Symantec™ Endpoint Protection Getting Started Guide

12167130

Symantec™ Endpoint Protection Getting Started Guide

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 11.00.00.00.00

PN: 12167130

Legal Notice

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
20330 Stevens Creek Blvd.
Cupertino, CA 95014

http://www.symantec.com

Getting Started

This document includes the following topics:

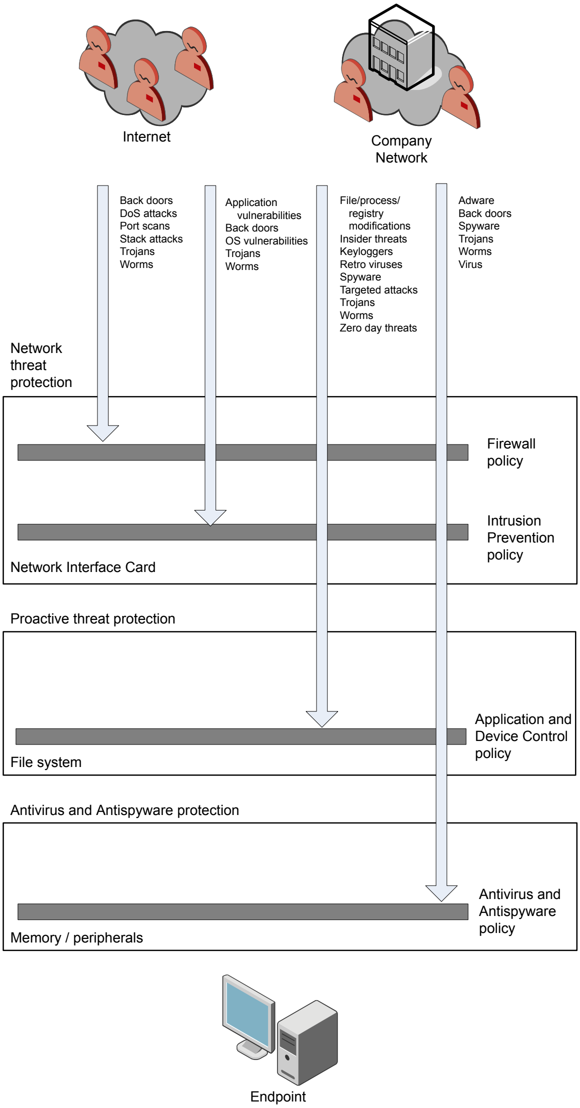
About Symantec Endpoint Protection

Symantec Endpoint Protection is the next-generation product that replaces specific versions of the following products:

- Symantec AntiVirus Corporate Edition
- Symantec Client Security
- Symantec Sygate Enterprise Protection
- Sygate Secure Enterprise
- Symantec WholeSecurity Confidence Online for Corporate PCs

Symantec Endpoint Protection provides advanced threat protection that protects your endpoints (laptops, desktops, and servers) from both known threats and those threats that have not been seen before. 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. Symantec Endpoint Protection provides multiple layers of protection for your endpoint computing devices.

Figure 1-1 Multiple protection layers



Symantec Network Access Control, which is purchased separately, is a companion product to Symantec Endpoint Protection. Symantec Network Access Control ensures that clients are compliant with your organization's security policies before they are allowed access to your network.

What's included with Symantec Endpoint Protection

Symantec Endpoint Protection includes the following core components:

- The Symantec Endpoint Protection client is installed on the endpoints that you want to protect. It combines antivirus, antispyware, firewall, intrusion prevention system, application control, device control, and proactive threat scanning (using Symantec SONAR technology) into a single client.

  It also contains Symantec Network Access Control, which remains dormant until activated. No redeployment of clients is needed to add Symantec Network Access Control to a network where Symantec Endpoint Protection is installed. An update to the Symantec Endpoint Protection Manager activates those features on the clients.
- Symantec Endpoint Protection Manager is installed on a computer that you want to host the management server software. Symantec Endpoint Protection Manager communicates with the Symantec Endpoint Protection clients and is configured through the Symantec Endpoint Protection Manager Console.
- Symantec Endpoint Protection Manager Console lets you centrally manage the Symantec Endpoint Protection clients. From the console you can install clients, set and enforce a security policy, and monitor and report on the clients. The console can be run from the computer hosting Symantec Endpoint Protection Manager or remotely through a Web-based interface.

Larger companies may want to install the following optional components to centralize resources within the corporate network:

- The LiveUpdate Server, also known as Central LiveUpdate Server, obtains security and product updates from Symantec and acts as a repository for those updates. Symantec Endpoint Protection Manager and Symantec Endpoint Protection clients can be configured to retrieve updates from this LiveUpdate Server.
- The Central Quarantine receives suspicious files and unrepaired infected items from the Symantec Endpoint Protection clients. Central Quarantine forwards a sample to Symantec Security Response, which analyzes the sample and if a threat is new, produces security updates.

Organizations that install Symantec Network Access Control may also want to install the hardware appliance, the Symantec Enforcer. The Enforcer works with Symantec Network Access Control clients to regulate their access to your network.

