

Release Notes for Symantec™
Endpoint Protection v12.1,
Symantec Endpoint
Protection Small Business
Edition v12.1, Symantec
Network Access Control
v12.1

Updated: Friday, June 24, 2011



Release Notes: Symantec™ Endpoint Protection v12.1, Symantec Endpoint Protection Small Business Edition v12.1, Symantec Network Access Control v12.1

This document includes the following topics:

- [About this document](#)
- [About Symantec Endpoint Protection version 12.1](#)
- [What's new in version 12.1](#)
- [Where to get more information](#)
- [Planning the installation](#)
- [Upgrading to a new release](#)
- [Upgrading your Symantec Endpoint Protection installation to include Symantec Network Access Control](#)

- [Known issues and workarounds](#)

About this document

Please review this document in its entirety before you install or roll out Symantec Endpoint Protection, Symantec Network Access Control, Symantec Endpoint Protection Small Business Edition, or call for technical support. It describes known issues and provides additional information that is not included in the standard documentation or the context-sensitive help.

This document contains information for all three versions of Symantec Endpoint Protection:

- Symantec Endpoint Protection, full version
- Symantec Network Access Control
- Symantec Endpoint Protection Small Business Edition

You should assume that all material applies to all versions. Known issues specific to Symantec Network Access Control appear in their own section, and known issues specific to Symantec Endpoint Protection Small Business Edition appear in their own section.

You can find the latest version of these release notes at the following URL:

[Release Notes](#)

About Symantec Endpoint Protection version 12.1

This release adds new platform support, new features, and defect fixes. Version 12.1 is the upgrade for the Symantec Endpoint Protection and Symantec Network Access Control 11.x product line. All functionality of version 11.x is maintained, unless otherwise noted.

See “[What's new in version 12.1](#)” on page 4.

What's new in version 12.1

The current release includes the following improvements that make the product easier and more efficient to use.

[Table 1-1](#) displays the new features in version 12.1.

Table 1-1 New features in version 12.1

Feature	Description
Better security against malware	<p>The most significant improvements include the following policy features to provide better protection on the client computers.</p> <ul style="list-style-type: none"> ■ The Virus and Spyware Protection policy detects threats more accurately while it reduces false positives and improves scan performance with the following technologies: <ul style="list-style-type: none"> ■ SONAR replaces the TruScan technology to identify malicious behavior of unknown threats using heuristics and reputation data. While TruScan runs on a schedule, SONAR runs at all times. ■ Auto-Protect provides additional protection with Download Insight, which examines the files that users try to download through Web browsers, text messaging clients, and other portals. Download Insight uses reputation information from Symantec Insight to make decisions about files. ■ Insight lets scans skip Symantec and community trusted files, which improves scan performance. ■ Insight Lookup detects the application files that might not typically be detected as risks and sends information from the files to Symantec for evaluation. If Symantec determines that the application files are risks, the client computer then handles the files as risks. Insight Lookup makes malware detection faster and more accurate. ■ The Firewall policy includes firewall rules to block IPv6-based traffic. ■ The Intrusion Prevention policy includes browser intrusion prevention, which uses IPS signatures to detect the attacks that are directed at browser vulnerabilities.

Table 1-1 New features in version 12.1 (*continued*)

Feature	Description
Faster and more flexible management	<p>Symantec Endpoint Protection Manager helps you manage the client computers more easily with the following new features:</p> <ul style="list-style-type: none"> ■ Centralized licensing lets you purchase, activate, and manage product licenses from the management console. ■ Symantec Endpoint Protection Manager registers with Protection Center version 2. Protection Center lets you centralize data and integrate management of Symantec security products into a single environment. You can configure some of the settings Protection Center uses to work with Symantec Endpoint Protection Manager. ■ The Symantec Endpoint Protection Manager logon screen enables you to have your forgotten password emailed to you. ■ Symantec Endpoint Protection Manager includes an option to let any of the administrators in a site reset their forgotten password. ■ You can configure when and how Symantec Endpoint Protection Manager restarts the client computer, so that the restart does not interfere with the user's activity. ■ The Monitors page includes a set of preconfigured email notifications that inform you of the most frequently used events. The events include when new client software is available, when a policy changes, license renewal messages, and when the management server locates unprotected computers. The notifications are enabled by default and support the BlackBerry, iPhone, and Android. ■ The Home page displays the high-level reports that you can click, which makes the Home page simpler and easier to read. The Home page also displays a link to notifications about log events that you have not yet read. ■ Improved status reporting automatically resets the Still Infected Status for a client computer once the computer is no longer infected. ■ You can now configure Linux clients to send log events to Symantec Endpoint Protection Manager.
Better server and client performance	<p>To increase the speed between the management server and the management console, database, and the client computers:</p> <ul style="list-style-type: none"> ■ The management server performs automatic database cleanup tasks to improve the server-client responsiveness and scalability. ■ Virus and spyware scans use Insight to let scans skip safe files and focus on files at risk. Scans that use Insight are faster and more accurate, and reduce scan overhead by up to 70 percent. ■ LiveUpdate can run when the client computer is idle, has outdated content, or has been disconnected, which uses less memory.

Table 1-1 New features in version 12.1 (*continued*)

Feature	Description
Support for virtual environments	<p>Enhanced to help protect your virtual infrastructure, Symantec Endpoint Protection includes the following new features:</p> <ul style="list-style-type: none"> ■ The Shared Insight Cache Server lets clients share scan results so that identical files only need to be scanned once across all the client computers. Shared Insight Cache can reduce the effect of full scans by up to 80%. ■ The Virtual Image Exception tool reduces the effect of scanning every single file in a trusted base image. Instead of continually scanning system files for viruses, the Virtual Image Exception tool lets you white list files from your baseline image on virtual machines. ■ Symantec Endpoint Protection Manager uses hypervisor detection to automatically detect which clients run on a virtual platform. You can create policies for groups of clients on virtual platforms. ■ The Symantec offline image scanner can scan offline VMware .vmdk files to ensure that there are no threats in the image.
Support for Mac clients	<p>In Symantec Endpoint Protection, you can configure the policies for Mac clients based on a location as well as a group.</p> <p>In Symantec Endpoint Protection Small Business Edition, you can now deploy and manage Mac clients in Symantec Endpoint Protection Manager.</p>
Improved installation process	<p>You can install the product faster and easier than before with the following new installation features:</p> <ul style="list-style-type: none"> ■ The Symantec Endpoint Protection Manager installation wizard lets you import a previously saved recovery file that includes client-server connection information. The recovery file enables the management server to reinstall existing backed-up certificates and to automatically restore the communication to the existing clients. ■ The management server Web service uses Apache instead of IIS. You do not need to install IIS first, as you did in previous versions. ■ The Client Deployment Wizard quickly locates unprotected computers on which you need to install the client software. The wizard also provides an email deployment link so that users can download the client software by using the Web. The wizard makes client software faster and easier to deploy. ■ You can upgrade to the current version of the product while the legacy clients stay connected and protected. ■ A new quick report for deployment shows which computers have successfully installed the client software.

