Release Notes for Symantec™ Endpoint Protection and Symantec Network Access Control, version 12.1

Revision Date: Friday, April 29, 2011,
4:00 PM PDT

Release Notes: Getting started with Symantec Endpoint Protection and Symantec Network Access Control

This document includes the following topics:

About this document

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

- Symantec Endpoint Protection Enterprise Edition

- 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 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 11.0 product line. All functionality of version 11.0 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	The most significant improvements include the following policy features to provide better protection on the client computers. ■ The Virus and Spyware Protection policy detects threats more accurately while it reduces false positives and improves scan performance with the following technologies: ■ 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	Symantec Endpoint Protection Manager helps you manage the client computers more easily with the following new features: ■ 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	To increase the speed between the management server and the management console, database, and the client computers: ■ 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 Mac clients	In Symantec Enterprise Protection, you can configure the polices for Mac clients based on a location as well as a group. In Symantec Enterprise Protection Small Business Edition, you can now deploy and manage Mac clients on Symantec Endpoint Protection Manager for Symantec Endpoint Protection Small Business Edition.
Improved installation process	You can install the product faster and easier than before with the following new installation features: ■ 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	Symantec Endpoint Protection Manager now supports the following additional operating systems: ■ 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 Symantec Endpoint Protection Manager now supports the following Web browsers: ■ Internet Explorer 7.0, 8.0, 9.0 ■ Firefox 3.6, 4.0 The Symantec AntiVirus for Linux client now supports the following additional operating systems: ■ 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 For information about using the Symantec AntiVirus client on Linux, see the *Symantec AntiVirus for Linux Client Guide*.

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

Feature	Description
Better Enforcer management in Symantec Endpoint Protection Manager	You can manage the Enforcers more easily by configuring the following Enforcer settings in Symantec Endpoint Protection Manager: ■ Ability for the clients in an Enforcer group to synchronize their system time constantly by using the Network Time Protocol server. ■ Improvements for updating lists of MAC addresses: ■ 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: **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. **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. ■ 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.
New Network Access Control features in Symantec Endpoint Protection Manager	Symantec Endpoint Protection Manager includes the following additional functionality for Symantec Network Access Control: ■ 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	Symantec Network Access Control includes the following new features: ■ 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 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 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 Client Guide
This guide includes procedures for users to use and configure the Symantec Endpoint Protection or Symantec Network Access Control client.
This guide includes procedures for users to use and configure the Symantec Endpoint Protection client.

- *Symantec LiveUpdate Administrator User's Guide*
  This guide explains how to use the LiveUpdate Administrator. This guide is located in the `Tools\LiveUpdate` directory 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` directory 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 Online Help 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 Releases and updates Manuals and documentation updates Contact options	http://www.symantec.com/business/support/overview.jsp?pid=54619 http://www.symantec.com/business/support/overview.jsp?pid=52788 http://www.symantec.com/business/support/overview.jsp?pid=55357
Virus and other threat information and updates	http://www.symantec.com/business/security_response/index.jsp

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

Types of information	Web address
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:	Symantec Endpoint Protection Small Business Edition: http://www.symantec.com/connect/security/forums/endpoint-protection-small-business Symantec Endpoint Protection: http://www.symantec.com/connect/security/forums/network-access-control

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 Plan network architecture and review and purchase a license within 30 days of product installation	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. For information to help you plan medium to large-scale installations, see the Symantec white paper, Sizing and Scalability Recommendations for Symantec Endpoint Protection. Purchase a license within 30 days of product installation.
Step 2	Review system requirements	Make sure your computers comply with the minimum system requirements and that you understand the product licensing requirements.
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.

Table 1-3 Installation planning *(continued)*

Step	Action	Description
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	Install Symantec Endpoint Protection Manager. If the network that supports your business is small and located in one geographic location, you need to install only one Symantec Endpoint Protection Manager. If your network is geographically dispersed, you may need to install additional management servers for load balancing and bandwidth distribution purposes. If your network is very large, you can install additional sites with additional databases and configure them to share data with replication. To provide additional redundancy, you can install additional sites for failover support
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	Prepare for client installation as follows: ■ 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	Install the Symantec Endpoint Protection client on your endpoint computers. Symantec recommends that you also install the client on the computer that hosts Symantec Endpoint Protection Manager.
Step 10	Post-installation tasks	

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 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 11.x or 12.0 is already installed.