What's new in this version

Symantec Endpoint Protection combines technologies from previous Symantec products in a new interface.

Symantec Endpoint Protection provides the following features:

- Essential threat protection technologies are combined into a single Symantec Endpoint Protection client:
  - Antivirus and Antispyware Protection adds rootkit detection and removal and has an improved resource footprint.
  - Network Threat Protection provides new rules-based firewall and Generic Exploit Blocking (GEB) that blocks malware before it can enter the computer. This feature provides protection that is based on signatures and protection against buffer overflows.
  - Proactive Threat Protection adds protection for zero-day attack threats without relying on signatures.
  - Administrators can customize the interface to control what configuration options are available to the end user and can completely hide the interface.
- Symantec Endpoint Protection is Symantec Network Access Control-ready with the purchase of Symantec Network Access Control.
- The redesigned management console can be used to:
  - Manage both Symantec Endpoint Protection and Symantec Network Access Control. You can manage all security technologies from a single console.
  - Monitor and report on security threats and system response from a central point.
  - Allow different administrators to access different levels of the management system based on their roles and responsibilities.

Administrators for legacy Symantec AntiVirus Corporate Edition and Symantec Client Security products should see the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control* for information on what has changed for these administrators.

Planning for installation

You must read the migration information in the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control* if you have any of the following products installed on your network:

- Symantec AntiVirus

- Symantec Client Security
- Symantec Sygate Enterprise Protection

The *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control* can be found in the Documentation folder on your product CD.

If this installation is a new installation, you should read the first three chapters in the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control* before beginning installation. The larger and more complex your network, the more important it is to read the documentation.

To aid in planning, you should identify the following hardware and software components:

- The types of hardware, operating systems, and applications for the computers on which you intend to run the Symantec Endpoint Protection client.
- All custom or other non-commercially available applications that are used in your production network. You should plan to test all key features of these applications in your test environment.
- Any existing endpoint security software that runs on your network, such as desktop firewalls or antivirus software.

Plan to create a test environment. The test environment should be isolated from your production network. Make sure that the test environment contains computers that are representative of the computers on your production network.

Companies without the resources to create a test environment should first install the Symantec Endpoint Protection client to only a few computers on the production network. The computers that you select should have hardware, operating systems, and applications that adequately represent your production network. These computers should not be mission-critical to the company.

Use the *Client Guide for Symantec Endpoint Protection and Symantec Network Access Control* to become familiar with how the software works on the test computers that run the Symantec Endpoint Protection client.

Installation overview

The *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control* contains detailed information about each step in the installation process.

Table 1-1 describes the high-level steps you take to install Symantec Endpoint Protection.

Table 1-1 Installation steps

Step	Action	Description
1	Install Symantec Endpoint Protection Manager	Decide on the computer to which you want to install the software and the type of database that you want to use. Then, run the installation program from the CD. The program first installs the manager software. It then installs and configures the database.
2	Create a client install package	For your test environment you can create and install default client software packages. Those clients are assigned to the Temporary group and use the default policies. If there are a large number of computers in your production environment, you may want to create custom security policies first. You can then create custom client installation packages before deploying to the clients. At the end of the database configuration, you are asked if you want to run the Migration and Deployment Wizard. This wizard creates and then pushes out a default client software installation package.
3	Deploy the client software	Decide how you want to deploy the client software. You can deploy the client software in several different ways. For ease of use, you can use the Migration and Deployment Wizard after you install the manager to deploy the default protection. Alternately, you can use the Migration and Deployment Wizard from the Start menu at any time.
4	Log on to Symantec Endpoint Protection Manager console	To log on, you can use the Start menu and the admin user name, with the password that you set during installation.
5	Locate your group in the console	On the Admin page, you can click Servers to see the group that you created during installation.
6	Configure LiveUpdate for site updates	You need to configure LiveUpdate properties for the site you have installed.
7	Configure LiveUpdate for client updates	After you configure the site, you need to configure a LiveUpdate Settings Policy and a LiveUpdate Content Policy for your clients.

Table 1-1 Installation steps *(continued)*

Step	Action	Description
8	Configure security policies and test Symantec Endpoint Protection	At a minimum, you should configure and test an Antivirus and Antispyware Policy for your clients. You may also want to configure a Firewall Policy and policies for the other types of protection.

About system installation requirements

Symantec software requires specific protocols, operating systems and service packs, software, and hardware. All the computers to which you install Symantec software should meet or exceed the recommended system requirements for the operating system that is used.

This document contains only minimal information about system requirements. This information may be sufficient to install to a small network or test network. You should refer to the full system requirements before you install the product on a more complex network.

See the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control* for more information.

Installing for the first time

These installation instructions apply only to a new, first-time installation.

