Release Notes for Symantec™ Endpoint Protection, Symantec Endpoint Protection Small Business Edition, and Symantec Network Access Control

Version 12.1, Release Update 1 MP1

Symantec

Symantec Endpoint Protection, Symantec Endpoint Protection Small Business Edition, and Symantec Network Access Control

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version: 12.1.1100 (RU1 MP1)

Updated: April 10, 2012

Release Notes for version 12.1, RU1, MP1

This document includes the following topics:

About Symantec Endpoint Protection

Symantec Endpoint Protection is a client-server solution that protects laptops, desktops, Windows and Mac computers, and servers in your network against malware. Symantec Endpoint Protection combines virus protection with advanced threat protection to proactively secure your computers against known and unknown threats.

Symantec Endpoint Protection protects against malware such as viruses, worms, Trojan horses, spyware, and adware. It provides protection against even the most sophisticated attacks that evade traditional security measures such as rootkits, zero-day attacks, and spyware that mutates. Providing low maintenance and high power, Symantec Endpoint Protection communicates over your network to

automatically safeguard computers against attacks for both physical systems and virtual systems.

This comprehensive solution protects confidential and valuable information by combining multiple layers of protection on a single integrated client. Symantec Endpoint Protection reduces management overhead, time, and cost by offering a single management console and the single client.

What's new in version 12.1 Release Update 1, MP1

Table 1-1 displays the new features in version 12.1 Release Update 1, MP1.

Table 1-1 New features in version 12.1.1100

Feature	Description
System requirements	■ Browser intrusion prevention in the Intrusion Prevention policy is compatible with Firefox 9 and Firefox 10. ■ The Quarantine server is supported on the Windows 64-bit operating system ■ Symantec Endpoint Protection Manager supports SQL Server 2012. See the knowledge base article, System Requirements for Symantec Endpoint Protection and Network Access Control 12.1 Release Update 1 (RU1) See the knowledge base article, System requirements for Symantec Endpoint Protection Small Business Edition 12.1 Release Update 1 (RU1)
Installation changes	The client installation package includes a new tool to automatically remove certain third-party security software before the Symantec Endpoint Protection client software is installed. In previous versions, you needed to uninstall third-party software separately before you deployed the client installation package. You can redeploy the client installation package with the new feature enabled. Click **Admin** > **Install Packages** > **Add Client Install Settings**. On the **Install Tab**, check **Automatically uninstall existing security software**. See "Uninstalling third-party security software from the client computer" on page 16. For a list of products that the tool uninstalls, see the following knowledge base article: About the Security Software Removal feature in Symantec Endpoint Protection 12.1 RU1
MAC Authentication Bypass (MAB) switch support	Symantec Network Access Control supports the following switches for MAB: ■ Cisco Catalyst Switch ■ Extreme Networks ■ Hewlett-Packard ProCurve Switch ■ Foundry Networks ■ 3Com

Table 1-1 New features in version 12.1.1100 *(continued)*

Feature	Description
Public support for remote monitoring applications	This release MP1 now includes the following built-in remote monitoring capabilities: ■ Improved logging to the Windows event log on the client. ■ New logging to the Windows event log on the server, to monitor license status and content status ■ New public opstate registry keys on the client. Includes registry keys that are moved from old locations and new registry keys to monitor content health and status on the client Documentation for remote monitoring support appears in the *Integration Guide for Remote Monitoring with Symantec Endpoint Protection*, located in the `/Tools/Integration/RemoteMonitoringGuide/` folder. Open Internet Explorer or Firefox and run `index.html`.

The Mac client is unchanged in this release.

Note for trialware users

For Symantec Endpoint Protection Trialware users, the download no longer contains the following folders:

- `\SEP`
- `\SEPx64`
- `\SEP_MAC`

The Symantec Endpoint Protection Manager administrator can export a Windows 32-bit, Windows 64-bit, and Mac client package.

Note: To create a 32-bit Windows client installation package without installing the Symantec Endpoint Protection Manager, go to the installation folder, which is usually `c:\Program Files\Symantec Endpoint Protection Manager\SEPM\Packages`. Copy `SAV32.dat` to `SAV32.zip`, and extract all from the `.zip` file to get an unmanaged client package. Run `Setup.exe` to install the unmanaged client. The 64-bit Windows client file name is `SAV64.dat`. The Mac client file name is `SEP_Mac.dat`.