Table 1-4 Process for upgrading to the latest Enterprise edition release

Action	Description
Back up the database	Back up the database used by the Symantec Endpoint Protection Manager to ensure the integrity of your client information.
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.
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.
Stop the Symantec Endpoint Protection Manager service	You must stop the Symantec Endpoint Protection Manager service prior to installation.
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.
Turn on replication after the upgrade	Turn on replication when the installation is complete to restore your configuration.
Upgrade Symantec client software	Upgrade your client software to the latest version. 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. You can also update clients with LiveUpdate if you permit clients to run LiveUpdate and if the LiveUpdate Settings policy permits

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

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.
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	Upgrade your client software to the latest version. 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. You can also update clients with LiveUpdate if you permit clients to run LiveUpdate and if the LiveUpdate Settings policy permits

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.

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

Note: Links to Knowledge Base articles may not work at first. There is a lag between product release and these articles. Try again in a week or so.

See “Symantec Network Access Control issues” on page 36.

See "Symantec Endpoint Protection Small Business Edition issues" on page 39.

Symantec Protection Center and Symantec Endpoint Protection Manager Web console issues

This section contains information about Symantec Protection Center and the Symantec Endpoint Protection Manager Web console.

The Symantec Endpoint Protection Manager and the Active Directory/LDAP servers do not synchronize properly

You can use Symantec Protection Center to add an Active Directory/LDAP server and set it to synchronize automatically with the Symantec Endpoint Protection Manager. This operation currently fails.

[2295732]

Upgrades, installation, uninstallation, and repair issues

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

UPGRADES

Symantec Endpoint Protection sometimes fails to install on systems with `ExpanDrive.sys` installed

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

The workaround is to uninstall `ExpanDrive.sys`.

[2273586]

On-demand client download may not complete the first time

When downloading the on-demand client, the download dialog may disappear, and no client may be downloaded. This appears to be a timing issue.

The workaround is to attempt the download a second time. That will work.

[2357557]

AutoUpgrade of 5.x clients to Symantec Endpoint Protection version 12.1 requires adding 11.x packages to Symantec Endpoint Protection Manager

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, administrators must manually import 11.x packages to Symantec Endpoint Protection Manager.

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

[2359294]

Clients report "Out of Date" and reports show "Download Protection Content" as being out of date or not available

This is an error that shows up in upgrades only.

To work around this error, open the **Reports** page and run a select a relevant report, such as **Computer Status > Virus Definition Distribution**. That report should give you accurate information.

[2367250]

INSTALLATION ISSUES

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]

Incompatibility appears with Symantec Endpoint Protection Manager and Altiris Recovery Solution 7.0 SP1

When you install Symantec Endpoint Protection Manager, you may get "delayed write" error messages from Altiris Recovery Solution 7.0 SP1. These messages relate to the **Snapshot Volume,** and not to the actual remote storage drive. You can safely ignore this error.

This incompatibility is scheduled to be resolved before final release.

[2302501]

Symantec Endpoint Protection Manager may quarantine operating files for Symantec Mail Security for Microsoft Exchange

This quarantine essentially disables SMSMSE.

To work around this issue, you must "whitelist" the following two directories:

- C:\Program Files\Symantec\SMSMSE\6.0\Server\Temp
- C:\Program Files\Symantec\SMSMSE\6.0\Server\Quarantine

To whitelist folders from scans:

1. On the **Exceptions Policy** page, click **Exceptions...**
2. Under **Exceptions**, click **Add > Windows Exceptions > Folder**.
3. In the **File or Folder** text box, type the names of the two folders listed above.
4. For a folder exception, select the type of scan (**Security Risk**, **SONAR**, or **All**) next to **Specify the type of scan that excludes this folder**.

   Security Risk is the default, but you should specify **All**.
5. Click **OK**.

Windows sometimes crashes after installation of the client

This crash appears intermittently on computers running Windows 7.

