Symantec AntiVirus™ Corporate Edition Patch Update

Symantec AntiVirus Corporate Edition Update

Documentation version 10.0.1.1007

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.

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
http://www.symantec.com

Contents

Chapter 1

What's new in Symantec AntiVirus

This chapter includes the following topics:

About this patch

This Symantec AntiVirus patch contains enhanced handling for security risks. These changes are largely transparent to the user. This patch also allows you to upgrade your existing Symantec AntiVirus 10.0.1.1000 clients and servers with these new capabilities without having to install a full build.

Auto-Protect blocking of security risks

A Block Security Risks checkbox has been added to Auto-Protect in Symantec AntiVirus to control the time at which Auto-Protect reacts to certain security risks. In cases where blocking security risks will not affect the stability of a computer, Auto-Protect can be configured to block the risks. If Symantec determines that blocking a security risk could compromise a computer's stability, then Auto-Protect allows the risk to install and immediately takes the action that is configured for the risk, regardless of whether the Block Security Risks checkbox is enabled.

When you enable Block Security Risks, the action that is set for a security risk's category takes precedence over the action that is set for the individual security risk. For example, if the adware category is set to Log only, then this feature is disabled for all instances of adware, even if you have configured an exception so that a specific piece of adware is to be quarantined.

If you disable Block Security Risks, Auto-Protect detects the security risks after they are installed or run, and handles them using the actions you have configured. Events are logged regardless of whether Block Security Risks is enabled or disabled.

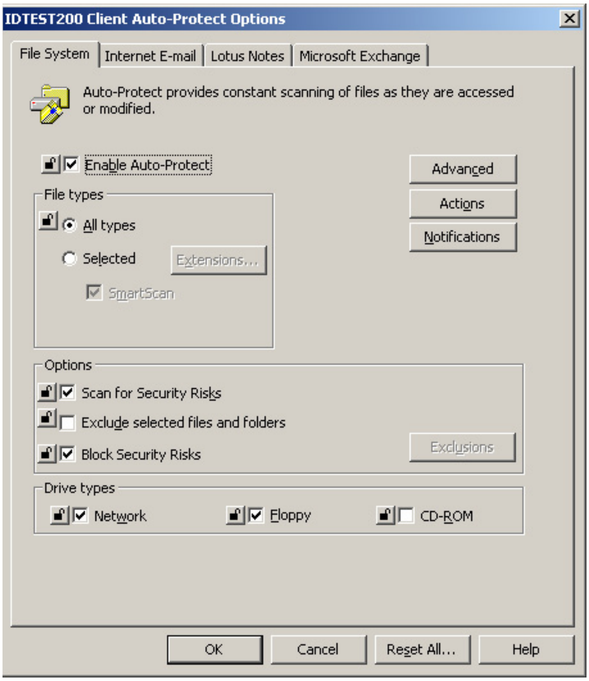
Block Security Risks can be enabled in the following locations:

- the Client Auto-Protect Options dialog box in the Symantec System Center™
- the Server Auto-Protect Options dialog box in the Symantec System Center
- the Symantec AntiVirus File System Auto-Protect dialog box in the Symantec AntiVirus user interface

Administrators can lock Block Security Risks from the Symantec System Center.

Figure 1-1 shows where you set Block Security Risks and Scan for Security Risks in the Client Auto-Protect dialog box in the Symantec System Center.

Figure 1-1 Block Security Risks location



IDTEST200 Client Auto-Protect Options

File System | Internet E-mail | Lotus Notes | Microsoft Exchange

Auto-Protect provides constant scanning of files as they are accessed or modified.

☑ Enable Auto-Protect

File types

● All types

○ Selected

☑ SmartScan

Options

☑ Scan for Security Risks

□ Exclude selected files and folders

☑ Block Security Risks

Drive types

☑ Network ☑ Floppy □ CD-ROM

Note: If Scan for Security Risks is disabled, the checkbox for Block Security Risks can still be checked, but the Block Security Risks setting is ignored until Scan for Security Risks is reenabled.

Security risk repair after restarts

Symantec AntiVirus is able to perform additional repairs after a system restart.

In some cases, Symantec AntiVirus cannot repair all the changes that are made by a security risk until you restart the computer. Some of the possible reasons include the following:

- The repair involves running processes that cannot be terminated, causing their binaries to be locked on the disk.
- The risk has files open for exclusive read, write, or delete privileges that cannot be deleted without a restart.
- The repair affects a Layered Service Provider.

Symantec AntiVirus notifies the user that a restart is necessary through the scan results window, if the user interface is enabled for that scan. Users may either restart immediately or postpone the restart until it is convenient.

Results of the repairs are logged to the Event log. Users can see the results of the repairs in the scan status window or the Risk History window and can right-click risks to see repair details.