You must perform a migration if you have installed on your network a migration-supported version of the following products:

- Symantec AntiVirus Corporate Edition
- Symantec Client Security
- Symantec Sygate Enterprise Protection
- Sygate Secure Enterprise

For information on migration, see the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control.*

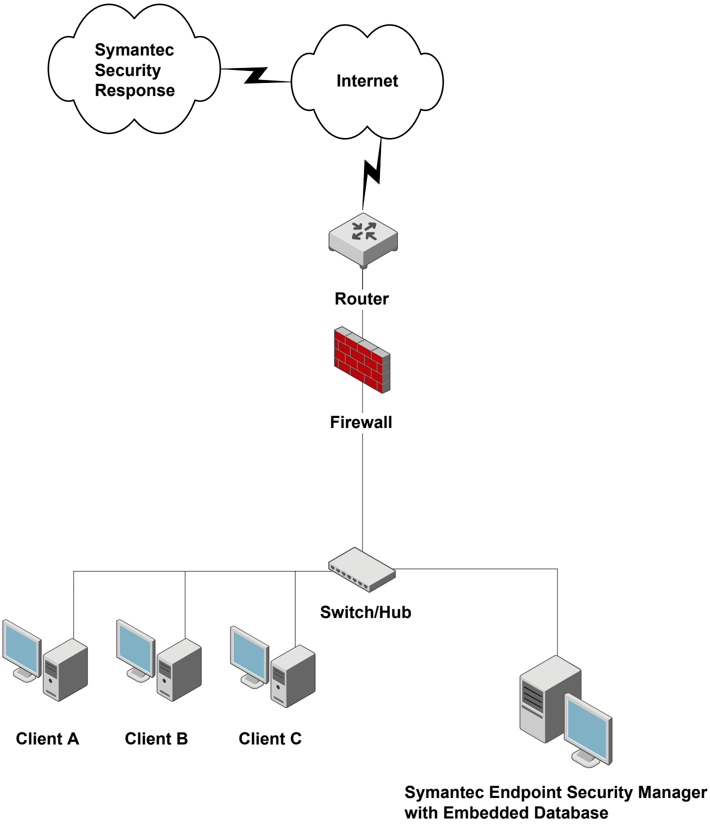
Before you install

If this installation is a first-time installation, you should install, configure, and test Symantec Endpoint Protection or Symantec Network Access Control software in a test environment.

Note: Small businesses that do not have test environment resources should install and test the client software on a few production clients.

Figure 1-2 shows one way to configure a test environment.

Figure 1-2 Sample test environment


Symantec Security Response
Internet
Router
Firewall
Switch/Hub
Client A
Client B
Client C
Symantec Endpoint Security Manager with Embedded Database

This test environment contains three clients and one server. The server runs three management components. The three management components are Symantec Endpoint Protection Manager, Symantec Endpoint Protection Manager Console, and the embedded Sybase database. These installation and configuration procedures are designed for this sample test environment.

The computers on which you install Symantec Endpoint Protection Manager must meet the following minimum software requirements:

- Windows 2000 Server with Service Pack 3, Windows XP, or Windows Server 2003

- Internet Information Services (IIS) version 5.0 or greater
- Internet Explorer 6.0

The computers on which you install client software must meet the following minimum software requirements:

- Windows 2000 Professional with Service Pack 3, Windows XP, or Windows Server 2003
- Internet Explorer 6.0 or greater

Installing and configuring Symantec Endpoint Protection Manager

Installing management software for the first time is divided into two parts. The first part installs Symantec Endpoint Protection Manager. The second part installs and configures the Symantec Endpoint Protection Manager database. In the first, you can accept all defaults. In the second part, you must add at least one custom value, which is a password.

Note: Management software does not include Symantec Endpoint Protection or any other client software that is managed.

To install Symantec Endpoint Protection Manager

1. Insert the installation CD and start the installation.
2. In the installation panel, do one of the following:
    - If you install Symantec Endpoint Protection, click **Install Symantec Endpoint Protection**.
    - If you install Symantec Network Access Control, click **Install Symantec Network Access Control**.
3. In the next installation panel, click **Install Symantec Endpoint Protection Manager**.
4. In the Welcome panel, click **Next**.
5. In the License Agreement panel, check **I accept the terms in the license agreement**, and then click **Next**.
6. In the Destination Folder panel, accept or change the installation directory.
7. Do one of the following:
    - To configure the Symantec Endpoint Protection Manager IIS Web as the only Web server on this computer, check **Create a custom Web site**, and then click **Next**.

- To let the Symantec Endpoint Protection Manager IIS Web server run with other Web servers on this computer, check **Use the default Web site**, and then click **Next**.

8 In the Ready to Install panel, click **Install**.

9 When the installation finishes and the Install Wizard Complete panel appears, click **Finish**.

Wait for the Management Server Configuration Wizard panel to appear, which can take up to 15 additional seconds.

To configure Symantec Endpoint Protection Manager

1 In the Management Server Configuration Wizard panel, click **Next**.

2 In the Site Type panel, check **Install my first Site**, and then click **Next**.

3 In the Server Information panel, accept or change the default values for the following boxes, and then click **Next**:

- Server Name
- Server Port
- Server Data Folder

4 In the Site Name panel, in the Site name box, enter your site name, and then click **Next**.

5 In the Encryption Password panel, type a value in both boxes, and then click **Next**.

Document this password when you install Symantec Endpoint Protection in your production environment. You need it for disaster recovery purposes, and for adding optional Enforcer hardware.