Table 1-1 New features in version 12.1 (*continued*)

Feature	Description
Support for additional operating systems	<p>Symantec Endpoint Protection Manager now supports the following additional operating systems:</p> <ul style="list-style-type: none"> ■ VMware Workstation 7.0 or later ■ VMware ESXi 4.0.x or later ■ VMware ESX 4.0.x or later ■ VMware Server 2.0.1 ■ Citrix XenServer 5.1 or later <p>Symantec Endpoint Protection Manager now supports the following Web browsers:</p> <ul style="list-style-type: none"> ■ Internet Explorer 7.0, 8.0, 9.0 ■ Firefox 3.6, 4.0 <p>The Symantec AntiVirus for Linux client now supports the following additional operating systems:</p> <ul style="list-style-type: none"> ■ RedHat Enterprise Linux 6.x ■ SUSE Linux Enterprise Server and Enterprise Desktop 11.x (includes support for OES 2) ■ Ubuntu 11.x ■ Fedora 14.x, 15.x ■ Debian 6.x <p>For information about using the Symantec AntiVirus client on Linux, see the <i>Symantec AntiVirus for Linux Client Guide</i>.</p>

Table 1-1 New features in version 12.1 (*continued*)

Feature	Description
<p>Better Enforcer management in Symantec Endpoint Protection Manager</p>	<p>You can manage the Enforcers more easily by configuring the following Enforcer settings in Symantec Endpoint Protection Manager:</p> <ul style="list-style-type: none"> ■ Ability for the clients in an Enforcer group to synchronize their system time constantly by using the Network Time Protocol server. ■ You can more easily update the list of MAC addresses with the following improvements: <ul style="list-style-type: none"> ■ For the DHCP Integrated Enforcer, you can import a text file that contains the MAC address exceptions that define trusted hosts. ■ For the LAN Enforcer, you can add, edit, and delete the MAC addresses that the Host Integrity checks ignore by using the following features: <p>MAC Authentication Bypass (MAP) bypasses the Host Integrity check for non-802.1x clients or the devices that do not have the Symantec Network Access Control client installed.</p> <p>Ignore Symantec NAC Client Check bypasses the Host Integrity check for 802.1x supplicants that do not have the Symantec Network Access Control client installed.</p> ■ You can add individual MAC addresses or use wildcards to represent vendor MAC strings. You can also import the MAC addresses from a text file. ■ You can add MAC addresses with or without an associated VLAN, which allows multiple VLANs to be supported.
<p>New Network Access Control features in Symantec Endpoint Protection Manager</p>	<p>Symantec Endpoint Protection Manager includes the following additional functionality for Symantec Network Access Control:</p> <ul style="list-style-type: none"> ■ Enforcer management server lists can include management servers from replication partners. Enforcers can connect to any management server at any site partner or replication partner. ■ The Compliance logs for the Symantec Network Access Control client provide additional information about log events and Host Integrity check results. You can now see which requirement caused a Host Integrity check on a client computer to fail. ■ LiveUpdate downloads Host Integrity templates to management servers. Therefore, client computers can get the Host Integrity policies that include updated Host Integrity templates. ■ Enforcer groups support limited administrator accounts and administrator accounts as well as system administrator accounts. For a large company with multiple sites and domains, you probably need multiple administrators, some of whom have more access rights than others.

Table 1-1 New features in version 12.1 (*continued*)

Feature	Description
New Enforcer features	<p>Symantec Network Access Control includes the following new features:</p> <ul style="list-style-type: none"> ■ 64-bit support for the Integrated Enforcers. ■ Support for the Network Policy Server (NPS) with the Microsoft Windows Server 2008 (Longhorn) implementation of a RADIUS server and proxy. The Enforcer can now authenticate the clients that run Windows Vista or later versions and that use 802.1x authentication. ■ For the DHCP Integrated Enforcer, you can selectively turn on scope-based enforcement for the scopes that you define. ■ The Gateway Enforcer supports both 802.1q trunking and On-Demand Clients at the same time. You can designate a single VLAN on a multiple trunk VLAN to host On-Demand Clients. ■ Support for the guest enforcement mode, which enables the Gateway Enforcer to act as a download server for On-Demand Clients. The Gateway Enforcer downloads On-Demand Clients to guest computers, enabling the clients to communicate to the Enforcer through the guest computers' Web browsers. In the guest enforcement mode, the Gateway Enforcer does not forward inline traffic. ■ Support for On-Demand Client "persistence": the capability to be "live" for a designated period. ■ The local database size has been increased to 32 MB to accommodate a larger number of MAC addresses.

Where to get more information

The product includes several sources of information.

The primary documentation is available in the Documentation folder on the product disc. Updates to the documentation are available from the Symantec Technical Support Web site.

The product includes the following documentation:

- *Symantec Endpoint Protection Getting Started Guide*
Symantec Endpoint Protection Small Business Edition Getting Started Guide
Symantec Network Access Control Getting Started Guide
This guide includes the system requirements and an overview of the installation process.
- *Symantec Endpoint Protection and Symantec Network Access Control Implementation Guide*
Symantec Endpoint Protection Small Business Edition Implementation Guide
This guide includes procedures to install, configure, and manage the product.

- *Symantec Endpoint Protection and Symantec Network Access Control Client Guide*
Symantec Endpoint Protection Small Business Edition Client Guide
 This guide includes procedures for users to use and configure the Symantec Endpoint Protection or Symantec Network Access Control client.
- *Symantec LiveUpdate Administrator User's Guide*
 This guide explains how to use the LiveUpdate Administrator. This guide is located in the Tools\LiveUpdate folder on the product disc.
- *Symantec Central Quarantine Implementation Guide*
 This guide includes information about installing, configuring, and using the Central Quarantine. This guide is located in the CentralQ folder on the product disc.
- *Symantec Endpoint Protection Manager Database Schema Reference*
 This guide includes the database schema for Symantec Endpoint Protection Manager.
- *Symantec Client Firewall Policy Migration Guide*
 This guide explains how to migrate from Symantec Client Firewall Administrator to Symantec Endpoint Protection Manager.
- Online Help for Symantec Endpoint Protection Manager and for the client
 These Online Help systems contain the information that is in the guides plus context-specific content.
- Tool-specific documents that are located in the subfolders of the `Tools` folder on the product disc.

Table 1-2 displays the Web sites where you can get additional information to help you use the product.

Table 1-2 Symantec Web sites

Types of information	Web address
Symantec Endpoint Protection software	http://www.symantec.com/business/products/downloads/
Public knowledge base	Symantec Endpoint Protection:
Releases and updates	http://www.symantec.com/business/support/overview.jsp?pid=54619
Manuals and documentation updates	Symantec Endpoint Protection Small Business Edition:
Contact options	http://www.symantec.com/business/support/overview.jsp?pid=55357 Symantec Network Access Control: http://www.symantec.com/business/support/overview.jsp?pid=52788

Table 1-2 Symantec Web sites (*continued*)

Types of information	Web address
Virus and other threat information and updates	http://www.symantec.com/business/security_response/index.jsp
Product news and updates	http://enterprisesecurity.symantec.com
Free online technical training	http://go.symantec.com/education_septc
Symantec Educational Services	http://go.symantec.com/education_sep
Symantec Connect forums	<p>Symantec Endpoint Protection: http://www.symantec.com/connect/security/forums/endpoint-protection-antivirus</p> <p>Symantec Endpoint Protection Small Business Edition: http://www.symantec.com/connect/security/forums/endpoint-protection-small-business</p> <p>Symantec Network Access Control: http://www.symantec.com/connect/security/forums/network-access-control</p>

Planning the installation

Table 1-3 summarizes the high-level steps to install Symantec Endpoint Protection.