Note: The repair will not be complete until after the restart.

Layered Service Provider repairs

Symantec AntiVirus can repair the effects of security risks that affect a Layered Service Provider (LSP) when that LSP cannot be removed from a chain of services without breaking a service until a restart occurs. For example, removing an LSP might break network connectivity and require a second restart to restore network access.

An LSP is a system driver that is typically integrated directly into the TCP/IP layer and manipulates the data that is transmitted in some way. For example, an LSP could be use to encrypt the data.

Users can see the results in the scan status window or the Risk History window, and can right-click risks to see repair details.

Hosts file repairs

Symantec AntiVirus can detect and repair security risk modifications to hosts files, which are used to map host names to IP addresses.

Hosts files may be used maliciously by virus and other security risk authors. For example, entries in the hosts file can be used to block users from visiting virus removal Web sites or to redirect the user to a counterfeit or malicious Web site.

The results of hosts file repairs are logged to the Event log. Users can see the results in the scan status window or the Risk History window, and can right-click risks to see repair details.

Directory remediation

Symantec AntiVirus detects and removes folders that are placed on your computer by security risks. If the configured action for the risk is Delete or Quarantine and the folder is empty, Symantec AntiVirus removes the folder automatically. If directory remediation is needed in the repair of a risk, users can right-click the risk to see that in the risk details.

Chapter 2

Applying the Symantec AntiVirus patch

This chapter includes the following topics:

About applying the patch

The Symantec AntiVirus patch lets you upgrade your Symantec AntiVirus clients and servers while preserving their configuration settings. Because of the complexity and size of Symantec AntiVirus software, applying a patch provides a quicker, less costly, and more efficient method by which to upgrade your clients and servers.

You can use standard installation methods to apply the Symantec AntiVirus patch, including local, network, Active Directory, or third-party tools. You can also patch Symantec AntiVirus clients and servers with an updated version of the ClientRemote Install Utility, which you must download to the computer from which you plan to roll out the patch to your clients and servers.

For more information on installing the Symantec AntiVirus patch using local, network, Active Directory, or third party tools methods, see the *Symantec AntiVirus Installation Guide*.

Warning: You can not uninstall the Symantec AntiVirus patch once it is installed on your clients and servers. If you need to remove the patch, you must first uninstall the Symantec AntiVirus client or server, then reinstall the previous Symantec software that does not contain the patch. To avoid this scenario, before you deploy the Symantec AntiVirus patch, you should install the patch in a test environment and ensure that the patch does not interfere with the normal operation of your computers and network.

Downloading the Symantec AntiVirus patch and ClientRemote Install Utility

You can download the Symantec AntiVirus patch from a designated FTP Web site. The Symantec AntiVirus patch is compressed into a ZIP file along with an updated version of the ClientRemote Install Utility. The updated ClientRemote Install Utility lets you deploy the patch to multiple computers at the same time.

To download the Symantec AntiVirus patch and ClientRemote Install Utility

1. Open the designated FTP Web site and locate the ZIP file that contains the Symantec AntiVirus patch that you want to install on your network.
2. Save the ZIP file to a local drive on your computer.
3. Uncompress the ZIP file using WinZip or a similar file compression utility.
4. If you plan on using the ClientRemote Install Utility from the Symantec System Center, copy the following files to c:\Program Files\Symantec\Symantec System Center\Deployment\ClientRemoteInstallation\
   - clientremote.exe
   - vpremote.exe
   - vpremote.dat
   - .msp patch file

   If the file already exists in the new location, replace the original file with the newly downloaded files.

Deploying the patch using the ClientRemote Install Utility

The ClientRemote Install Utility lets you remotely deploy an MSI patch to Symantec AntiVirus clients and servers in your network from the Symantec System Center console or as a standalone tool. An advantage to remotely patching clients and servers is that users do not need to log on to their computers as administrators prior to the installation. You can patch multiple computers at the same time without having to visit each computer individually.

Note: To remotely deploy the Symantec AntiVirus patch, you must have administrator rights to the domain to which the computers that you want to patch belong.

The Symantec AntiVirus patch consists of the following files:

MSI patch (.msp)	Contains the new features and security enhancements that are installed over the existing Symantec AntiVirus clients and servers.
Vpremote.dat	Contains the commands for the specific MSI patch that the ClientRemote Install Utility uses for patch deployment. If you change the MSI patch file name, you must edit vpremote.dat to reflect this change in the command line.

The Symantec AntiVirus patch is copied to the target computers that you select. You can not specify where the patch is downloaded. The default location is the c:\temp folder. The patch upgrades only the target computers that have the correct Symantec AntiVirus client and server versions installed.

