether the GUP works correctly. |
|                          | - **Check Domain Logon**  
  The client checks whether the end user is logged on to the correct domain or workgroup. The client switches the end user to a different policy if the end user is not logged on to the correct domain. |
|                          | - **Check Wireless SSID**  
  The client checks the SSID of a client computer to make sure that the computer is connected to the company’s network. |
|                          | - **Disable Print Screen**  
  This client disables the Windows Print Screen functionality. Because data in a picture is harder to detect than data in text, Print Screen captures represent a higher security risk. |
|                          | - **Check Security Center Status**  
  The client checks the status of different security products that are configured through Windows Security Center. For example, the client can check whether an antivirus product is running and enabled or whether Windows Firewall is running and enabled. |
| Enforcers                | - Symantec Network Access Control can now quarantine an infected client.  
  - The Enforcers now run on Red Hat Enterprise Linux 6.1.  
  - The Enforcers include support for the Dell Force10 switch.  
  - The Enforcers include support for Enforcer Syslog events, which provides better monitoring.  
  - You can assign a management server list to an Enforcer so that the Enforcer communicates to multiple management servers.  
  - The Enforcers can now authenticate to servers in one management server list, but remain authorized to connect to servers in another management server list. |
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 1-3 describes the differences between host-based enforcement and network-based enforcement.

<table>
<thead>
<tr>
<th>Type of enforcement</th>
<th>Description</th>
</tr>
</thead>
</table>
| Host-based self enforcement | Allows the client computers to obtain and run the software they need to automatically remediate compliance failures. When the client computer is remediated, it can safely access the network. Host-based enforcement uses 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:  
  - Self-enforcement uses the firewall to police network access, providing the easiest and fastest enforcement deployment option. You can implement self-enforcement more easily if the organization has already deployed the Symantec Endpoint Protection product.  
  - Peer-to-peer enforcement ensures that client-to-client communication occurs only between the company computers and compliant computers outside the company. Compliant computers have the latest company security policy. |
| 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 enforcement requires an Enforcer appliance. |

See “Components of Symantec Network Access Control” on page 8.
Components of Symantec Network Access Control

Table 1-4 lists the product’s components and describes their functions.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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.  
  
  See “Installing Symantec Endpoint Protection Manager” on page 17.                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                         |
| Database                                       | 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.                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                         |
| 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 about using the client, see the Symantec Endpoint Protection and Symantec Network Access Control Client Guide.  
  
  See “About Symantec Network Access Control” on page 4.                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                         |
| Symantec Protection Center                     | Symantec Protection Center lets you integrate management consoles from multiple supported Symantec security products into a single management environment. Symantec Endpoint Protection integrates with Protection Center by means of a series of Web services.  
  You download and install Protection Center version 2 separately.                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                         |
| LiveUpdate Administrator (optional)            | The LiveUpdate Administrator 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.                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                         |
### Table 1-4 Symantec Network Access Control product components (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 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 (optional) | 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. |

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

### 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 1-5 Phases for deploying Symantec Network Access Control

<table>
<thead>
<tr>
<th>Phase</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Phase 1 | Install Symantec Endpoint Protection Manager and Symantec Network Access Control clients. Use Symantec Endpoint Protection Manager to configure Host Integrity policies. | You can control access for the laptops, desktops, and servers your organization that manages with self-enforcement. With self-enforcement, computers can obtain the software they need to comply with your security policy.  
See “Getting up and running on Symantec Endpoint Protection Manager for the first time” on page 10. |
### Table 1-5 Phases for deploying Symantec Network Access Control (continued)

<table>
<thead>
<tr>
<th>Phase</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Phase 2 | Install and configure a Gateway Enforcer appliance. | For partial network protection, control wired and wireless access to the network for managed and unmanaged clients and for guest computers.  
Managed clients are those that running the Symantec Network Access Control client.  
Unmanaged clients are those that:  
- Are not running Symantec Network Access Control client software.  
- Are running Symantec Network Access Control client software, but do not have the latest policy updates.  
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 24. |
| Phase 3 | Install and configure a LAN Enforcer appliance | For complete network protection, you can control LAN access for client computers and guest computers.  
- For managed clients, use a LAN Enforcer appliance.  
- For unmanaged clients, use the LAN or Gateway Enforcer appliances.  
See “Installing an Enforcer appliance” on page 24. |

See “About the types of enforcement in Symantec Network Access Control” on page 7.