[2312234]

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 may have effects in 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:

```
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 in installing Symantec Endpoint Protection client on computers with encrypted hard disks

The symptom is that the system 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.

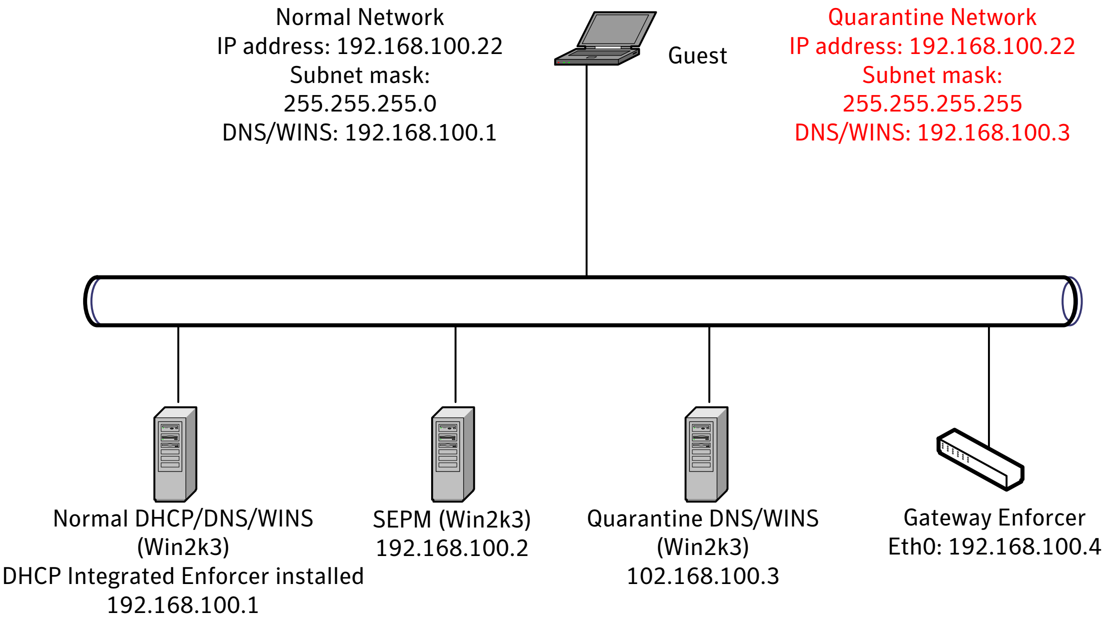
[2357592]

Setting up guest access challenge using the Symantec Network Access Control DHCP Integrated Enforcer

Guest Access and the DHCP Integrated Enforcer require a Gateway Enforcer and DNS server, because the DHCP Integrated Enforcer does not support DNS spoofing.

The first step towards enabling this solution is to set up a separate DNS server and Gateway Enforcer in the quarantine network. The guest endpoint receives a restricted and quarantined IP address with this DNS server. This quarantine DNS server resolves all DNS request to the Gateway Enforcer. The guest endpoint receiving the DNS resolution sends all HTTP request to the Gateway Enforcer. The Gateway Enforcer which then redirects the request to the on-demand Web server for download of the on-demand client. Once the download to the endpoint completes, Host Integrity checking runs and the result of this (configurable policy) outcome determines access for the endpoint. If the Host Integrity check passes, the endpoint is granted a normal IP address with the normal DNS server. If Host Integrity fails, the endpoint remains with a quarantined IP address with the quarantined DNS server.

Figure 1-1 Network diagram of DHCP Integrated Enforcer configured to prevent DNS spoofing



To configure the DHCP Integrated Enforcer

1 Configure the DHCP Integrated Enforcer to connect to your Symantec Endpoint Protection Manager.

2 Set up the DHCP Integrated Enforcer to use a secure subnet mast for quarantine IP addresses.

3 Configure the DHCP Integrated Enforcer to add static routes to quarantine IP addresses in the DHCP server. Static routes include DHCP server (192.168.100.1), DNS server (192.168.100.3), SEPM server (192.168.100.2), and Gateway Enforcer internal IP address (192.168.100.4)

4 Verify that static routes are added in the DHCP server. This is configured on the Enforcer console: click **Scope options** and ensure that **033 Static Route Option**"is checked for each route.

5 Add a DNS server. Right click on **Scope options**, and then click **Configure options...**.

6 On the **Advanced** tab, select **DHCP Standard Options** as the **Vendor class** and **Default User Class** as the **User class**.

7 In the **Available Options** scrolling box, click to select **006 DNS Servers**.

8. In the **IP address** fill-in box, add the normal DNS server IP address (**192.168.100.1**).
9. Click **Apply**.
10. Add a WINS server, using your usual procedures.
11. Configure quarantine IP address scope settings.