The ClientRemote Install Utility Status window displays the download progress of the Symantec AntiVirus patch to the target computers. You can verify that the patch is successfully installed on your clients and servers from the Symantec System Center by checking that the Symantec AntiVirus version information is updated.

Note: You must install the Symantec AntiVirus server from the CD Start menu to deploy Symantec AntiVirus clients using the ClientRemote Install Utility. If you install Symantec AntiVirus server from the SAV folder in the CD, you cannot use this utility.

Starting the patch deployment

You can patch Symantec AntiVirus clients and servers using the ClientRemote Install Utility as a standalone tool, or from the Symantec System Center.

Note: Windows XP Service Packs 1 and 2 include firewalls that can interfere with Symantec AntiVirus installation communications between servers and clients. If any of your Symantec AntiVirus clients and servers run Windows XP, you must disable the Windows XP firewall on them before you install the client and server software.

To start the patch deployment from the standalone tool

1. Navigate to and double-click the newly downloaded version of **clientremote.exe**.
2. Continue the patch deployment.
   See "Running the ClientRemote Install Utility" on page 14.

To start the patch deployment from the Symantec System Center

1. In the Symantec System Center console, in the left pane, do one of the following:
   - Click **System Hierarchy**.
   - Under System Hierarchy, select any object.
2. On the Tools menu, click **ClientRemote Install**.
   Make sure that you updated the files in the ClientRemote Installation folder.
   See "Downloading the Symantec AntiVirus patch and ClientRemote Install Utility" on page 12.
3. Continue the installation.
   See "Running the ClientRemote Install Utility" on page 14.

Running the ClientRemote Install Utility

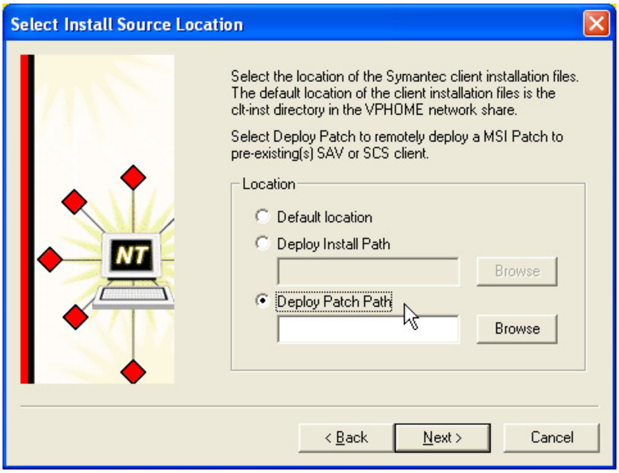
The ClientRemote Install Utility program runs after you start the patch deployment process.

See "Starting the patch deployment" on page 14.

When you use the ClientRemote Install Utility, in the Select Install Source Location dialog box, you can select to deploy either a full product installation or a patch. When you select the Deploy Patch Path, you must browse to the MSI patch file (.msp) that you want to deploy to the Symantec AntiVirus clients and servers in your network.

To run the ClientRemote Install Utility

1 In the ClientRemote Install Utility Welcome panel, click **Next**.



Select Install Source Location

Select the location of the Symantec client installation files. The default location of the client installation files is the clt-inst directory in the VPHOME network share.

Select Deploy Patch to remotely deploy a MSI Patch to pre-existing(s) SAV or SCS client.

Location

○ Default location

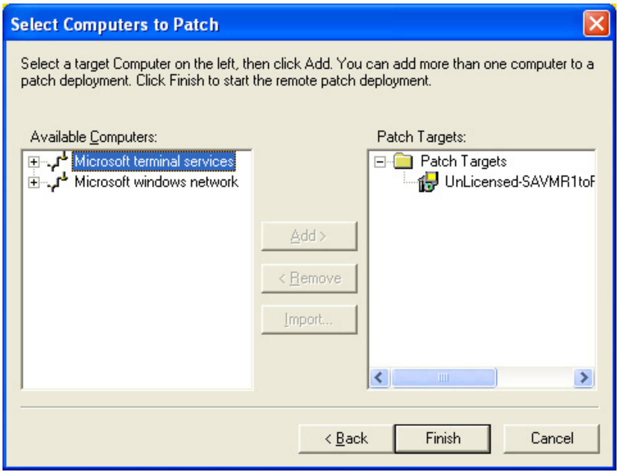
○ Deploy Install Path

● Deploy Patch Path

2 In the Select Install Source Location panel, select **Deploy Patch Path**, and then click **Browse**.

3 In the Open dialog box, select the MSI patch that you want to use to update your clients and servers, and then click **Open**.
Verify that the appropriate vpremote.dat is saved to the same folder as the MSI patch.

4 In the Select Install Source Location panel, click **Next**.



Select Computers to Patch

Select a target Computer on the left, then click Add. You can add more than one computer to a patch deployment. Click Finish to start the remote patch deployment.