Where to get more information about Symantec Endpoint Protection

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 Tools 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 Tools product disc.
- *Symantec Endpoint Protection Manager Database Schema Reference*
  This guide includes the database schema for 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 Tools 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	Symantec Endpoint Protection: http://www.symantec.com/business/support/overview.jsp?pid=54619 Symantec Endpoint Protection Small Business Edition: http://www.symantec.com/business/support/overview.jsp?pid=55357 Symantec Network Access Control: http://www.symantec.com/business/support/overview.jsp?pid=52788
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	Symantec Endpoint Protection: http://www.symantec.com/connect/security/forums/endpoint-protection-antivirus Symantec Endpoint Protection Small Business Edition: http://www.symantec.com/connect/security/forums/endpoint-protection-small-business Symantec Network Access Control: 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 and review and purchase a license	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 (Small Business Edition) or 60 days (full version) of product installation.
Step 2	Review system requirements	Make sure the computers on which you will install the client and management server software comply with the minimum system requirements. Understand the product licensing requirements. See the knowledge base article: System Requirements for Symantec Endpoint Protection and Network Access Control 12.1
Step 3	Prepare computers for installation	To install both management server and clients, you must be logged in with a Windows account that grants local administrator access. Uninstall other security software from your computers either by configuring your Symantec Endpoint Protection client install package to automatically uninstall it, or by manually uninstalling it. Some programs may have special uninstallation routines. See the documentation for the third-party software. Make sure administrator access to remote systems is available. Open firewalls (including ports and protocols) to allow remote deployment between the Symantec Endpoint Protection Manager and the endpoint computers.

Table 1-3 Installation planning *(continued)*

Step	Action	Description
Step 4	Prepare to install management server	You may wish to decide on the following before installation of the management server: ■ A password for your login to the management console ■ An email address where you can receive important notifications and reports ■ An encryption password, which may be needed depending on the options selected during installation If you decide to use a Microsoft SQL Server database, additional steps are required prior to installation. These include, but are not limited to, configuring or creating a database instance configured to use mixed mode or Windows authentication mode. You will also need to provide database server administration credentials in order to create the database and the database user. These will be specifically for use with the management server. You will also need to create a password for the database user, and a username if you do not want to accept the default. You should have this information available and configuration tasks completed before you begin installation of the management server.
Step 5	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 or load balancing support. Failover and load balancing can only be used with Microsoft SQL Server databases.
Step 6	Prepare and deploy client software	Determine which method would work best in your environment to deploy the client software to your computers. Install the Symantec Endpoint Protection client on your endpoint computers. **Note:** Symantec recommends that you also install the client on the computer that hosts Symantec Endpoint Protection Manager.

Table 1-3 Installation planning *(continued)*

Step	Action	Description
Step 7	Post-installation tasks	Verify that your client computers are online and protected. Become familiar with the features and functions of the Symantec Endpoint Protection management console and perform configuration and optimization tasks, including: ■ Create client groups and locations. ■ Adjust client policies and settings. ■ Configure exclusions to prevent applications and files from being scanned. ■ Check notifications. ■ Create additional administrator accounts. ■ Register your product serial number, and import your license file into the console. For the full version, if you have not implemented replication, you may deploy the same `.SLF` file to multiple management servers. The number of clients reporting to your management servers must not exceed the total number of licensed seats. You can also perform some of these steps prior to client deployment.

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

Upgrading to a new release of Symantec Endpoint Protection

You can upgrade to the newest release of the product to take advantage of new features. To install a new version of the software, you must perform certain tasks to ensure a successful upgrade or migration.

Before you upgrade, review the following information:

- System requirements
  See the knowledge base article: System Requirements for Symantec Endpoint Protection and Network Access Control 12.1
- New features in this version
  See "What's new in version 12.1 Release Update 1, MP1" on page 4.
- Feature changes between the previous version and the newest version of the client
- Compatible server upgrade paths

- Compatible Windows client upgrade paths
- Compatible Mac client migrations

Table 1-4 displays the steps you need to perform to upgrade to the latest version.