6 In the Database Server Choice panel, check **Embedded Database**, and then click **Next**.

7 In the Set User panel, in the Password boxes, type a password to use with Admin to log on to the console, and then click **Next**.

When the installation finishes, you have the option of deploying client software with the Installation and Migration Wizard. If you do not deploy client software at this time, refer to the Client Installation chapter for details on how to install client software. Logon to the console with the user name and password that you entered here.

Configuring and deploying client software

The Installation and Migration Wizard lets you configure a client software package. The Push Deployment Wizard then optionally appears to let you deploy the client software package. If you do not select to use the Push Deployment Wizard, you can start it manually by using ClientRemote.exe from the \tomcat\bin directory.

Note: This procedure assumes that you deploy client software to 32-bit computers and not to 64-bit computers. This procedure also has you select a directory in which to place installation files. You may want to create this directory before you start this procedure. Also, you need to authenticate with administrative credentials to the Windows Domain or Workgroup that contain the computers.

Deploying client software to computers that run firewalls, and that run Windows XP/Vista, have special requirements. Firewalls must permit remote deployment over TCP port 139 and the computers that are in workgroups and that run Windows XP must disable simple file sharing. Windows Vista has additional requirements.

To configure client software

1. In the Management Server Configuration Wizard Finished panel, check **Yes**, and then click **Finish**.
2. In the Welcome to the Migration and Deployment Wizard panel, click **Next**.
3. In the What would you like to do panel, check **Deploy the client**, and then click **Next**.
4. In the next unnamed panel, check **Specify the name of a new group that you wish to deploy clients to**, type a group name in the box, and then click **Next**.
5. In the next panel, uncheck any client software that you do not want to install, and then click **Next**.
6. In the next panel, check the options that you want for packages, files, and user interaction.
7. Click **Browse**, locate and select a directory in which to place the installation files, and then click **Open**.
8. Click **Next**.
9. In the next unnamed panel, check **Yes**, and then click **Finish**.

   Do not check Launch Administrator Console. It can take up to 5 minutes to create and export the installation package for your group before the Push Deployment Wizard appears.

To deploy the client software with the Push Deployment Wizard

1. In the Push Deployment Wizard panel, under Available Computers, expand the trees and select the computers on which to install the client software, and then click **Add**.
2. In the Remote Client Authentication dialog box, type a user name and password that can authenticate to the Windows Domain or Workgroup that contains the computers, and then click **OK**.
3. When you have selected all of the computers and they appear in the right pane, click **Finish**.
4. When installation completes, click **Done**.

Logging on to and locating your group in the console

Your first activity is to log on to the console and locate your group.

Logging on to the management console

The management console lets you manage clients.

To log on to the management console

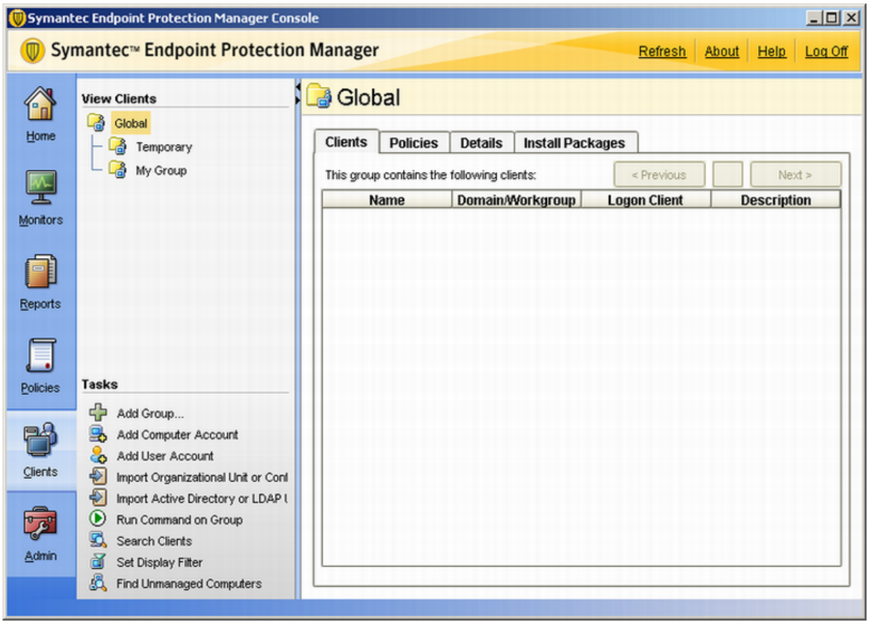
1. Click **Start > Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager Console**.
2. In the Symantec Endpoint Protection Manager logon prompt, in the User Name box, type **admin**.
3. In the Password box, type the admin password that you created during installation, and then click **Log on**.

About locating your group in the console

After you log on, you should locate the group that you created during installation. Then verify that the client computers to which you deployed software appear in that group.

Figure 1-3 illustrates an example of a group that was created during installation.

Figure 1-3 Group



This group contains the following clients:

About policies

Symantec Endpoint Protection Manager lets you configure and apply policies to groups or locations in groups. All client computers that are in the groups and locations receive the permissions and features that are specified in the policies. For example, if a LiveUpdate Settings policy specifies to run LiveUpdate daily at 10:00 P.M., all clients that receive that policy run LiveUpdate daily.