Table 1-3 Installation planning

Step	Action	Description
Step 1	Plan network architecture and review and purchase a license	<p>Understand the sizing requirements for your network. In addition to identifying the endpoints requiring protection, scheduling updates, and other variables should be evaluated to ensure good network and database performance.</p> <p>For information to help you plan medium to large-scale installations, see the Symantec white paper, Sizing and Scalability Recommendations for Symantec Endpoint Protection.</p> <p>Purchase a license within 30 days (Small Business Edition) or 60 days (full version) of product installation.</p>
Step 2	Review system requirements	Make sure your computers comply with the minimum system requirements and that you understand the product licensing requirements.

Table 1-3 Installation planning (*continued*)

Step	Action	Description
Step 3	Prepare computers for installation	Uninstall other virus protection software from your computers, make sure system-level access is available, and open firewalls to allow remote deployment.
Step 4	Open ports and allow protocols	Remotely deploying the client requires that certain ports and protocols are open and allowed between the Symantec Endpoint Protection Manager and the endpoint computers.
Step 5	Identify installation settings	Identify the user names, passwords, email addresses, and other installation settings. Have the information on hand during the installation.
Step 6	Install the management server	<p>Install Symantec Endpoint Protection Manager.</p> <p>If the network that supports your business is small and located in one geographic location, you need to install only one Symantec Endpoint Protection Manager. If your network is geographically dispersed, you may need to install additional management servers for load balancing and bandwidth distribution purposes.</p> <p>If your network is very large, you can install additional sites with additional databases and configure them to share data with replication. To provide additional redundancy, you can install additional sites for failover support</p>
Step 7	Migrate Symantec legacy virus protection software	If you are running legacy Symantec protection, you usually migrate policy and group settings from your older version.
Step 8	Prepare computers for client installation	<p>Prepare for client installation as follows:</p> <ul style="list-style-type: none"> ■ Identify the computers on which to install the client software. ■ Identify the methods to use to deploy the client software to your computers. ■ Uninstall third-party virus protection software from your computers. ■ Modify or disable the firewall settings on your endpoint computers to allow communication between the endpoints and the Symantec Endpoint Protection Manager. ■ Set up the console computer groups to match your organizational structure.
Step 9	Install clients	<p>Install the Symantec Endpoint Protection client on your endpoint computers.</p> <p>Symantec recommends that you also install the client on the computer that hosts Symantec Endpoint Protection Manager.</p>

Table 1-3 Installation planning (*continued*)

Step	Action	Description
Step 10	Post-installation tasks	<p>Perform the following post-installation tasks after you install Symantec Endpoint Protection:</p> <ul style="list-style-type: none"> ■ Install additional clients, if necessary. ■ As needed, migrate Symantec legacy virus protection software if you did not perform this task earlier. ■ Become familiar with the features and functions of the console. ■ Verify that your client computers are online and protected. ■ Check the LiveUpdate schedule and adjust if necessary. ■ Check notifications. ■ Set up computer groups. ■ Create additional administrator accounts. ■ Register your product serial number, and import your license file into the console.

For comprehensive instructions for installing and configuring the product, see the *Symantec Endpoint Protection and Symantec Network Access Control Implementation Guide*.

Upgrading to a new release

You can upgrade to the latest release of the product. To install a new version of the software, you must perform certain tasks to ensure a successful upgrade.

The information in this section is specific to upgrading from Symantec Sygate 5.1, or Symantec Endpoint Protection 11.x software in environments where a version of Symantec Endpoint Protection or Symantec Network Access Control 11.x is already installed.

The information in this section is specific to upgrading software in environments where a version of Symantec Endpoint Protection 11.x or Symantec Endpoint Protection Small Business Edition 12.0 is already installed.

Table 1-4 Process for upgrading to the full version

Step	Action	Description
Step 1	Back up the database	Back up the database used by the Symantec Endpoint Protection Manager to ensure the integrity of your client information.

Table 1-4 Process for upgrading to the full version (*continued*)

Step	Action	Description
Step 2	Turn off replication	Turn off replication on all sites that are configured as replication partners. This avoids any attempts to update the database during the installation.
Step 3	If you have Symantec Network Access Control installed, enable local authentication	Enforcers are not able to authenticate clients during an upgrade. To avoid problems with client authentication, Symantec recommends that you enable local authentication before you upgrade. After the upgrade is finished, you can return to your previous authentication setting.
Step 4	Stop the Symantec Endpoint Protection Manager service	You must stop the Symantec Endpoint Protection Manager service prior to installation.
Step 5	Upgrade the Symantec Endpoint Protection Manager software	Install the new version of the Symantec Endpoint Protection Manager on all sites in your network. The existing version is detected automatically, and all settings are saved during the upgrade.
Step 6	Turn on replication after the upgrade	Turn on replication when the installation is complete to restore your configuration.
Step 7	Upgrade Symantec client software	<p>Upgrade your client software to the latest version.</p> <p>When Symantec provides updates to client installation packages, you add the updates to a Symantec Endpoint Protection Manager and make them available for exporting. You do not, however, have to reinstall the client with client-deployment tools. The easiest way to update clients in groups with the latest software is to use AutoUpgrade. You should first update a group with a small number of test computers before you update your entire production network.</p> <p>You can also update clients with LiveUpdate if you permit clients to run LiveUpdate and if the LiveUpdate Settings policy permits</p>

Table 1-5 Process for upgrading to the Small Business Edition

Step	Action	Description
Step 1	Back up the database	Back up the database used by the Symantec Endpoint Protection Manager to ensure the integrity of your client information.
Step 2	Stop the Symantec Endpoint Protection Manager service	The Symantec Endpoint Protection Manager service must be stopped during the installation.

Upgrading your Symantec Endpoint Protection installation to include Symantec Network Access Control

Table 1-5 Process for upgrading to the Small Business Edition (*continued*)

Step	Action	Description
Step 3	Upgrade the Symantec Endpoint Protection Manager software	Install the new version of the Symantec Endpoint Protection Manager in your network. The existing version is detected automatically, and all settings are saved during the upgrade.
Step 4	Upgrade Symantec client software	<p>Upgrade your client software to the latest version.</p> <p>By default, the upgraded Symantec Endpoint Protection Manager automatically upgrades the managed clients. To disable this feature, right-click your Group, select Properties, and then check Disable Automatic Client Package Updates.</p> <p>Note: This feature was added in version 12.0.1001.95, and is retained for version 12.1.x. This feature was not available in version 12.0.122.192</p>

Upgrading your Symantec Endpoint Protection installation to include Symantec Network Access Control

If you have already installed Symantec Endpoint Protection Manager and want to upgrade your installation to include Symantec Network Access Control, use the following procedure.

To upgrade your Symantec Endpoint Protection installation to include Symantec Network Access Control

- 1 Insert the disc labeled DVD-SNAC-EE in your DVD drive.

If you downloaded the product, unzip the folder and extract the entire product disc image to a physical disc, such as a hard disk.
- 2 Follow the instructions as detailed in the *Symantec™ Network Access Control Getting Started Guide*. In summary, those steps are:
 - If the installation does not start immediately, run `Setup.exe` from the DVD or from the location where you downloaded and unzipped the installation files.
 - Click **Install Symantec Network Access Control**.
 - Click **Install Symantec Endpoint Protection Manager**. Installation packages are copied to your server.