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 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 that Symantec Endpoint Protection Manager uses to ensure the integrity of your client information.
Step 2	Turn off replication	Turn off replication on all sites that are configured as replication partners to avoid 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 management server service before you install a newer version.
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.

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

Step	Action	Description
Step 7	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 displays the steps you need to perform to upgrade to the latest version of Symantec Endpoint Protection Small Business Edition.

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

Step	Action	Description
Step 1	Back up the database	Back up the database that Symantec Endpoint Protection Manager uses to ensure the integrity of your client information.
Step 2	Stop the Symantec Endpoint Protection Manager service	You must stop the management server service before you install a newer version.
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. 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**. **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

Known issues and workarounds

The issues in this section are new for Symantec Endpoint Protection version 12.1 RU1 MP1.

Please review this document in its entirety before you install 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 13.
- Known issues that apply only to Symantec Endpoint Protection Small Business Edition.
- Known issues that apply only to the full version of Symantec Endpoint Protection.
  See "Symantec Endpoint Protection full version issues" on page 16.
- 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 19.
- Known inaccurate information that is found only in the documentation for any one of the versions.
  See "Documentation issues" on page 20.

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

Preparing for and repairing duplicate client IDs for cloned clients

You can deploy multiple Windows clients by cloning a base image with a Symantec Endpoint Protection client. However, the cloned clients use identical client IDs. The Symantec Endpoint Protection Manager database records the cloned computers as the same client, and causes reporting and management problems.

To work around this issue, first read about how to clone a client in either a physical environment or virtual environment. If you have already cloned the client using an improperly prepared image, you can repair duplicate client IDs by using the RepairClonedImage.exe tool.

How to prepare a Symantec Endpoint Protection 12.1 client for cloning

How to repair duplicate IDs on cloned Symantec Endpoint Protection 12.1 clients

[2434179]

Symantec Endpoint Protection Manager issues

This section contains information about Symantec Endpoint Protection Manager.

Symantec Security Response links may be disabled

The Symantec Security Response links on the Symantec Endpoint Protection Manager management console home page cannot be used if a proxy is enabled. This is by design, as the proxy is disabled in the embedded browser.

[2727152]

Windows XP has policy deployment limitations on the number of concurrent users

When deploying policies to clients, be aware that Windows XP supports a limited number of concurrent users if the clients are in "push" mode. Use "pull" mode on Windows XP servers for up to 100 clients.

[2479503]

After you configure Symantec Endpoint Protection Manager to upload Symantec AntiVirus 10 logs, update the legacy log location

If you configure Symantec Endpoint Protection Manager to upload Symantec AntiVirus 10 logs, the management server saves these legacy logs in `C:/Program Files/Symantec/Symantec Endpoint Protection Manager/data/inbox/log/tex/legacy`. The management server saves Symantec Endpoint Protection 12.1 logs to `C:/data/inbox/log/tex/legacy`. If you either

previously upgraded from Symantec AntiVirus, or manually deleted the legacy log folder, the management server does not process the legacy logs.

To configure the management server to upload legacy logs, click **Home** > **Preferences**, and on the **Logs and Reports** tab, click **Upload Symantec AntiVirus version 10.x log files**.

To work around this issue, update the legacy log location.

To update the legacy log location

1. In the following folder, `C:\Program Files\Symantec\Symantec Endpoint Protection Manager\Php\Include\Resources`, backup `Reporter.php`.
2. Open `Reporter.php`, and change the `$upload_dir` path from:

   `C:/Program Files/Symantec/Symantec Endpoint Protection Manager/data/inbox/log/tex/legacy`

   to

   `C:/data/inbox/log/tex/legacy`
3. Save `Reporter.php`.

[2562849]

After you log on to a remote Symantec Endpoint Protection Manager console, a "Failed to connect to the server" error appears

If you install Symantec Endpoint Protection Manager behind a NAT firewall, and log on to the console remotely, the following error might appear: "Failed to connect to the server." After you click **OK**, the **Home**, **Monitors**, and **Reports** pages appear blank.

To work around this issue, add the TCP port 8445 to the VM configuration.