For Symantec Endpoint Protection, multiple policies exist. Policies exist for LiveUpdate, Antivirus and Antispyware protection, Global Exclusions, and so forth. For Symantec Network Access Control, two policies exist, one for LiveUpdate and one for Host Integrity.

Note: For legacy Symantec AntiVirus and Symantec Client Security users, the settings that applied to groups, management servers, and clients are now contained in policies.

Configuring LiveUpdate for site updates

You should configure the frequency that the Symantec Endpoint Protection Manager checks for and downloads new updates to the site. You also configure client updates with LiveUpdate Content policies, so be sure to download all types that you want clients to receive.

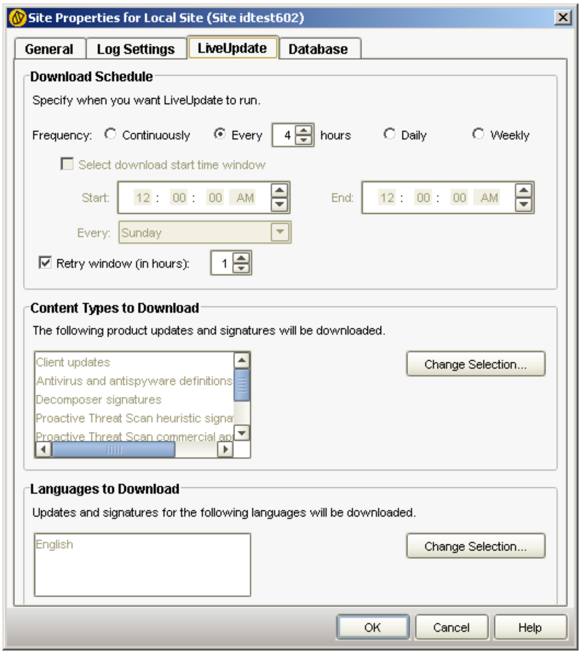
Symantec Endpoint Protection Manager for Symantec Network Access Control only supports product updates.

To configure LiveUpdate for the site

1 In the console left pane, click **Admin**.

2 In the lower-left pane, click **Servers**.

3 In the upper-left pane, right-click **Local Site**, and then click **Properties**.



Site Properties for Local Site (Site idtest602)

Download Schedule

Specify when you want LiveUpdate to run.

Frequency: ○ Continuously ● Every 4 hours ○ Daily ○ Weekly

□ Select download start time window

Start: 12 : 00 : 00 AM End: 12 : 00 : 00 AM

Every: Sunday

☑ Retry window (in hours): 1

Content Types to Download

The following product updates and signatures will be downloaded.

Client updates
Antivirus and antispyware definitions
Decomposer signatures
Proactive Threat Scan heuristic signa
Proactive Threat Scan commercial ap

Languages to Download

Updates and signatures for the following languages will be downloaded.

English

4 On the LiveUpdate tab, under Download Schedule, check the Frequency options with which to download the latest definitions.

5 For details about setting other options in this dialog box, click **Help**.

6 When you finish setting the site's LiveUpdate properties, click **OK**.

Configuring LiveUpdate for client updates

When you create a group with the Installation and Migration Wizard, your group receives default policies. If you create a new policy of the same type as a default policy and apply it to the group, the default policy disappears. For example, you can create a LiveUpdate policy that is called MyLiveUpdate policy and apply it to a group that uses a default LiveUpdate policy. MyLiveUpdate then takes the place of the default LiveUpdate policy. Other groups can also share the new policy that you create.

Two types of LiveUpdate policies exist. A LiveUpdate Settings policy specifies the frequency that clients run LiveUpdate to check for content updates. A LiveUpdate Content policy specifies the content that clients can receive when they run LiveUpdate.

Configuring a LiveUpdate Settings policy

When you create a group with the Installation and Migration Wizard, your group receives default policies. You can either create a new policy and replace the default policy, or edit the default policy. A best practice is to create a new policy and modify the default policy.

To configure a LiveUpdate settings policy

1. On the console, click **Policies**.
2. In the View Policies pane, click **LiveUpdate**.
3. In the lower-left Tasks pane, click **Add a LiveUpdate Setting Policy**.
4. In the Overview pane, in the Policy name box, type a name for the policy.
5. Under LiveUpdate policy, click **Schedule**.
6. In the Schedule pane, accept or change the scheduling options.
7. Under LiveUpdate policy, click **Advanced Settings**.
8. Decide whether to keep or change the default settings.
9. For details about the settings, click **Help**.

   Generally, you do not want users to modify update settings. However, you may want to let them manually launch a LiveUpdate session if you do not support hundreds or thousands of clients.
10. When you have configured your policy, click **OK**.
11. In the Assign Policy dialog box, Click **Yes**.
12. In the Assign LiveUpdate Policy dialog box, check the groups and locations to which to apply the policy, and then click **Assign**.

    If you cannot select a nested group, that group inherits policies from its parent group, as set on the Clients Policies tab.
13. In the Apply LiveUpdate Policy dialog box, click **OK**, and complete the application.