- The Management Server Upgrade Wizard runs. Click **Next** when prompted to upgrade the management server. The Server upgrade status screen shows that the Wizard imports packages, then upgrades templates.
- When the status screen shows "Upgrade Succeeded," click **Next**.
- In the **Upgrade Succeeded** dialog box, **Start the Symantec Endpoint Protection Manager** is chosen. Click **Finish**, and you are prompted to log on to Symantec Endpoint Protection Manager.
- You have upgraded your Symantec Endpoint Protection Manager to provide Symantec Network Access Control capabilities, packages, and menu choices. To confirm, click **Policies**, and you see **Host Integrity** as a new choice. This is one of the Symantec Network Access Control capabilities that you added.
- Configure and deploy your clients.

Note: At this point, you have activated the user interface for the product features. To activate enforcement and license reporting, you must activate your Symantec Network Access Control product licenses with either serial numbers or slf license files. For instructions, see "Activating your product license" in the *Symantec™ Network Access Control Getting Started Guide*.

[2409621]

Known issues and workarounds

The issues in this section are new for Symantec Endpoint Protection version 12.1. Please review this document in its entirety before you install or roll out Symantec Endpoint Protection, Symantec Network Access Control, Symantec Endpoint Protection Small Business Edition, or call for technical support. It describes known issues and provides the additional information that is not included in the standard documentation or the context-sensitive help.

The "known issues" section is divided into parts according to the version of Symantec Endpoint Protection you are using:

- Known issues that apply to all versions.
See ["Issues applying to all versions of Symantec Endpoint Protection"](#) on page 18.
- Known issues that apply only to Symantec Endpoint Protection Small Business Edition.
See ["Symantec Endpoint Protection Small Business Edition issues"](#) on page 29.

Known issues and workarounds

- Known issues that apply only to the full version of Symantec Endpoint Protection.
See [“Symantec Endpoint Protection full version issues”](#) on page 29.
- Known issues that apply only to Symantec Network Access Control. These issues include issues related to the Enforcer and to Host Integrity/Security Compliance.
See [“Symantec Network Access Control issues”](#) on page 35.
- Known issues that are found only in the documentation for any one of the versions. These are primarily typos. Anything that relates directly to the product is located in the product-specific sections.
See [“Documentation issues”](#) on page 41.

Note: Some of the links to knowledge base articles that are included in the product and the documentation may not work until the final product release.

Issues applying to all versions of Symantec Endpoint Protection

The known issues listed in this section apply to all versions of Symantec Endpoint Protection.

Upgrades, installation, uninstallation issues

This section contains information about upgrades, installation, uninstallation, and repair.

UPGRADES

Symantec Endpoint Protection client sometimes fails to install on systems with ExpanDrive for Windows installed

In some instances, ExpanDrive for Windows is incompatible with the Symantec Endpoint Protection client. This incompatibility appears more often in cases where Backup Exec is backing up to a drive managed by ExpanDrive for Windows at the time of upgrade to the latest version of Symantec Endpoint Protection. In those instances the system "blue screens" on `ExpanDrive.sys` before finishing the installation.

The workaround is to uninstall ExpanDrive for Windows.

[2273586]

Notification email not generated after upgrade

Administrators can opt to be notified by email when system events happen. On systems that upgrade and that are using a default mail server, the notification email is not generated.

The workaround is to explicitly set the email server address. In Symantec Endpoint Protection Manager, click **Admin > Servers > %select server% > Email server**, and enter the server address.

[2363295]

INSTALLATION

Minimum hard disk requirement for the Windows client is 900MB

The documentation states a different requirement, but under some circumstances this amount of disk space may be insufficient. Plan for 900MB of free space on the hard disks of Windows client computers.

[2384226]

When using the Web console, client package downloads may not complete the first time

When creating client packages, depending on your browser security settings, you may see a message saying that your download was blocked, or asking if you want to download the file. The download is blocked even if you accept the download in the browser.

If you create the package the second time, the package should be downloaded successfully.

[2357557]

During installation of the client, Windows Security Center may incorrectly state that "Symantec Endpoint Protection is turned off"

You can safely ignore this warning. You do not need to take any action.

[2120916]

Windows Event Viewer may show an Apache error related to domain names

This Apache error, number 3299, relates to the DNS suffix that is defined for your computer. It has no effect on Symantec Endpoint Protection, although it might affect other programs.

To determine your configuration, type the following string at the command prompt: `ipconfig /all` and press **Enter**. You should see a display similar to the following:

Known issues and workarounds

```
Windows IP Configuration

Host Name . . . . . : SEPM

Primary DNS Suffix . . . . . :

Node Type . . . . . : Hybrid

IP Routing Enabled. . . . . : No

WINS Proxy Enabled. . . . . : No
```

If you have no entry on the line for the Primary DNS Suffix, you may see this error.

[2322768]

Changing system clock may cause false "license expired" messages

If your system clock is changed and changed back, the Web server service must be restarted. The symptom you may see is "Unexpected server error."

To resolve this issue, restart the service `semwebsrv`.

[2362071]

PGP users may experience difficulties installing the Symantec Endpoint Protection client on computers with encrypted hard disks

The symptom is that the computer rolls back the installation after the PGP pre-boot process.

The workaround is to remove the PGP encryption, install the Symantec Endpoint Protection client, and re-enable the encryption.

[2357592]

Best practice: Use Silent or Show me the progress bar installation packages on the computers that run 32-bit and 64-bit Windows Vista, Windows 2008 Server, and Windows 7 operating systems

On 32-bit and 64-bit Windows Vista, Windows 2008 Server, and Windows 7 operating systems, you should not select **Interactive mode** when you do the following:

- Add installation packages to a group
- Export installation packages

Interactive installations on 32-bit and 64-bit Windows Vista, Windows 2008 Server, and Windows 7 operating systems prompt users to continue in Session 0, which most users will not see or understand. When you install on these operating

systems, use the **Silent** or **Show me the progress bar** installation setting. This usage requires you to create a named **Client Installation Setting**.

[2393258]

Hostnames with underscore “_” characters are not supported

If your Symantec Endpoint Protection Manager is installed on a host with an underscore “_” character in the server name, such as “SEPM_Server”, you may have issues logging in to the Web console. This is because Internet Explorer does not support cookies created on servers with illegal characters in the hostname. An underscore is an illegal character in a TCP hostname, as documented in RFC 952.

To work around this issue, rename your server before migrating. If you change the hostname of your Symantec Endpoint Protection Manager server after installation, you should run the **Server Configuration Wizard** after you rename your server.

[2398196]

Migration

This section contains information about migration from one version or release to another.

LiveUpdate no longer shares definitions among products

You can use LiveUpdate to update your definitions. However, those definitions will not update your other Symantec products.

To work around this change in LiveUpdate, re-enable the scheduler in your other Symantec products and update them independently of Symantec Endpoint Protection.

[2374182]

Installing the security certificate in Internet Explorer 8

When you install Symantec Endpoint Protection Manager, one of the steps you must go through is the installation of the security certificate.

To install the security certificate

- 1** On the certificate alert screen, click **Continue to this website (not recommended)**.
- 2** In the browser address box, click **Certificate Report**.
- 3** In the **Untrusted Certificate** window, click **View Certificates**.