[2536390]

After you click the Test Account option to authenticate a directory server for an administrator account, an Account Authentication Failed error message appears

If your company uses Active Directory for directory authentication, you use the same user name and password for an administrator account in Symantec Endpoint Protection Manager as for the directory server. When the administrator logs on to the management server, the user name and password the administrator uses is authenticated by the directory server.

You can create an administrator account with an anonymous user name and password in case the directory server password changes. If the password changes, the administrator is never locked out of the management server. However, in

Windows 2003 Active Directory server, anonymous authentication is disabled by default. Therefore, when you add a directory server with an anonymous user name to an administrator account and click **Test Account**, an **Account Authentication Failed** error message appears. To access the **Test Account** option, click **Admin** > **Add an administrator** > **Authentication**.

To work around this issue, the administrator can still log on to the management server using a valid user name and password.

[2483802]

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.

INSTALLATION

This section discusses installation defects and possible solutions.

Uninstalling third-party security software from the client computer

You can automatically uninstall the third-party security software that is currently installed on your client computers. You add this feature to a client installation package.

To add this setting to a client installation package, do the following:

1. In the Symantec Endpoint Protection Manager console, click **Admin**. Then select **Install Packages > Client Install Settings > Add Client Install Settings . . .**
2. In the **Add Client Install Settings** dialog box, check **Automatically uninstall existing security software**.

Note: Carefully review the message that appears. To see which third-party applications are removed, see the knowledgebase article that is linked in the message. You can also read the article at the following location:

Third-party application removal

---

3. Select the other settings you want to use, name the package and enter a description as desired, and then click **OK**.

Note: Do not use this feature if you have multiple antivirus vendors installed on the same system.

[2597629] [2495281]

The permissible characters possible for the SQL Server database password are incorrect

The user documentation understates the permissible characters that can be used for the SQL Server database.

The correct list includes all of the following characters: `~`#$%^&-_=+\|:"<>.'/.`

[2365060]

UPGRADES

MIGRATION

This section contains information about migration.

Symantec Endpoint Protection Manager 12.1 Release Update 2 (RU2) to drop support for SQL Server 2000 and SQL Server 2005 SP1-SP3

You should plan to migrate your SQL Server databases to new versions before that release.

[2642407]

Symantec Endpoint Protection Manager policy issues

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

APPLICATION AND DEVICE CONTROL POLICIES

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

The default rule Stop software installers [AC8] in the Application and Device Control policy does not correctly block write and delete access to *.exe files

If you enable the default rule **Stop software installers [AC8]**, the Application and Device Control policy incorrectly allows users to copy certain executables to their client computers.

To work around this issue, add the process `%windir%\system32\dllhost.exe` to the exclusion list of the rule that allows `svchost.exe`.

To add the process

1. In the Application and Device Control policy, check **Stop software installers [AC8]**, and then click **Edit**.
2. Under **Apply this rule to the following processes**, click **Add**.
3. Under **Process name to match**, type **%windir%\system32\dllhost.exe**, and then click **OK**.

[2518607]

VIRUS AND SPYWARE PROTECTION POLICIES

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

A new checkbox to block security risks from being installed is present on the client

Beginning with Symantec Endpoint Protection version 11.0 RU7, including Symantec Endpoint Protection version 12.x, there is a new checkbox on the client. On the client, click **Change Settings**, and next to **Virus and Spyware Protection**, click **Configure Settings**. On the **Auto-Protect** tab, click **Advanced**. Under **Other** options, click **Delete newly created security risk files if the action is "leave alone (log only)"**.

When you click this check box, Symantec Endpoint Protection automatically deletes the newly created or saved files that are security risks.

[2386164]

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.

After you upgrade the Mac client from version 12.1 to 12.1 RU1, restart the Mac client computer

If you upgraded the Mac client from version 12.1 to version 12.1 RU1, the Mac client might display two virus scan messages. This issue occurs after the end user plugs in a hard disk drive and the mount scan starts. The issue is caused because two instances of certain Mac OS X processes are running in the background.

To work around this issue, restart the Mac client computer.

[2566901]

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 19.
- Host Integrity and security compliance issues
  See "Host Integrity issues" on page 20.

Enforcer issues

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

Windows On-Demand clients do not have a persistence option

The persistence option is only applicable for Mac On-Demand clients.