Configuring a LiveUpdate Content policy

By default, all clients in a group receive the latest versions of all content updates. If a group is configured to get updates from a management server, the clients receive only the updates that the server downloads. If the LiveUpdate content policy is configured to allow all updates, but the management server is not configured to download all updates, the clients receive only what the server downloads. What the server downloads is configurable from the Admin pane.

Note: LiveUpdate Content policies are not available for Symantec Network Access Control clients.

To configure a LiveUpdate Content policy

1. On the console, click **Policies**.
2. In the View Policies pane, click **LiveUpdate**.
3. In the LiveUpdate Policies pane, click the **LiveUpdate Content** tab.
4. In the lower-left Tasks pane, click **Add a LiveUpdate Content Policy**.
5. In the Overview pane, in the Policy name box, type a name for the policy.
6. If you configure Symantec Endpoint Protection, in the LiveUpdate Content pane, click **Security Definitions**.
7. In the Security Definitions pane, check the updates to download and install, and uncheck the updates to disallow.
8. In the LiveUpdate Content Policy window, click **OK.**
9. In the Assign Policy dialog box, click **Yes**.
10. In the Assign LiveUpdate Content Policy dialog box, check one or more groups to which to apply this policy, and then click **Assign**.

    If you cannot select a nested group, that group inherits policies from its parent group, as set on the Clients Policies tab.
11. In the Apply LiveUpdate Policy dialog box, click **OK**, and complete the application.

Configuring and testing Symantec Endpoint Protection

After you configure and install a LiveUpdate policy, you should create and apply an Antivirus and Antispyware protection policy.

Note: This section assumes that you purchased Symantec Network Access Control and installed it.

Configuring a default Antivirus and Antispyware policy

Next, you should configure an Antivirus and Antispyware policy for your group. This procedure has you edit the default policy that is currently only applied to the group. You can, however, create a new policy and apply it to your group.

To configure a default Antivirus and Antispyware policy

1. On the console, in the left pane, click **Clients**.
2. Under `My_Group`, on the Policies tab, under Policies, across from Antivirus and antispyware policy [shared], click **Tasks > Edit Policy**.
3. In the Edit Policy dialog box, click **Convert Non-Shared**.
4. In the AntiVirus and Antispyware panel, click **File System Auto-Protect**.
5. On the Scan Details tab, verify that **Enable File System Auto-Protect** is checked, and that the lock icon is in the unlocked mode (for testing).

   Generally, you want this setting locked, but for initial testing purposes, leave it unlocked. Locking a setting prevents users from changing a setting.
6. On the Actions tab, under Detection, click **Non-macro virus**.
7. Under Actions for: Non-macro virus, inspect the default sequence of actions that occur when a non-macro virus is detected.

   The first action is to try to clean the virus. If it is not possible to clean, the virus is quarantined.
8. On the Notifications tab, inspect the message that appears on client computers when a virus or security risk is detected.

   You can change this message later if necessary.
9. In the left pane, click **Administrator-defined scans**.
10. On the Scans tab, under Name, click **Full Scan every Friday at 8 PM**, and then click **Edit**.
11. Become familiar with the options on the different tabs and change them if necessary.

    Full scans are always recommended initially. After full scans are run, Quick scans and Auto-Protect are effective to secure client computers.
12. When you understand the scan options, click **OK**.
13. In the left pane, click **Quarantine**.

14 In the Quarantine pane, under Additional Options, click **Clean-up options**.

15 In the Clean-up options dialog box, review the settings for purging repaired and quarantined files.

Become familiar with these settings if you want to change them in the future.

16 Click **OK**.

Testing antivirus capabilities

You should experiment with antivirus detection in a controlled test environment to become familiar with alerts and log entries. Before you test antivirus detection, download the latest antivirus test file Eicar.com onto transportable media such as a memory stick. You can download Eicar.com at the following URL:

http:// www.eicar.org

Testing Auto-Protect

Auto-Protect is the Symantec real-time process that inspects every file that executes or is user-accessed to see if it is a virus or security risk. Auto-Protect determines whether files are viruses or security risks by using the definitions that you download from Symantec. You can see how Auto-Protect works by using a benign virus called Eicar. Several versions are available from at the following URL:

http://www.eicar.org.

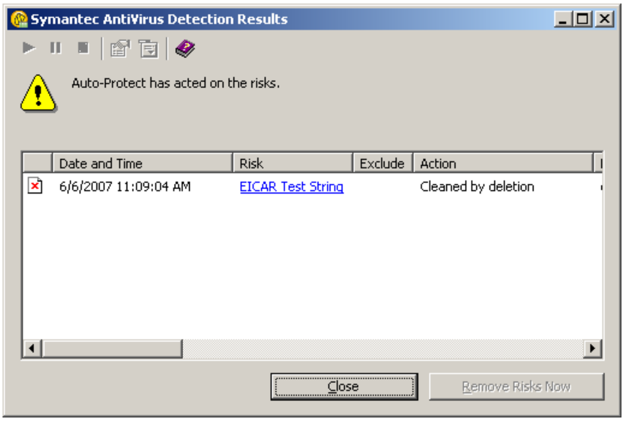
To test Auto-Protect

1 On a client computer, in the lower-right corner, right-click the Symantec Endpoint Protection shield, and click **Disable Auto-Protect**.