- 4 On the **View Certificates** window, click **Install Certificate**.
- 5 In the **Certificate Import Wizard**, click **Show Physical Stores**.
- 6 Click **Place all certificates in the following store** and then click **Browse**.
- 7 In the **Select Certificate Store** window, expand **Trusted Root Certification Authorities**, click **Local Computer**, and then click **OK**.
- 8 In the **Certificate Import** confirmation message, click **OK**.
- 9 In the **Certificate** dialog, click **OK**.
- 10 Restart Internet Explorer 8.

[2307849]

Symantec Endpoint Protection Manager issues

This section contains information about Symantec Endpoint Protection Manager.

Client cannot connect to groups with double-byte names

When you import a SyLink file that has groups that are named with double-byte characters, the import fails. The SylinkDrop tool can be used to register clients to different Symantec Endpoint Protection Manager servers, to change unmanaged clients to managed clients, and so on. In some instances where a group is named with DBCS characters, this results in a "hang" on the client.

To work around this problem, change the language version of non-Unicode programs to the language that you need. Then import the SyLink file. The client is properly managed and reflected in Symantec Endpoint Protection Manager.

[2292093, 2273612]

Help for the Advanced Settings filter of the audit log is missing

Context-sensitive help for the **Audit log and quick report** contains an incorrect note and is missing information about advanced options. The note should be replaced with the following text:

Note: The filter option fields are not case-sensitive. Some fields accept wildcard characters. You can use the wildcard character question mark (?), which matches any one character, and the asterisk (*), which matches any string of characters. The following table should be included in the Help:

Table 1-6 Advanced Settings filter options for views of the Audit log

Option	Description
Event type	<p>Specifies the type of events that you want to view.</p> <p>You can select one of the following event types:</p> <ul style="list-style-type: none"> ■ All ■ Policy added ■ Policy deleted ■ Policy edited ■ Add shared policy upon system install ■ Add shared policy upon system upgrade ■ Add shared policy upon domain creation
Policy name	<p>Specifies the name of the policy that you want to view information about.</p> <p>This field accepts a comma-separated list as input. You can use the wildcard character question mark (?), which matches any one character, and the asterisk (*), which matches any string of characters.</p>
Domain	<p>Specifies the domain that you want to view information about.</p> <p>This field accepts a comma-separated list as input. You can use the wildcard character question mark (?), which matches any one character, and the asterisk (*), which matches any string of characters. You can also click the dots to select from a list of known domains.</p>
Site	<p>Specifies the local or the remote site that you want to view information about.</p> <p>You can use the wildcard character question mark (?), which matches any one character, and the asterisk (*), which matches any string of characters. You can also click the dots to select from a list of known sites.</p>
Server	<p>Specifies the server that you want to view information about.</p> <p>You can use the wildcard character question mark (?), which matches any one character, and the asterisk (*), which matches any string of characters. You can also click the dots to select from a list of known servers.</p>
User	<p>Specifies the user that you want to view information about.</p>

Table 1-6 Advanced Settings filter options for views of the Audit log
(continued)

Option	Description
Limit	Specifies how many entries to display on each page of the view. You can select from 20, 100, 200, and 1000 entries. The default limit is 20 entries.

[2374356]

Symantec Endpoint Protection Manager policy issues

This section includes information about working with policies in Symantec Endpoint Protection Manager.

VIRUS AND SPYWARE PROTECTION POLICIES

This section includes information about issues relating to Virus and Spyware Protection policies.

Insight troubleshooting and proxy exclusions: additional information

If your client computers use a proxy with authentication, you must specify trusted Web domain exceptions for Symantec URLs. The exceptions let your client computers communicate with Symantec Insight and other important Symantec sites. For information about the recommended exceptions, see the related Technical Support knowledge base article:

[Insight troubleshooting and proxy exclusions](#)

Using URL and .PAC proxy settings with authentication within IE does not allow reputation traffic

The traffic to the Download Insight servers is blocked when using proxy servers with authentication that are defined by URL or .PAC proxy settings. As a result, the reputation data on the Download Insight servers is not considered in evaluating potential threats.

Symantec recommends that you create exclusions on your proxy servers to allow network traffic. Exclusions are as follows:

Table 1-7 Exclusions you should set to allow reputation traffic

Type of traffic	Server address
Ping submissions	https://stnd-avpg.crsi.symantec.com https://avs-avpg.crsi.symantec.com https://stnd-ipsg.crsi.symantec.com https://bash-avpg.crsi.symantec.com
Sample submissions	https://central.ss.crsi.symantec.com https://central.nrsi.symantec.com https://central.avsi.symantec.com https://central.b6.crsi.symantec.com
CAT submissions	https://tuslgwynwapex01.symantec.com
Error submissions	https://stnd-lueg.crsi.symantec.com
Insight reports	https://ent-shasta-mr-clean.symantec.com
Insight	https://ent-shasta-rrs.symantec.com
Licensing	https://services-prod.symantec.com
Telemetry	https://tses.symantec.com/
SETI	https://tses.symantec.com/
LiveUpdate	http://liveupdate.symantecliveupdate.com

[2272505]

Multi-threaded scans are not supported in Symantec Endpoint Protection 12.1

Support for multi-threaded scans in earlier Symantec Endpoint Protection 11.x versions used registry keys, which is not a supported approach in 12.1. You should not use those registry keys, which are located in:

- 64 bit system:
`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Symantec\Symantec Endpoint Protection\AV`
- 32 bit system:
`HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\AV`

[2315424]

Customers using PGP may experience problems with virus definitions loading correctly

You may have problems with virus definitions loading properly via LiveUpdate if you use PGP's file shredding option.

To work around this issue, turn off the PGP file shredding option.

[2305817]

Shared Insight Cache port clarification

The **Shared Insight Cache Settings** pane should include the following descriptions:

Listening Port	The port on which the server listens. The listening port is used by clients to submit scan results for files and to make requests to determine if the client should scan a file. The default port number is 9005.
Status Listening Port	The port the server uses to communicate status within the system. The status listening port uses a SOAP-based interface on the port specified in the configuration section. This interface provides a mechanism by which an administrator can query information and status about the Cache Server. The default port number is 9006.

FIREWALL and INTRUSION PREVENTION POLICIES

This section includes information about issues relating to Firewall and Intrusion Prevention policies.

Browser window appears to hang when Intrusion Prevention makes a detection

For some browser Intrusion Prevention detections, Symantec Endpoint Protection might need to close the browser. If Symantec Endpoint Protection needs to close the browser, it displays a confirmation alert. In some cases, the alert message might be hidden by the browser window, and the browser appears to hang.

To work around this issue, move or minimize the browser window to view the alert message and click **OK** to terminate the browser.

[2279752]

EXCEPTIONS POLICIES

This section includes information about issues relating to Exceptions policies.

Tamper Protection may be triggered by third-party software

Some third-party software may make changes that inadvertently attempt to modify Symantec components. The result is that Tamper Protection displays notifications about these actions.

To work around this issue, ensure that the application is safe, and then create an exception for it in your Exceptions policies. You should also contact Symantec directly and send in your Control log.

You should also send your Tamper Protection log events (which appear in the Control log) to Symantec. Contact Technical Support for instructions on how to upload the log.

[2319187]

Context-sensitive help for Monitors > Logs > Risk logs page has missing/incorrect description for Action

The following text should replace the description for the **Action** option:

You can select an action to create an exception for the selected item in the log.