For details, see the following KB article:

Persistent feature for On-Demand clients

[2689458]

MAC Authentication Bypass (MAB) and the LAN Enforcer: missing details in the documentation

When a LAN Enforcer appliance receives a MAB request, it looks up the address in the local MAB database first. If the entry is located in the local MAB database, the LAN Enforcer appliance authenticates the client based on 802.1x-aware switch

model. If an entry cannot be located in the local MAB database, the LAN Enforcer appliance then tries to connect to any available LDAP server. If an LDAP server is not available to authenticate a client's MAC address or a client's MAC address is not available in the database of the LDAP server, the LAN Enforcer appliance then tries to connect to any available RADIUS server. After the LAN Enforcer appliance receives the authentication result, it then sends a message to the RADIUS server to accept or reject the packet. The LAN Enforcer appliance then completes the authentication session.

[2481906]

Imported trusted MAC addresses do not appear in an exported group properties file

In the Symantec Endpoint Protection Manager console, you can import a list of MAC addresses for trusted hosts for an Integrated Enforcer. If you export the list in a group properties file and re-import the file to a second management server, the MAC addresses do not appear.

To work around this issue, first export the group properties file without the MAC addresses and import the file to the second management server. To export the group properties file, click **Admin** > **Servers** > **Export group properties**. Then, import the MAC addresses on the second management server by using the **Advanced** tab for the Integrated Enforcer.

[2403371]

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.

Tamper Protection detects and blocks running `SepLiveUpdate.exe` when it is executed by a Host Integrity policy

If you create a Host Integrity policy that detects old virus definitions, it runs `SepLiveUpdate.exe` to update those definitions. Currently that operation fails because Tamper Protection blocks `SepLiveUpdate.exe`. Symantec recommends against using this form of remediation in your Host Integrity policies.

[2663653]

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 about Symantec Endpoint Protection" on page 6.

Correction: MAC Authentication Bypass (MAB) supports Host Integrity

Earlier documentation stated incorrectly that MAB does not support Host Integrity. That is incorrect. MAB does support Host Integrity.

[2481906]

Trusted Web Domain Exception help mistakenly omits FTP

The description for this help topic should read as follows:

You specify a URL or host name or IP address when you specify a trusted Web domain exception. HTTPS URLs are not supported. You must create individual exceptions for files or applications that users might download from a site using an HTTPS URL.

[2678063]

Information is incorrect in "About the types of Auto-Protect"

The topic "About the types of Auto-Protect" incorrectly states the version of Lotus Notes that Auto-Protect supports. Symantec Endpoint Protection supports Lotus Notes versions 4.5 through 8.x.

[2657360]

Submissions topic contains incorrect reference to percentages

The topic "About submissions throttling" contains incorrect information about the percentages of computers that are allowed to send submissions. Previous versions of Symantec Endpoint Protection Manager let you configure a percentage of computers that are allowed to submit information to Symantec. The option is removed.

[2616828]

Incorrect information in the topic, "Monitoring protection with reports and logs"

The documentation on viewing logs states that you can clear the infected status of computers from the log on computer status. This function is no longer available.

[2674042]

Path for viewing the Access log is incorrect

The topic, "Enabling and viewing the Access log to check whether the client connects to the management server," in the *Symantec™ Endpoint Protection and Symantec Network Access Control Implementation Guide* provides the wrong path.

In the task, "To view the Apache HTTP server Access log," the path to the Access log is:

Drive:\Program Files\Symantec\Symantec Endpoint Protection Manager\apache\logs\access.log, and not *Drive*:\Program Files\Symantec\Symantec Endpoint Protection Manager\apache\access.log.

Links to "About commands you can run on client computers" are incorrect in the documentation

There are numerous links to the topic "About commands you can run on client computers" that are incorrectly linked. In the PDF of the *Symantec Endpoint Protection and Symantec Network Access Control Implementation Guide*, the links should go to the online help. Search for "commands client" and choose the second topic.

[2365306]

Legal Notice

Copyright © 2012 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, Bloodhound, Confidence Online, Digital Immune System, LiveUpdate, Norton, Sygate, and TruScan are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation

or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com