12. Right click on **Scope options**, and then click **Configure options...**.
13. On the **Advanced** tab, select **DHCP Standard Options** as the **Vendor class** and **SNAC_QUARANTINE** as the **User class**.
14. In the **Available Options** scrolling box, click to select **006 DNS Servers**.
15. In the **IP address** fill-in box, add the quarantine DNS server IP address (**192.168.100.3**).
16. Click **Apply**.
17. Add a quarantine WINS server, with the quarantine address of **192.168.100.3**.
18. Click **Apply**.

Next you set up the Gateway Enforcer.

To configure the Gateway Enforcer as a guest appliance

1. Connect **eth0** to the network and set the IP address to **192.168.100.4**.
2. Disconnect **eth1**.
3. Configure settings for configuration of Symantec Endpoint Protection Manager, using the command-line interface on the Gateway Enforcer:

   ```
   configure
   spm ip 192.168.100.2 key sygate group Gateway
   ```

4. Ensure that the Enforcer is connected to Symantec Endpoint Protection Manager, by issuing the `show status` command.
5. Enable on-demand, using the command-line interface:

   ```
   On-demand
   Spm-domain name <domain name>
   Client-group <client group full path>
   Enable
   Show
   ```

Next you set up a quarantine Windows DNS setup for HTTP redirect.

To set up a quarantine Windows DNS HTTP redirect

1. Open the DNS management console on the quarantine DNS server (192.168.100.3).
2. Right click **Forward Lookup Zones** and select **New Zone**. The **New Zone Wizard** appears.
3. In the **New Zone Wizard**, click **Next**.
4. Select **Primary zone**, and click **Next**.
5. Type a period (.) as the **Zone name**, and click **Next**.
6. Select **Create a new file with this file name**, type **root.dns**, and click **Next**.
7. Select **Do not allow dynamic updates**, and click **Next**.
8. Click **Finish**.

Create a new host under the **.(root)** zone that you just created.

To create a new host in the .(root) zone

1. Right click on the **.(root)** zone, and then select **New Host**.
2. Type an asterisk (*) as the **Name** and the Gateway Enforcer IP address (**192.168.100.4**) as the IP address for the new host.
3. Click **Add Host**.

Change the lookup IP address of the DNS server itself.

To change the IP address of the DNS server

1. Double click the DNS server name in the right panel.
2. Change the IP address to the Enforcer IP address (**192.168.100.4**), and click **OK**.

Optional: You may want to set up the WINS server to resolve in the same fashion as the DNS server. Computer names are resolved by the WINS server. If the endpoint is not registered to a domain, it resolves its computer name through WINS server. You may choose to set up a separate WINS server in quarantine to resolve all computer names in the internal network to the Gateway Enforcer **eth0** (**192.168.100.4**).

You should test your configuration.

To test your configuration

1 On the command prompt on the client computer, type