Table 1-8 Action options for the Risk logs

Option	Description
Add risk to Exceptions policy	Creates a known risk exception. Applies only to files that are detected as security risks (such as adware or spyware) that are known security risks.
Add file to Exceptions policy	Creates an exception for the detected file so that virus and spyware scans no longer detect the file. The file is identified by its file path.
Add folder to Exceptions policy	Creates an exception for the folder where the detected files resides. Applies only to virus and spyware scans, not to SONAR scans. The exception does not automatically include subfolders.
Add extension to Exceptions policy	Creates an exception for the extension of the detected file. For example, if the file that you select has an extension of .doc, then DOC is added to the list of extensions that virus and spyware scans do not scan.

Table 1-8 Action options for the Risk logs (*continued*)

Option	Description
Trust Web domain	Creates a trusted Web domain exception that applies to the URL from which the file was downloaded. The exception only applies to files that are detected by Download Insight.
Allow application	Creates an application exception with an action of Ignore. The file is identified by its hash. The exception applies to both SONAR and any virus and spyware scan.
Block application	Creates a SONAR application exception with an action of Quarantine. The files is identified by its hash.
Delete from Quarantine	Does not create an exception. Removes the selected item from the client computers' Quarantine.

[2372914]

Context-sensitive help for Monitors > Logs > SONAR logs page has missing/incorrect description for Action

The following text should replace the description for the **Action** option:

You can select an action to create an exception for the selected item in the log.

Table 1-9 Action options for the SONAR logs

Option	Description
Add folder to Exceptions policy	Creates a SONAR folder exception for the folder where the file resides and does not automatically apply to subfolders. The exception applies only to SONAR.
Allow application	Creates an application exception with an action of Ignore. The file is identified by its hash. The exception applies to both SONAR and any virus and spyware scan.
Block application	Creates a SONAR application exception with an action of Quarantine. The file is identified by its hash.

Table 1-9 Action options for the SONAR logs (*continued*)

Option	Description
Trust Web domain	Creates a trusted Web domain exception that applies to the URL from which the file was downloaded. The exception only applies to files that are detected by Download Insight.

[2372914]

Symantec Endpoint Protection Small Business Edition issues

These issues are found only in Symantec Endpoint Protection Small Business Edition.

LiveUpdate may fail on Small Business Edition clients that are installed in a DBCS path

The symptom of the failure is an error, "Failed to process update..." even though the update has downloaded successfully.

To work around this issue, do not install clients in a path that is defined with DBCS characters.

[2322728]

Symantec Endpoint Protection full version issues

This section includes items that only apply to the full version of Symantec Endpoint Protection.

Upgrades, installation, uninstallation, and repair issues

This section contains information about upgrades, installation, uninstallation, and repair issues.

UPGRADES

AutoUpgrade of 5.x clients to 12.1 clients requires adding 11.x packages to Symantec Endpoint Protection Manager and optionally downloading Host Integrity packages

The process for autoupgrading legacy clients is described in the documentation. In addition to the steps that are described at the beginning of chapter 7, you must manually import 11.x packages to Symantec Endpoint Protection Manager. If you

plan to implement Host Integrity policies, you must also download the Windows Host Integrity package.

To work around this issue, manually import legacy Symantec Endpoint Protection 11.x packages from the product disc to legacy Symantec Sygate Endpoint Protection 5.1 clients first, then autoupgrade to Symantec Endpoint Protection version 12.1 clients.

[2359294]

Migration issues

This section contains information about migration.

Migration from a dedicated IIS Web site to Apache only uses the first custom port

Symantec Endpoint Protection version 12.1 now uses Apache for Web services rather than Internet Information Services (IIS). While most of the transition is automatic, some areas require you to take action.

If Symantec Endpoint Protection Manager was installed using a dedicated IIS Web site, you may have configured that Web site to assign multiple ports to listen on. Apache only listens on one of those ports after migration. Not listening on the other ports may cause clients to be disconnected.

To work around this issue, manually enter the missing ports into Apache's `httpd.conf` file.

An example follows. Enter the appropriate ports in your `httpd.conf` file.

Editing the `httpd.conf` file to listen to ports 80 and 8080

- 1 Open the `httpd.conf` file with a text editor.
- 2 Find the line that begins with `Listen`.
- 3 Add two lines after it:

```
Listen 80  
Listen 8080
```

- 4 Save the file.

For additional information on the `httpd.conf` file usage, see [Apache's documentation](#).

[2040661]

Symantec Endpoint Protection 12.1 clients may connect to Symantec Endpoint Protection Manager 11.x servers, but this is not a supported configuration

Symantec does not support the use of Symantec Endpoint Protection Manager 11.x servers with 12.x clients. However, it may work in some cases. Symantec strongly recommends that you upgrade your servers first, and then your clients. This approach helps to avoid data loss and other unintended consequences.

[2244591]

Symantec Endpoint Protection 11.x clients can migrate to Symantec Endpoint Protection 12.1, but may continue reporting to the original Symantec Endpoint Protection Manager version 11.x

Clients that have already been connected successfully to an 11.x management server can migrate successfully to version 12.1. However, they stay connected to their 11.x management server.

To configure clients to report to the 12.1 Symantec Endpoint Protection Manager, run the SylinkDrop tool, located in `Tools\SylinkDrop` on the product disc.

[2376026]

Symantec Endpoint Protection Manager issues

This section contains information about Symantec Endpoint Protection Manager.

The Quarantine Server has intermittent forwarding failures in Symantec Endpoint Protection 12.1

Symantec Endpoint Protection 12.1 sometimes fails to forward quarantine items to the Quarantine Server.

To resolve this issue, be certain that Microsoft .Net framework version 3.5 is installed on your computer.

[2293167]

Default autoreplication timing has changed with this release

The Autoreplicate option performs the replication process every two hours. Previous versions of the product automatically replicated every five minutes.

[2348121]

Potential conflicts exist with database maintenance jobs

If you install Symantec Endpoint Protection Manager with the Microsoft SQL database, the management server automatically performs database maintenance tasks. If you have already set up database maintenance tasks for the Microsoft

SQL database using another tool, such as the SQL Server Management Studio, the tasks may result in an undesired outcome. To work around this issue, disable the database maintenance tasks in Symantec Endpoint Protection Manager.

To disable database maintenance tasks

- 1 In the console, click **Admin**, and then click **Servers**.
- 2 Under **Servers**, click the icon that represents the database.
- 3 Under **Tasks**, click **Edit Database Properties**.
- 4 On the **General** tab, uncheck both of the following options:
 - **Truncate the database transaction logs**
 - **Rebuild Indexes**

[2365974]

Instructions for changing the SSL port are missing a step

The topic, "Changing the SSL port assignment," in the *Symantec™ Endpoint Protection and Symantec Network Access Control Implementation Guide*, is missing a step.

After step 2, add the following step:

2.1 Edit the line `VirtualHost _default_:443` to read `VirtualHost _default_:new port`. For example, if the new port number is 53300, the edited string becomes `VirtualHost _default_:53300`.

[2365848]

Symantec Endpoint Protection Manager policy issues

This section includes information about working with policies in Symantec Endpoint Protection and Symantec Network Access Control.

VIRUS AND SPYWARE PROTECTION POLICIES

This section includes the known issues information related to Virus and Spyware Protection policies.