2 If you have not downloaded eicar.com, go to http://www.eicar.org, and then locate and download eicar.com to the client computer.

3 In the lower-right corner, right-click the Symantec Endpoint Protection shield, and click **Enable Auto-Protect**.

4 Double-click **eicar.com**.



Symantec AntiVirus Detection Results

Auto-Protect has acted on the risks.

	Date and Time	Risk	Exclude	Action
☒	6/6/2007 11:09:04 AM	EICAR Test String		Cleaned by deletion

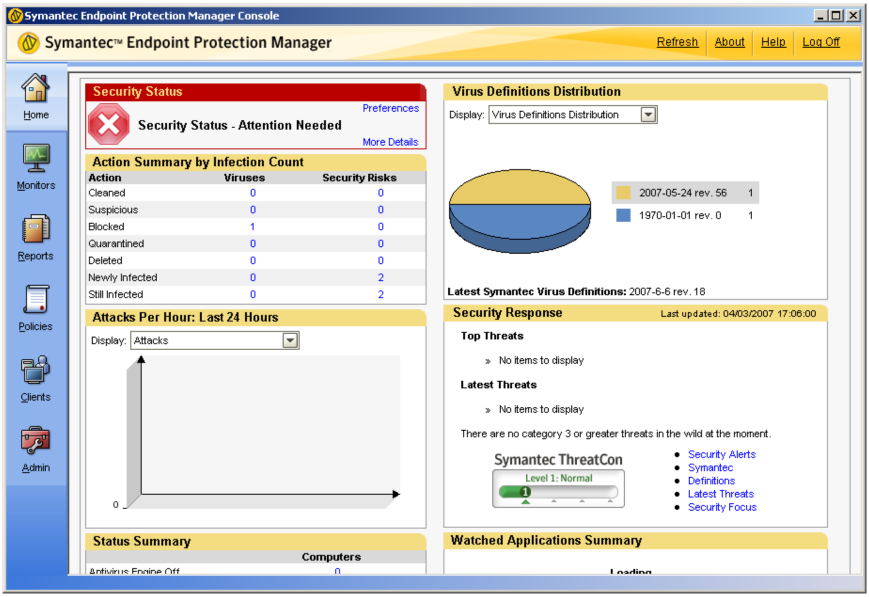
5 Read and become familiar with the details in the message prompt(s).

Managing the detected threat

After Symantec Endpoint Protection detects and isolates eicar.com, it sends the information to Symantec Endpoint Protection Manager. You can then see that the activity that occurred from the Home page in Symantec Endpoint Protection Manager Console. This task is a primary task that you perform in a production environment. When clients detect real threats, you first display details about the threat. You then decide if Auto-Protect mitigated the threat and then clear the status.

To manage the detected threat

1 In the console, click **Home**.



Security Status

Security Status - Attention Needed

Virus Definitions Distribution

2007-05-24 rev. 56	1
1970-01-01 rev. 0	1

Latest Symantec Virus Definitions: 2007-6-6 rev. 18

Action Summary by Infection Count

Action	Viruses	Security Risks
Cleaned	0	0
Suspicious	0	0
Blocked	1	0
Quarantined	0	0
Deleted	0	0
Newly Infected	0	2
Still Infected	0	2

Attacks Per Hour: Last 24 Hours

Security Response Last updated: 04/03/2007 17:06:00

Top Threats

» No items to display

Latest Threats

» No items to display

There are no category 3 or greater threats in the wild at the moment.

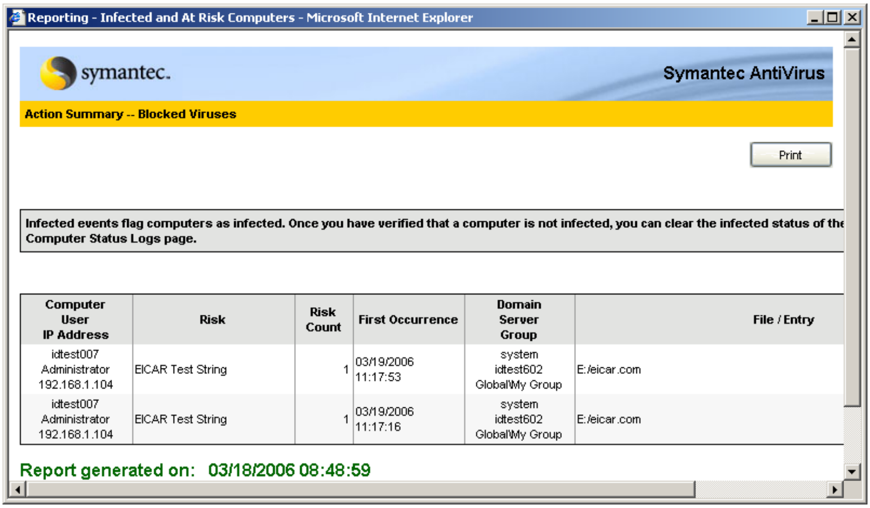
Status Summary

	Computers
Antivirus Engine Off	0

Watched Applications Summary

Loading

2 In the Viruses column for the Blocked row, click the number.


Reporting - Infected and At Risk Computers - Microsoft Internet Explorer
symantec.
Symantec AntiVirus
Print

Action Summary -- Blocked Viruses

Infected events flag computers as infected. Once you have verified that a computer is not infected, you can clear the infected status of the
Computer Status Logs page.