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

You should assess your security requirements and decide if the default settings provide the balance of performance and security you require. Some performance enhancements can be made immediately after installing Symantec Endpoint Protection Manager.
Table 1-6 lists the tasks that you should perform to install and protect the computers in your network immediately.

### Table 1-6  Tasks to install and configure Symantec Endpoint Protection Manager

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plan your network architecture</td>
<td>Before you install the product, perform the following tasks:</td>
</tr>
<tr>
<td></td>
<td>■ Make sure the computer on which you install the management server has the minimum system requirements.</td>
</tr>
<tr>
<td></td>
<td>For the most current system requirements, see: Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control</td>
</tr>
<tr>
<td></td>
<td>■ If you are installing or upgrading to the Microsoft SQL Server database, make sure you have the user name and password information.</td>
</tr>
<tr>
<td></td>
<td>■ For networks with more than 500 clients, determine the sizing requirements.</td>
</tr>
<tr>
<td></td>
<td>For more information to help you plan medium to large-scale installations, see the Symantec white paper: Symantec Endpoint Protection Sizing and Scalability Best Practices White Paper</td>
</tr>
<tr>
<td>Install or migrate the management server</td>
<td>Whether you install the product for the first time, upgrade from a previous version, or migrate from another product, you install Symantec Endpoint Protection Manager first.</td>
</tr>
<tr>
<td></td>
<td>See “Installing Symantec Endpoint Protection Manager” on page 17.</td>
</tr>
<tr>
<td>Increase the time that the console leaves you logged on</td>
<td>The console logs you out after one hour. You can increase this period of time.</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Create groups and locations</td>
<td>You can add groups that contain computers based on the level of security or function the computers perform. For example, you might want to put computers with a higher level of security in one group, or a group of Mac computers in another group. Use the following group structure as a basis: ■ Desktops ■ Laptops ■ Servers You can migrate existing Active Directory groups when you install Symantec Endpoint Protection Manager. If you are running legacy Symantec protection, you usually upgrade policy and group settings from your older version. You can apply a different level of security to computers based on whether they are inside or outside the company network. To use this method, you create separate locations and apply different security policies to each location. In general, computers connecting to your network from outside of your firewall need to have 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.</td>
</tr>
<tr>
<td>Disable inheritance on special groups</td>
<td>By default, groups inherit the security and the policy settings from the default parent group, “My Company.” You must disable inheritance before you can change the security and the policy settings for any new groups you create.</td>
</tr>
<tr>
<td>Change communication settings to increase performance</td>
<td>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 and the randomization interval. For under 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. ■ Increase the download randomization to between one and three times the heartbeat interval.</td>
</tr>
<tr>
<td>Modify and test the Host Integrity policy</td>
<td>Add requirements to the Host Integrity policy. <strong>Warning:</strong> Before you deploy the policy to client computers, test that the policy works the way that it should.</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Activate the product license</strong></td>
<td>Purchase and activate a license within 60 days of product installation. See “Activating or importing your Symantec Endpoint Protection or Symantec Network Access Control 12.1 product license” on page 19.</td>
</tr>
<tr>
<td><strong>Prepare computers for client installation (optional)</strong></td>
<td>If you plan to deploy client software remotely, modify or disable the firewall settings on your client computers to allow communication between the computers and the management server. You use the ClientRemote.exe tool, located in the /Tools/PushDeploymentWizard folder on the product disc.</td>
</tr>
<tr>
<td><strong>Install the client software with the Client Deployment Wizard</strong></td>
<td>Create a client installation package and deploy it on your client computers. As a best practice, change the name of the default export package to a name that uniquely identifies the package in your system. See “Deploying clients using a Web link and email” on page 22. Use Computer mode for most environments, not User mode.</td>
</tr>
</tbody>
</table>
| **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 are communicating 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 the client last communicated with the management server.  
   - The Restart Required column displays which 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.  
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. |
| **Check the LiveUpdate schedule and adjust if necessary** | Make sure that the content updates download to client computers at a time that affects users the least. |
| **Configure Symantec Endpoint Protection Manager to send email alerts** | Make sure that you have the notifications set up to alert you in case of an event. Alerts and notifications are critical to maintaining a secure environment and can also save you time. |
For information on how to perform these tasks, see the *Symantec Endpoint Protection and Symantec Network Access Control Installation and Administration Guide*.

## System requirements for Symantec Network Access Control

In general, the system requirements for Symantec Endpoint Protection Manager and the clients are the same as those of the supported operating systems.