User authentication fails between Symantec Endpoint Protection Manager and the Cache Server when the user name or host name uses DBCS or high-ASCII characters

You can enter user names and host names using DBCS or high-ASCII characters. However, that usage causes communication to fail between Symantec Endpoint Protection Manager and the Cache Server.

To work around this problem, do not use DBCS or high-ASCII characters for user names or host names.

[2321474]

Global Scan Options help link contents are incorrect

In the Symantec Endpoint Protection Shared Insight Cache tool, the help screen for Global Scan Options is incorrect. The correct entry is:

Username	If you configure the Shared Insight Cache for basic authentication, type the authentication user name.
Change Password	If you configure the Shared Insight Cache for basic authentication, click this option to specify and confirm the authentication password.

[2374377]

PROACTIVE THREAT PROTECTION POLICIES

This section includes the known issues information related to Proactive Threat Protection policies.

Registry key condition for application control rule interprets specified registry value data as string-only

If you create a registry key condition for an application control rule, and you enter the registry key value data, the data is treated like a string. The data is not treated like a number. For example, if you create a registry key condition with the name `AAA` and the registry key value data of `111`, and the application rule is set to block, the rule only blocks `AAA` when it is created as a string. It does not block `AAA` when it is created as any other registry data type.

[2222096]

When using Protection Center to access Symantec Endpoint Protection Manager, the Browse button in the "Search for Applications" dialog box does not launch

You can find specific information about the applications that your clients run. You can use this information to help you set up policy features that control or detect applications, such as firewall or application and control rules. This feature is inoperative in the Protection Center view of Symantec Endpoint Protection Manager.

To search for applications, launch Symantec Endpoint Protection Manager directly, rather than using Protection Center.

[2360274]

Application and Device Control cannot be reliably managed on the client

Application and Device Control enabling and disabling should only be managed on the Symantec Endpoint Protection Manager.

[2361600]

Symantec Endpoint Protection Windows and Mac client issues

This section contains information about Symantec Endpoint Protection client issues on both the Windows and Mac platforms.

Device control notifications only appear the first time a device is blocked

Assume that you have a Device Control policy that contains a rule that blocks new devices, writes to the log, and displays a notification. The first time a new device is plugged in, everything works fine. Symantec Endpoint Protection has blocked the device by setting the device driver to "disabled." The next time the device is plugged in, no notification is displayed, and no log is generated. This behavior is because the device driver is not loaded (as it is set to disabled), so the Device Control policy is not triggered.

This behavior is a known limitation.

[2222901]

Clients may become disconnected from Symantec Endpoint Protection Manager when using Location Based Communication Settings

Symantec Endpoint Protection is designed so that clients can know their location (in the office, at home, on the road, etc.). Based on that location, their policies can change, including the Management Server to which they are linked.

If you are using a policy that is triggered by a location, the client may become disconnected when it is using that location-based policy.

To work around this problem:

- Change the client's location, even temporarily.
- Restart the client.

[2295065]

Clients configured as Group Update Providers (GUP) may experience slight slowdowns

This slowdown has been noted and the product team is working on improving the download rate and bandwidth usage.

[2346194]

The Symantec Endpoint Protection client may have difficulty doing a forced shutdown if password protection is implemented

Implementing a forced shutdown of the Symantec Endpoint Protection client may not work properly if the client has implemented password protection. Normally, issuing the command `smc -stop` should stop all client services. The command does not work reliably in this situation.

To work around this issue, either do not implement password protection on the service shutdown command, or do not use the command.

[2350794]

Network Threat Protection does not show Unicode supplementary characters properly

When application names are displayed in the **Network** dialog boxes on the client, the file names of those applications that are named with Unicode supplementary characters display as two question marks. This display appears in the **Network Activity** dialog box and in the dialog box that asks the user whether to allow an application to access the network.

[2235266]

The documentation for External Communications Settings > Proxy Server incorrectly refers to HTTPS configuration

On the Symantec Endpoint Protection Manager, clicking **Clients > Policies > External Communications Settings > Proxy Server (Windows)** or **Proxy Server (Mac)** shows **Proxy Configuration**. Beneath, it provides a location for **Port**. The documentation incorrectly refers to HTTPS for the Proxy Configuration and for the Port.

You can safely ignore the documentation references to HTTPS on this dialog box.

[2395521, 2407418, 2406066]

Symantec Network Access Control issues

The issues listed in the following sections relate specifically to:

- Symantec Network Access Control
- The Symantec Network Access Control clients, including the on-demand clients
- The Symantec Enforcer, including both the Enforcer appliance and the Integrated Enforcers
- Host Integrity, which manages security compliance at the client level

- **Enforcer and Symantec Network Access Control client issues**
See [“Enforcer issues”](#) on page 36.
- **Host Integrity and security compliance issues**
See [“Host Integrity issues”](#) on page 39.

Enforcer issues

This section includes information about Enforcer features, which are only available in Symantec Network Access Control.

Readme links on Enforcer DVD are broken; use the links on the Symantec Network Access Control DVD

The links to Release Notes on the Enforcer DVD are broken. For correct links, use the links on the Symantec Network Access Control DVD instead.

[2414290, 2414940]

The Symantec Endpoint Encryption encrypted OS partition cannot be checked by Host Integrity in the Windows on-demand client using user-level privileges

On Windows XP SP3, if the encrypted partition was encrypted using user-level privileges, Host Integrity checks it under the same privilege level, and fails. This failure is because the HI check creates a javascript file that cannot be written into the profile space under user-level privileges.

To work around this issue, create the partition and check the partition under administrator privilege level, if possible.

[2227714]

Symantec Endpoint Protection Manager does not respond to a RADIUS request from the Enforcer

In some cases, Symantec Endpoint Protection Manager does not respond to a RADIUS request from the Enforcer for 802.1x authentication of a client. The most likely cause for this is a port conflict.

To work around this problem, see the knowledge base article, [Error: "Port 1812 is already in use. Stop your Radius server if you have the Enforcer installed." while installing Symantec Endpoint Protection Manager.](#)

[1451524]

Symantec Endpoint Protection does not support upgrades of the Enforcer appliance from Symantec Endpoint Protection 11 MR 4 to Symantec Endpoint Protection 12.1

This upgrade path is not supported. You must install a new image.

[2206255]

Quarantined Symantec Network Access Control clients' user interface mistakenly shows them as connected for a few seconds

When Symantec Network Access Control clients are moved to a quarantine VLAN because they fail a Host Integrity compliance check, the client user interface is slow to update.

It is safe to ignore this defect. The user interface updates in 5-10 seconds, but the quarantine properly takes effect immediately.

[1945979]

The Gateway Enforcer's on-demand configuration does not automatically update when the Enforcer is configured to connect to a new Symantec Endpoint Protection Manager

If you connect the Gateway Enforcer to a different management server, you must refresh the on-demand client configuration. This problem appears with the domain-ID and the client group name.

To work around this problem, the on-demand functionality has to be toggled (disabled and then enabled) to use the new Symantec Endpoint Protection Manager's domain-ID and client group.

[2115639]

Enforcers that are part of different failover groups should not be placed into the same group on Symantec Endpoint Protection Manager

Enforcer groups and Symantec Endpoint Protection Manager groups use different IDs internally. While this configuration is an advantage in most cases, it can cause confusion when two Enforcers use the same hub, for example, to reach Symantec Endpoint Protection Manager.

To work around this confusion, place Enforcers that are in different Enforcer failover groups into different Symantec Endpoint Protection Manager groups.