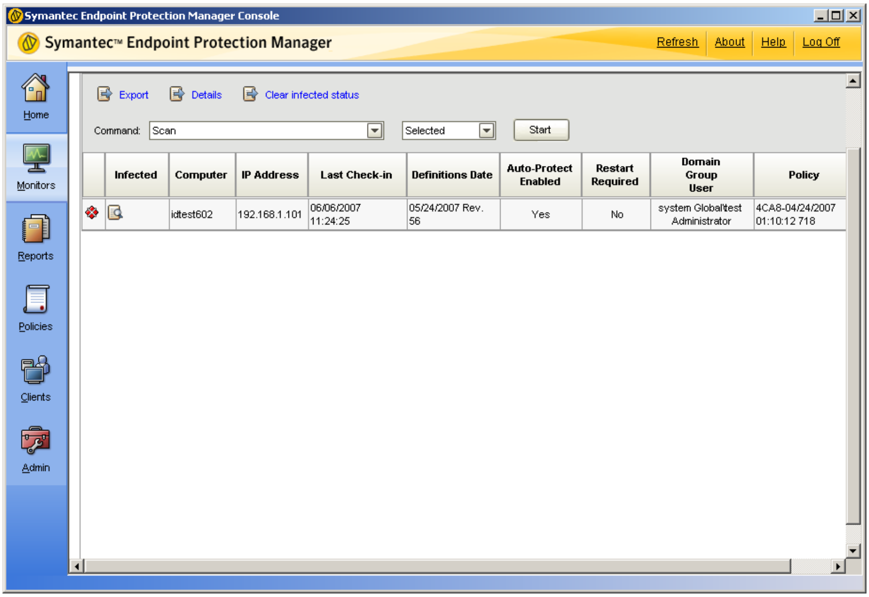
Computer User IP Address	Risk	Risk Count	First Occurrence	Domain Server Group	File / Entry
idtest007 Administrator 192.168.1.104	EICAR Test String	1	03/19/2006 11:17:53	system idtest602 Global\My Group	E:/eicar.com
idtest007 Administrator 192.168.1.104	EICAR Test String	1	03/19/2006 11:17:16	system idtest602 Global\My Group	E:/eicar.com

Report generated on: 03/18/2006 08:48:59

3 In the Reporting - Infected and AT Risk Computers window, become familiar with the reported information, and then close the window.

4 Click **Monitors**.

5 On the Logs tab, in the Log Type drop-down, click **Computer Status**, and then click **View Log**.



Command: Scan | Selected

	Infected	Computer	IP Address	Last Check-in	Definitions Date	Auto-Protect Enabled	Restart Required	Domain Group User	Policy
❖	🔍	idtest602	192.168.1.101	06/06/2007 11:24:25	05/24/2007 Rev. 56	Yes	No	system Global\test Administrator	4CA8-04/24/2007 01:10:12 718

6 To display information about the infection, click **Details**.

7 To clear the Infected Status, click **Clear infected status**.

Configuring the security status icon

The Home page displays the security status of your client computers. The two possible statuses are Good and Poor. You can control when the status is Good and Poor by setting security status threshold preferences.

To configure the security status icon

1 In the console, click **Home**.

2 Under Security Status, click **More Details**.

3 In the Security Status dialog box, review the features that trigger the Good and Poor status.

4 In the upper-right corner, click **X**.

5 Under Security Status, click **Preferences**.

6 In the Preferences dialog box, on the Security Status tab, review the security status triggers and thresholds that you can set.

All thresholds default to 10 percent.

7 For security status details, click **Help**.

To trigger the Poor status, disable Auto-Protect on one of your test clients.

8 Click **OK**.

9 To review the security status of your managed clients at any time, on the Home page, click the status icon.

Where to get more information

Sources of information include the following:

- *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control*
- *Client Guide for Symantec Endpoint Protection and Symantec Network Access Control*
- *LiveUpdate Administration Guide* (Symantec Endpoint Protection only)
- *Symantec Central Quarantine Administration Guide* (Symantec Endpoint Protection only)
- Online Help that contains all of the content that is in the guides and more

The primary documentation is available in the Documentation folder on the installation CDs. Some individual component folders contain component-specific documentation. Updates to the documentation are available from the Symantec Technical Support Web site.

Table 1-2 lists the additional information that is available from the Symantec Web sites.

Table 1-2 Symantec Web sites

Types of information	Web address
Public Knowledge Base Releases and updates Manuals and documentation updates Contact options	http://www.symantec.com/techsupp/enterprise/
Virus and other threat information and updates	http://securityresponse.symantec.com
Product news and updates	http://enterprisesecurity.symantec.com