Available Computers:

- Microsoft terminal services
- Microsoft windows network

Patch Targets:

- Patch Targets
  - UnLicensed-SAVMR1toF

5 In the Select Computers to Patch panel, under Patch Targets, select the patch that you want to use to update your clients and servers.

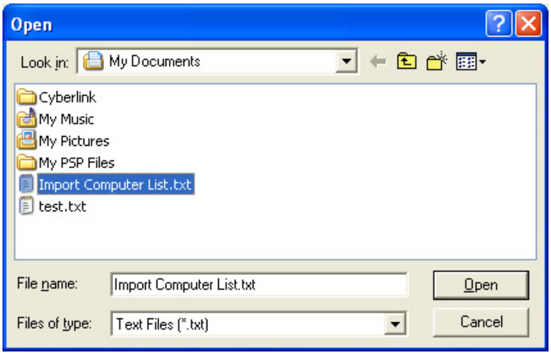
6 Do one of the following:

- If you created a text file that contains IP addresses to import computers, continue to step 7.
- If you did not create a text file that contains IP addresses, continue to step 11.

You can create a text file using Notepad, and then type the IP addresses that you want to import on separate lines in the file.

For more information on creating a text file with IP addresses to import, see the *Symantec AntiVirus Installation Guide*.

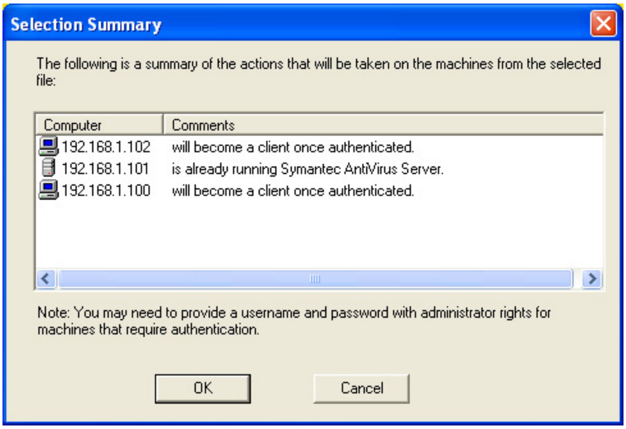
7 To import the list of computers, click **Import**.



File name: Import Computer List.txt

Files of type: Text Files (*.txt)

8 Locate and double-click the text file that contains the computer names.



The following is a summary of the actions that will be taken on the machines from the selected file:

Computer	Comments
192.168.1.102	will become a client once authenticated.
192.168.1.101	is already running Symantec AntiVirus Server.
192.168.1.100	will become a client once authenticated.

Note: You may need to provide a username and password with administrator rights for machines that require authentication.

During the authentication process, you may need to provide a user name and password for computers that require authentication.

9 In the Selection Summary dialog box, click **OK**.
During the authentication process, Setup checks for error conditions. You are prompted to view this information interactively on an individual computer basis or to write the information to a log file for later viewing.
If you create a log file, it is located under C:\Winnt\Savcecln.txt.

10 Select one of the following:

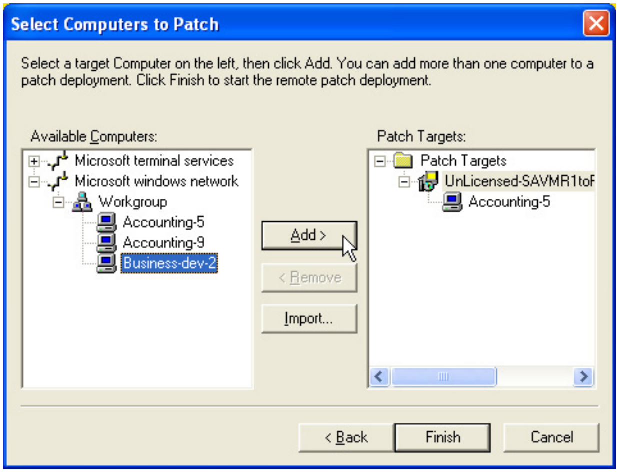
Yes	Display the information.
No	Write to a log file.

11 Do one of the following:

- If you have more computers to add individually, continue to step 12.
- If you do not have more computers to add individually, continue to step 15.

12 Under Available Computers, expand **Microsoft windows network**, and then select a computer.

13 Click **Add**.



Select a target Computer on the left, then click Add. You can add more than one computer to a patch deployment. Click Finish to start the remote patch deployment.

14 Repeat steps 6 and 7 until all of the computers that you want to patch are added.

15 In the Select Computers to Patch panel, click **Finish**.

16 In the Status of Remote Client Installations window, click **Done**.
Target computers may need to be rebooted after the patch installation.