```
ipconfig /release
ipconfig /renew
```

The client should get a quarantine IP address with `255.255.255.255` as the subnet mask, and `192.168.100.3` as the DNS server

2 Clear the DNS cache. Type **ipconfig /flushdns**

3 Open a Web browser and type **www.yahoo.com**.

You should be redirected to the Gateway Enforcer on-demand Web site.

4 Download the on-demand client , and pass Host Integrity checks.

5 Your client is issued a normal IP address and `192.168.100.1` as the DNS server.

UNINSTALLATION

Uninstallation and reinstallation of the client fails in some cases

In some cases, if you uninstall the Symantec Endpoint Protection client and then attempt to reinstall it, that attempt fails.

To work around this issue, run Symantec CleanWipe after unstalling the client. Contact Symantec for instructions, and to upload your log files. We will provide a link to download CleanWipe and for instructions on its use. When you have finished with CleanWipe, installation of the client works properly.

[2305111]

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 changes from Internet Information Services (IIS) to Apache for web services. 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 further 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

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]

Migrating to Symantec Endpoint Protection 12.1 with Symantec Mail Security for Microsoft Exchange (SMSMSE) installed results in corrupted SMSMSE virus definitions

A fresh installation of SMSMSE and Symantec Endpoint Protection 12.1 works fine. However, in a migration case, there is a potential for corruption of SMSMSE virus definitions.

[2293552]

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.

Use the following steps to install the 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. On both the client and the server OS East Asian languages are installed. The language version of non-Unicode programs is set to English

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]

Right-click or drop-down menus may not be removed in the user interface

When you use Symantec Endpoint Protection Manager through a Web browser, right-click or drop-down menus may stay on screen after you finish with them.

To work around this problem, refresh your browser window.

[2290329]

The Quarantine Server is currently inoperative in Symantec Endpoint Protection 12.1

Symantec Endpoint Protection 12.1 does not currently work properly with the Quarantine Server. Users should not test this functionality.

[2293167]

Symantec Endpoint Protection add-in error sometimes appears when starting Microsoft Outlook

In some cases, an error appears when starting Outlook after the installation of Symantec Endpoint Protection.

To work around this issue, disable the add-in through your Outlook **Tools > Options** or **Tools > Trust Center** menus (depending upon your version).

[2315020]

Customers using PGP may experience problems with virus definitions loading correctly

This issue seems to be related to PGP's file shredding option. Symantec is investigating further

[2305817]

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]

Problems running `SylinkDrop.exe` tool

`SylinkDrop.exe` replaces the `Sylink.xml` file on the client. It should be capable of being run from any folder. Currently, that aspect of the tool fails.

To work around this defect, run `SylinkDrop.exe` from the installation folder, usually: `C:\Program Files\Symantec\Symantec Endpoint Protection\`*`Build version number`*`\bin`.

[2359100]

Potential conflicts exist with database maintenance jobs

Installing Symantec Endpoint Protection Manager with SQL database creates database maintenance tasks for the Symantec Endpoint Protection Manager database. If the database administrator already has created these tasks for all databases these tasks will conflict, resulting in a possible undesired outcome. Symantec recommends that if a database administrator already has these tasks created for all databases, the tasks should be disabled from 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, click to clear both of the following options:
   - **Truncate the database transaction logs**
   - **Rebuild Indexes**

Warning: If you perform these tasks in SQL Server Management Studio, uncheck these options in Symantec Endpoint Protection Manager and take similar steps in that product.

[2365974]

Symantec Endpoint Protection Manager policy issues

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

GENERAL POLICY ISSUES

This section describes general policy-related issues.

The use of local proxy auto-config (PAC) files to configure proxy servers fails

There is no workaround.

[2357933]

LIVEUPDATE POLICIES

This section includes the known issues information related to LiveUpdate policies.

Intelligent Updater fails to load new definitions

Intelligent Updater fails with the log message, “IU failed while deploying because a compatible product could not be found on the system. Please make sure that a compatible Symantec product is installed on the system.”

[2270179]

VIRUS AND SPYWARE PROTECTION POLICIES

This section includes the known issues information related to Antivirus and Antispyware policies.

Insight troubleshooting and proxy exclusions: additional information

f 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:

Trusted intranet option also applies to Insight Lookup

The "Automatically trust any file downloaded from an intranet website" option that appears in the Download Insight settings also applies to Insight Lookup. Even if you disable Download Insight and the option appears grayed out, Insight Lookup still uses the option if it is enabled.

[2246961]

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 1-6 Exclusions you should set to allow reputation traffic

Type of traffic	Server address
Ping submissions	`https://etavpgw.crsi.symantec.com:443`
Sample submissions	`https://etncogw.crsi.symantec.com:443` `https://etexpgw.crsi.symantec.com:443`
CAT submissions	`https://tus1gwynwapex01.symantec.com:443`
Error submissions	`https://etavpgw.crsi.symantec.com:443`
Insight reports	`https://ent-shasta-mr-clean.symantec.com:443`
Insight	`https://ent-shasta-rrs.symantec.com:443`

[2272505]

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. Move or minimize the browser window to view the alert message and click **OK** to terminate the browser.

[2279752]

Multi-threaded scans are not supported in Symantec Endpoint Protection v12.1

This feature was added in an earlier release, based on the use of a Registry key. Given the architectural changes in Symantec Endpoint Protection v12.1, that registry key approach no longer works. This feature is an enhancement that may appear in a future release.

The earlier Registry key locations, which should no longer be used:

- 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

This issue seems to be related to PGP's file shredding option. Symantec is investigating further

[2305817]

Scans catch threats, but do not submit them to Shared Insight Cache

Active scans catch threats and cache them locally, but do not submit them to the Shared Insight Cache.

[2321476]

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]

Shared Insight Cache port clarification