[2317172]

On-demand Mac clients generated by the Symantec Network Access Control 11.0.5 Enforcer cannot be upgraded

There are differences in the encryption keys used in versions of the on-demand client after Symantec Network Access Control 11.0.5. These differences cause Mac on-demand clients after version 11.0.5, including 12.1 clients, to fail to start from Symantec Network Access Control Enforcers of version 11.0.5 and earlier.

To work around this issue, upgrade your Enforcer image to Symantec Network Access Control 11.0.6343 or later, or to version 12.1.

[2332534]

When the guest-enforcement feature is enabled for On-Demand clients, the eth1 of the Gateway Enforcer should be disabled

When in guest enforcement mode, the eth1 port of the Gateway Enforcer should be disabled. If it is not, you are creating a potential security hole. Note that the eth1 interface sill still show as enable if you issue the command `configure show interface`. You can safely ignore this message.

[2103402]

MAC address overlapping of VLAN ID is not supported from file imports in Symantec Network Access Control version 12.1

MAC addresses can be imported into the LAN Enforcer. However, overlapping of addresses is not supported. When MAC address conflicts with VLAN IDs occur, the LAN Enforcer drops the second most current conflicted MAC address. The LAN Enforcer then shows that dropped MAC address with its VLAN ID in the Enforcer log message.

[2106972]

Changing from Gateway Enforcer to LAN Enforcer may improperly permit the On-Demand Client to be downloaded

If the Gateway Enforcer has the On-Demand Client enabled, you may see this behavior after re-initializing to the LAN Enforcer. Downloading the On-Demand Client from a LAN Enforcer is not expected behavior, and thus may cause unexpected behavior. The LAN Enforcer cannot manage the On-Demand Client properties such as authentication configuration, PEAP/TLS credential configuration, and so on.

To work around this issue, you should disable the On-Demand Client before reinitializing the Enforcer.

[2103543]

How to change the RADIUS authentication port with the Integrated Enforcer

In some cases, the RADIUS authentication port may be set to a non-standard port number. The RADIUS port defaults to 1812.

To set the RADIUS port to be 1812:

1 Change the following registry key to read as shown below

```
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint  
Protection\SNAC\Enforcer\NAC Communication Service\smsinfo -  
CurrentSEPMRadiusAuthenticationPort:1812
```

2 Restart the Enforcer server from the user interface, or restart the services Symantec Integrated Enforcer and Symantec NAC Communication Service

Note: If you change the RADIUS port on Symantec Endpoint Protection Manager, you should mirror that change on the Integrated Enforcer, substituting the new port number for "1812" in the above procedure.

[2232004]

Host Integrity issues

This section includes information about Host Integrity policies, which are available only with Symantec Network Access Control. Host Integrity policies ensure compliance with organizational security policies.

Host Integrity may show as "disabled" in the Troubleshooting dialog box for the client when Host Integrity is first enabled

Host Integrity checking is disabled while content downloads. Once content downloads, the Host Integrity check commences and an accurate report or remediation takes place.

[2297661]

Compliance checking may be delayed while content downloads

The Compliance check requires that Symantec Network Access Control client download content from Symantec Endpoint Protection Manager. In some cases, this download may take a long time. To prevent inaccurate Compliance status messages, this check is disabled until the required content is downloaded. To determine the actual Security Compliance status of a particular client, consult the status in the **Help > Troubleshooting** dialog box.

Note: The effect of this issue is that the Enforcer reports clients as having passed security compliance checks even though the actual status is unknown.

[2325358]

Host Integrity quarantine policies do not work on the On-Demand Client for Mac

The On-Demand Client for the Mac does not support switching to a quarantine location when Host Integrity fails. This feature only works with the On-Demand Client for Windows.

[2104391]

Host Integrity results display in English only on 5.1 clients

When upgrading from Symantec Sygate Enterprise Protection 5.1, the Symantec Enforcement Agent (SEA) is also upgraded. Host Integrity rules that are applied to the SEA client work properly. However, this client displays some untranslated key words and its security log is not formatted, because this client was not designed for localization. All functionality is present, however.

[2201086]

When the local user pauses a Host Integrity Compliance check, a different user cannot do a Host Integrity check using remote login

This behavior is as designed. A remote login by the same user as the one pausing the Host Integrity check works well. It is only the case of a different user that does not work.

[2169351]

Windows Symantec Network Access Control client shows Host Integrity as "passing" even though only a Mac Host Integrity rule is configured

This error appears when both Windows and Mac On-Demand clients are in the same group.

The workaround is to assign the clients to different groups for Host Integrity compliance checking purposes.

[2180255]

When there is no Host Integrity policy assigned to a group, the Symantec Endpoint Protection client behaves differently than the Symantec Network Access Control client or either On-Demand client

The clients all send "disabled" as their status to the Enforcer. The Enforcer treats this as "Host Integrity pass," and each type of client is approved. The exception is the Symantec Endpoint Protection client. It sends "disabled," and the Enforcer quarantines that type of client.

[2330894]

Client computers that are low on system resources may have Host Integrity failures

Client computers that are running low on RAM, disk space, Windows resources, and so on, frequently run slowly. In addition, those computers may have Host Integrity failures that do not provide "verbose" security log information.

To work around this problem, reduce the number of applications running, reduce the number of browser windows in use, and so on.

[2394506]

Client Host Integrity logs may show "cannot be authenticated"

In some cases, client computers may fail Host Integrity checks with the following error: "The most recent Host Integrity content has not completed a download or cannot be authenticated." This message appears in the **Security** log of the client and in the **Compliance > Host Compliance** log of Symantec Endpoint Protection Manager. When the client fails Host Integrity compliance checks, the usual result is that the client is quarantined until a subsequent compliance check is successful.

The usual cause of this Host Integrity failure is that the computer is restarted when in the middle of a Host Integrity check.

To confirm a client's Host Integrity status, run another Host Integrity compliance check. From Symantec Endpoint Protection Manager, follow the instructions under "Creating and testing a Host Integrity policy," in *Symantec™ Endpoint Protection Implementation Guide*. Examine the **Security** log for further details.

[2394715]

Documentation issues

This section includes information about product documentation.

The user documentation might be updated between product releases. You can locate the latest user documentation at the Symantec Technical Support Web site. The Support site provides individual articles and links that are designed to provide installation assistance, best practices, and FAQs.

See "[Where to get more information](#)" on page 10.

Symantec Endpoint Protection Integration Component documentation version 7.1 is not localized in some languages

The localized version of the *User Guide* is available in version 7.0 only for the following languages:

- Simplified Chinese

- Traditional Chinese
- Korean
- French
- Italian
- German
- Spanish
- Brazilian
- Russian
- Czech
- Polish

[2250404]

Cannot open Help or knowledge base articles

The default security settings of some operating systems block access to Symantec help and knowledge base articles. This problem may appear when you click links to other knowledge base articles. In some cases, those links fail with a Javascript permission error.

To work around this issue, add "symantec.com" (without the quotation marks) to your Trusted Sites security level.

[2052056]

Context-sensitive help for Client Install Settings > Basic Settings does not match the user interface

Under **Select an installation type**, one of the choices is **Unattended**. In the user interface, this appears as **Show progress bar only**. The result is the same as shown in the context-sensitive help: users do not interact with installation screens, but they see a Windows progress dialog box. **Show progress bar only** is the default setting.

[2384702]