Table 1-7 displays the minimum requirements for the Symantec Endpoint Protection Manager.

Table 1-8 displays the minimum requirements for the Symantec Network Access Control client.

Table 1-9 displays the minimum requirements for the Symantec Network Access Control On-Demand client.

### Table 1-7 Symantec Endpoint Protection Manager system requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>■ 32-bit processor: 1-GHz Intel Pentium III or equivalent minimum</td>
</tr>
<tr>
<td></td>
<td>(Intel Pentium 4 or equivalent recommended)</td>
</tr>
<tr>
<td></td>
<td>■ 64-bit processor: 2-GHz Pentium 4 with x86-64 support or equivalent minimum</td>
</tr>
<tr>
<td>Note:</td>
<td>Intel Itanium IA-64 processors are not supported.</td>
</tr>
<tr>
<td>Physical RAM</td>
<td>1 GB of RAM for 32-bit operating systems, 2 GB of RAM for 64-bit operating</td>
</tr>
<tr>
<td></td>
<td>systems, or higher if required by the operating system</td>
</tr>
<tr>
<td>Hard drive</td>
<td>4 GB or more free space; plus 4 GB for the locally installed database.</td>
</tr>
<tr>
<td>Display</td>
<td>1024 x 768</td>
</tr>
</tbody>
</table>
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
- SQL Server 2008 R2
- SQL Server 2012

Note: If you install the Symantec Endpoint Protection Manager and the SQL database on the same computer, a minimum of 4 GB of RAM is recommended.

For information about the system requirements for the Symantec AntiVirus client on Linux, see the *Symantec AntiVirus for Linux Implementation Guide*. 
Table 1-8  
**Symantec Network Access Control client system requirements**

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
</table>
| Processor     | ■ 32-bit processor for Windows: 1-GHz Intel Pentium III or equivalent minimum (Intel Pentium 4 or equivalent recommended)  
■ 64-bit processor for Windows: 2-GHz Pentium 4 with x86-64 support or equivalent minimum. 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 Server 2003 (32-bit, 64-bit, R2, SP1 or later)  
■ Windows Server 2008 (32-bit, 64-bit)  
■ Windows Server 2012  
■ 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 |

Table 1-9  
**Symantec Network Access Control On-Demand client system requirements**

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
</table>
| Processor     | ■ Windows: Intel Pentium II 550 MHz (1 GHz for Windows Vista) or faster  
■ Mac: Intel CPU only |
Table 1-9  Symantec Network Access Control On-Demand client system requirements (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>■ Windows XP Home or Professional (32-bit, SP2 and SP3)</td>
</tr>
<tr>
<td></td>
<td>■ Windows Vista (32-bit, 64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows 7 (32-bit, 64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows 8 (32-bit, 64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2003 (32-bit, 64-bit, R2, SP1 or later)</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2008 (32-bit, 64-bit, R2)</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2012</td>
</tr>
<tr>
<td></td>
<td>■ Windows Small Business Server 2008 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows Essential Business Server 2008 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Mac OS X 10.5, 10.6 or 10.7</td>
</tr>
<tr>
<td>Disk space and physical RAM</td>
<td>■ Download size: 9 MB. The amount of free disk space that is needed</td>
</tr>
<tr>
<td></td>
<td>to run the client: 100 MB.</td>
</tr>
<tr>
<td></td>
<td>■ Physical RAM for either Windows or Mac On-Demand Client: 512 MB</td>
</tr>
<tr>
<td>Web browser</td>
<td>■ For Windows On-Demand Client: Microsoft Internet Explorer 6.0 or later; Mozilla Firefox 2.0, 3.0, 3.5, 3.6.3, 11.0</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Clients from version 11.0 RU6 and lower do not support Firefox 3.6.3.</td>
</tr>
<tr>
<td></td>
<td>■ For Mac On-Demand Client: Apple Safari 4.0 and 5.0; Mozilla Firefox 2.0, 3.0, 3.5, 3.6.3</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Clients from version 11.0 RU6 and lower do not support Firefox 3.6.3.</td>
</tr>
<tr>
<td>Other</td>
<td>■ Video display: Super VGA (1,024 x 768) or higher</td>
</tr>
<tr>
<td></td>
<td>■ At least one Ethernet adapter (with TCP/IP installed)</td>
</tr>
</tbody>
</table>

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

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:** The Symantec Endpoint Protection Manager requires access to the system registry for installation and normal operation. To prepare a server that runs Windows Server 2003 to install Symantec Endpoint Protection Manager using a remote desktop connection, you must first allow remote control on the server. You must also use a remote console session, or shadow the console session.