When setting the cache settings on the **Shared Insight Cache Settings** pane, the descriptions are very brief. What follows is a more detailed explanation of each port.

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.

NETWORK THREAT PROTECTION POLICIES

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

Network threat protection does not show Unicode supplementary characters properly

When application names are displayed in the **Network Threat Protection** dialog boxes, 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]

SQL Server failover clustering fails when Network Threat Protection is enabled

To work around this failure, disable Network Threat Protection.

[2302616]

Browser protection may fail on Windows 7 SP1 computers

Some components of browser protection may fail on computers running the Windows 7 SP1 operating system. This failure does not appear on computers running other operating systems.

[2302269]

Connections using Remote Desktop Protocol (RDP) may be blocked by a firewall rule

This defect appears in both new installations and migrations. The defect is related to a firewall rule that is set to "Block all other IP traffic and log."

To work around this defect, set this rule to "Allow."

[2323785]

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]

Some SONAR detections may falsely show Microsoft Windows as a risk

This detection is accurate, but labeling it as a Windows risk is not precise. Open the SONAR logs to see details on the actual detection.

[2312615]

Application browser does not launch when you click the "Browse" button in the "Search For Application" dialog box in when using Protection Center to access Symantec Endpoint Protection Manager

Application and Device Control policy protects a system's resources from applications and manages the peripheral devices that can attach to computers.One way that you can choose applications to watch is to browse for them. This feature is inoperative in the Protection Center view of Symantec Endpoint Protection Manager.

To use **Application and Device Control** browsing, 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. Client management of **Application and Device Control** rules will not stay enabled or disabled after the client restarts.

[2361600]

EXCEPTIONS POLICIES

This section describes the known issues related 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 issues warnings 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 Tamper Protection logs.

[2319187]

IPS policy exceptions are not working in the beta release

In the beta release, it is not possible to create IPS policy exceptions for Intrusion Prevention policies.

[2319186]

Symantec Endpoint Protection and Symantec Network Access Control Windows client issues

This section contains information about Symantec Endpoint Protection clients and Symantec Network Access Control clients on Windows computers.

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]

Registering a client to a group that is named with DBCS characters may fail when using the SylinkDrop tool

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.

Until this problem is resolved, Symantec recommends not using DBCS characters in group names.

[2273612]

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. Move or minimize the browser window to view the alert message and click **OK** to terminate the browser.

[2279752]

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]

Adding all features to a managed client that only has virus protection makes it become self managed

This defect appears when you create a package with the full suite of features and apply it to managed clients that are running virus protection only.

[2312242]

Registry Mechanic sometimes conflicts with the Symantec Endpoint Protection client

The conflict shows as a "hang" when starting the client.

To work around this problem, create an exception for Registry Mechanic in Application and Device Control.

[2312669]

Tray icon may not appear on clients with Limited User Accounts

In some cases, clients with Limited User Accounts may not see the tray icon. However, Symantec Endpoint Protection is still present and can be launched from the **Start** menu.

[2286505]

Client may not properly change location-based settings

Symantec Endpoint Protection is designed so that clients 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.

Multiple fail-safes exist to ensure that client communications remain unbroken. However, in some cases the client gets "stuck" in one location with one set of policies and communication settings.

To work around this problem, the administrator should "push" new policies to the client, possibly even using the SyLinkDrop tool.

[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.

The product team is aware of this issue and is working on a resolution.

[2350794]

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 issues

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

The Symantec Endpoint Encryption encrypted OS partition cannot be checked by Host Integrity in 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.

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

[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 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]

On-demand client download may not complete the first time

When downloading the on-demand client, the download dialog may disappear, and no client may be downloaded. This appears to be a timing issue.

The workaround is to attempt the download a second time. That will work.

[2357557]

HOST INTEGRITY POLICIES

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.

Security Compliance checking may be delayed while content downloads

The Security Compliance scan requires that Symantec Endpoint Protection download content from Symantec Endpoint Protection Manager. In some cases, this download may take a long time. To prevent inaccurate Security Compliance status messages, this scan 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 is that the Enforcer will report clients as having passed security compliance checks when 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 some untranslated key words and its security log is not formatted for 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, display 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 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 clients are in the same group.

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

[2180255]

Symantec Endpoint Protection Small Business Edition issues

The issues that follow are found only in Symantec Endpoint Protection Small Business Edition. For issues that relate to Symantec Endpoint Protection as a whole, see the rest of this document.

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 defect, do not install clients in a path that is defined with DBCS characters.

[2322728]

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 in some cases

The default security settings of some operating systems block access to Symantec help and Knowledge Base articles. This problem may appear when clicking links for more information. 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]