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. Insert and display the product disc.

   The installation should start automatically. If it does not start, double-click **Setup.exe**.

   If you downloaded the product, unzip the folder and extract the entire product disc image to a physical disc, such as a hard disk. Run **Setup.exe** from the physical disc.

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 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 the management server during installation” on page 19.

11. After the server and the database configuration, you optionally migrate your Symantec legacy virus protection installation to the new version.

    See “Deploying clients using a Web link and email” on page 22.
Configuring the management server during installation

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

See “Installing Symantec Endpoint Protection Manager” on page 17.

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: default or custom. The wizard provides information about each type.
■ Whether you want to use a recovery file.

Note: If this is your 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 email server name and port number.
■ You can optionally add partner information if you have a Symantec Sales Partner who 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 Endpoint Protection or Symantec Network Access Control 12.1 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 a license after you upgrade from a previous version, such as Symantec Endpoint Protection 11.x.

Activating an additional paid license in response to an over-deployment status.

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 import your Symantec Network Access Control 12.1 license into a Symantec Network Access Control-enabled management server only.

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

- The Symantec Endpoint Protection 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 the first three of the following steps.

**To activate or import your Symantec Endpoint Protection or Symantec Network Access Control 12.1 product license**

1. On the Symantec Endpoint Protection Manager console, click **Admin**.
2. On the **Admin** page, click **Licenses**.
3. Under **Tasks**, click **Activate license**.
4. In the **License Activation Wizard**, select **Activate a new license**, and then click **Next**. If you do not see this panel, continue to the next step.
5 On the **License Activation** panel, select the option that matches your situation, and then click **Next**.

The following table describes each option:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>I have a serial number</strong></td>
<td>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 <strong>I have a Symantec License File</strong>.</td>
</tr>
<tr>
<td><strong>I have a Symantec License File (.slf)</strong></td>
<td>In most cases, a Symantec license file (.slf file) is sent to you 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. <strong>Note:</strong> You must extract the .slf file from the .zip file before you can use it to activate your product license. <strong>Warning:</strong> 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.</td>
</tr>
</tbody>
</table>

You can find information about eFlex at the following URL: [Enterprise Options](#)

6 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 was attached to your Symantec notification email. Click **Open**, and then click **Next**.
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.

Click **Finish**.

---

**Deploying clients using a Web link and email**

The Web link and email method creates a URL for each client installation package. You send the link to users in an email or make it available from a network location.

Web link and email performs the following actions:

- Selects and configures the client installation packages.
  Client installation packages are created for 32-bit and 64-bit Windows computers. The installation packages are stored on the computer that runs Symantec Endpoint Protection Manager.

- Notifies the computer users about the client installation packages.
  An email message is sent to the selected computer users. The email message contains instructions to download and install the client installation packages. Users follow the instructions to install the client software.

The Mac client install package is automatically exported as a `.zip` archive file. To expand the package and extract the folder containing the Apple installer file (.pkg) and the Additional Resources folder, you must use either the Mac Archive Utility or the ditto command. You cannot use the Mac `unzip` command, a third-party application, or any Windows application to expand this file. You must keep the `.pkg` file and the Additional Resources folder together to complete the installation successfully.

Before you deploy the client installation package with email, make sure that you correctly configure the connection from the management server to the mail server.

You start the client deployment from the console.
To deploy clients by using a 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** to create a new installation package, and then click **Next**.

   **Existing Package Deployment** lets you deploy the packages that have been exported previously, but you can only use Remote Push with this option.

   **Communication Update Package Deployment** lets you update client communication settings on the computers that already have the client installed. Use this option to convert an unmanaged client to a managed client. You can only use Remote Push or Save Package with this option.

3. For a new package, make selections from **Install Packages**, **Group**, **Install Feature Sets**, **Install Settings**, **Content Options**, and **Preferred Mode**. Click **Next**.

   **Note**: To uninstall third-party security software on the client, you must configure custom Client Install Settings before launching the Client Deployment Wizard. To see which third-party software the client package removes, see the following knowledge base article: *About the third-party security software removal feature in Symantec Endpoint Protection 12.1*.

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 online location, like an intranet page.

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

6. 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 are restarted. Depending on the client restart settings of the deployed client, you or the computer users may need to restart the client computers.
Installing an Enforcer appliance

Table 1-10 lists the steps to install all types of Enforcer appliances.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Learn where to place Enforcers in your network.</td>
<td>Enforcers need to be placed in specific locations on your network to ensure that all endpoints comply with your security policy.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Set up the appliance.</td>
<td>Connect the Enforcer appliance to your network. See “About the Enforcer appliance indicators and controls” on page 24. See “Setting up an Enforcer appliance” on page 26.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Configure the appliance.</td>
<td>Log on and configure the Enforcer appliance from the Enforcer command line. See “Logging on to an Enforcer appliance” on page 27. See “Configuring an Enforcer appliance” on page 28.</td>
</tr>
</tbody>
</table>

About the Enforcer appliance indicators and controls

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

Figure 1-1 shows the controls, indicators, and connectors that are located behind the optional bezel on the front panel.

Figure 1-1  Enforcer appliance front panel

1  DVD-ROM drive
2  Power switch
3  Reset icon
4  USB ports
5  Hard drive light
Figure 1-2 shows the back panel of the system.

**Figure 1-2** Enforcer appliance back panel (Failopen model shown)

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 24.

See “Setting up an Enforcer appliance” on page 26.
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 24.

See “About the Enforcer appliance indicators and controls” on page 24.

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 27.
See “Configuring an Enforcer appliance” on page 28.

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:

<table>
<thead>
<tr>
<th>Level</th>
<th>Access Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Superuser</td>
<td>Access to all commands</td>
</tr>
<tr>
<td>Normal</td>
<td>Access only to the <code>clear</code>, <code>exit</code>, <code>help</code>, and <code>show</code> commands for each level of the command hierarchy</td>
</tr>
</tbody>
</table>

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

See “Setting up an Enforcer appliance” on page 26.

**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 28.
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

   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 27.
Where to get more information about Symantec Network Access Control

The primary documentation is available in the Documentation folder on the product disc. Tool-specific documents are located in the subfolders of the Tools folder on the product disc.

Updates to the documentation are available from the Symantec Technical Support Web site at the following location:

Network Access Control

The product includes the following documentation:

- Symantec Endpoint Protection and Symantec Network Access Control Installation and Administration Guide
- Symantec Endpoint Protection and Symantec Network Access Control Client Guide
- Symantec LiveUpdate Administrator User's Guide
  The LiveUpdate tool is located in the Tools\LiveUpdate folder on the Tools product disc.
- Symantec Endpoint Protection Manager Database Schema Reference
  This document is located on the Symantec Technical Support Web site: Endpoint Protection

Table 1-11 displays the Web sites where you can get additional information to help you use the product.

<table>
<thead>
<tr>
<th>Types of information</th>
<th>Web address</th>
</tr>
</thead>
<tbody>
<tr>
<td>software</td>
<td></td>
</tr>
<tr>
<td>Public knowledge base</td>
<td><a href="http://www.symantec.com/business/support/overview.jsp?pid=52788">http://www.symantec.com/business/support/overview.jsp?pid=52788</a></td>
</tr>
<tr>
<td>Releases and updates</td>
<td></td>
</tr>
<tr>
<td>Manuals and documentation updates</td>
<td></td>
</tr>
<tr>
<td>Contact options</td>
<td></td>
</tr>
<tr>
<td>Virus and other threat information and updates</td>
<td><a href="http://www.symantec.com/business/security_response/index.jsp">http://www.symantec.com/business/security_response/index.jsp</a></td>
</tr>
<tr>
<td>Product news and updates</td>
<td><a href="http://enterprisesecurity.symantec.com">http://enterprisesecurity.symantec.com</a></td>
</tr>
</tbody>
</table>
Table 1-11  Symantec Web sites (continued)

<table>
<thead>
<tr>
<th>Types of information</th>
<th>Web address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free online technical training</td>
<td><a href="http://go.symantec.com/education_septc">http://go.symantec.com/education_septc</a></td>
</tr>
<tr>
<td>Symantec Educational Services</td>
<td><a href="http://go.symantec.com/education_sep">http://go.symantec.com/education_sep</a></td>
</tr>
<tr>
<td>Symantec Connect forums</td>
<td><a href="http://www.symantec.com/connect/security/forums/network-access-control">http://www.symantec.com/connect/security/forums/network-access-control</a></td>
</tr>
</tbody>
</table>
Where to get more information about Symantec Network Access Control