Solutions Guide for Symantec™ Endpoint Protection and Symantec Network Access Control

symantec™

Solutions Guide for Symantec™ Endpoint Protection 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 11.00.02.00.00

Legal Notice

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
20330 Stevens Creek Blvd.
Cupertino, CA 95014

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's maintenance offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

For information about Symantec's Maintenance Programs, you can visit our Web site at the following URL:

www.symantec.com/techsupp/

Contacting Technical Support

Customers with a current maintenance agreement may access Technical Support information at the following URL:

www.symantec.com/techsupp/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system

- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/techsupp/

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp/

Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and maintenance contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Maintenance agreement resources

If you want to contact Symantec regarding an existing maintenance agreement, please contact the maintenance agreement administration team for your region as follows:

Asia-Pacific and Japan	contractsadmin@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Symantec Early Warning Solutions — These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.

Managed Security Services — These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.

Consulting Services — Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.

Educational Services — Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

www.symantec.com

Select your country or language from the site index.

Contents

Technical Support 4

Chapter 1 Introducing solutions 11

About solutions 11

Section 1 Best practices for administering clients 13

Chapter 2 Troubleshooting communication problems with the management server 15

About communication problems 16

About checking the communication between the management server and the client 16

About checking the communication between the management server and the console or the database 17

Viewing the client status in the management console 20

About the client status icon in the client 21

Viewing the policy serial number 22

About performing a manual policy update to check the policy serial number 22

Using the ping command to test the connectivity to the management server 23

Using a browser to test the connectivity to the management server 23

Using Telnet to test the connectivity to the management server 24

Checking the inbox logs on the management server 25

Checking the IIS logs on the management server 25

About checking the debug log on the client computer 25

Verifying the connection with the database 26

Configuring the rights for IIS 28

Chapter 3 Troubleshooting when a client does not update content

Chapter 3 Troubleshooting when a client does not update content 31

About troubleshooting content update problems on clients 32
About types of content for Symantec Endpoint Protection 33
About determining how a client is configured to receive content 34
About network connectivity and clients 34
About checking the client's connection status 35
Making sure that the client can communicate with its content provider 36
About determining whether a client is receiving content updates from the management server 37
About comparing the content on the client to the content on the management server 38
Comparing the content cache 38
Using the management console to compare content versions 39
Viewing the latest LiveUpdate downloads to the management server 40
Checking the LiveUpdate settings on the management server 41
Checking the LiveUpdate content policy settings 41
About checking the LiveUpdate Settings policy 42
Running a manual LiveUpdate session from the management console 42
What to do if you still have problems after verifying connectivity and LiveUpdate settings 43
    Viewing the LiveUpdate log 43
    About viewing the debug log on the client 44
    Creating a sylink log 44
    About using the DebugView tool 45

Chapter 4 Setting up and managing mobile clients and remote clients 47

About mobile clients and remote clients 47
Setting up groups and locations 48
About common mobile client and remote client scenarios 51
About location awareness criteria 51
    Setting up Scenario One location awareness conditions 52
    Setting up Scenario Two location awareness conditions 53
Strengthening your security policies for remote clients 55
    About best practices settings for a Firewall Policy 56
    About best practices settings for an Antivirus and Antispyware Policy 57

About best practices settings for a LiveUpdate Policy 57
About best practices settings for an Application Control Policy 58
About client notifications 58
Customizing client log management settings 58
Managing load balancing and roaming 59
Monitoring remote clients 59

Chapter 5 Symantec Endpoint Protection organization: Servers, sites, and Group Update Providers 61

About the Symantec Endpoint Protection management topology 61
Organizational factors to consider 62
Deciding to create one site or multiple sites 63
Deciding how to update content 64
About high availability and failover 66
About load balancing and roaming 67

Section 2 Best practices for overall security 69

Chapter 6 Managing TruScan proactive threat scans 71

About managing TruScan proactive threat scans 71
About managing exceptions 72
Monitoring the scan events 73
Creating exceptions for detected processes 74
Adjusting scan settings 76

Index 81

Chapter 1

Introducing solutions

This chapter includes the following topics:

- About solutions

About solutions

Symantec Endpoint Protection and Symantec Network Access Control are comprehensive sets of software that are designed to solve network security problems. They provide threat protection for all sizes of enterprise, from the smallest to the largest. They are built to be flexible and highly manageable and provide a high number of configuration choices. Therefore, there are many factors that influence how best to set up and use the software.

You can use solutions to help you manage a secure environment for your organization's network. Each solution offers either a set of scenarios or a discussion of the best practices that you can use. The solution depends on various factors, such as the types and numbers of endpoints, available technical support staff, and numbers of sites. For example, solutions can help you resolve the issues that affect the communication with and the security of the client computers.

For more information about the solutions available in Knowledge Base articles and FAQs, refer to the Symantec Technical Support Web site at the following URL:

www.symantec.com/techsupp/

Before you implement a solution, you must read the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control* and the *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control* and install the software in a test environment. Solutions are designed for the system administrator who installs and maintains the products.

Section 1

Best practices for administering clients

- Troubleshooting communication problems with the management server
- Troubleshooting when a client does not update content
- Setting up and managing mobile clients and remote clients
- Symantec Endpoint Protection organization: Servers, sites, and Group Update Providers

Chapter 2

Troubleshooting communication problems with the management server

This chapter includes the following topics:

- About communication problems
- Viewing the client status in the management console
- About the client status icon in the client
- Viewing the policy serial number
- About performing a manual policy update to check the policy serial number
- Using the ping command to test the connectivity to the management server
- Using a browser to test the connectivity to the management server
- Using Telnet to test the connectivity to the management server
- Checking the inbox logs on the management server
- Checking the IIS logs on the management server
- About checking the debug log on the client computer
- Verifying the connection with the database
- Configuring the rights for IIS

About communication problems

You might need to check the communication between the management server and other components for several reasons. For example, the client might not receive policy updates or content updates or the appropriate rights may not be configured for IIS. These components include the client, console, and the database.

About checking the communication between the management server and the client

If you have trouble with client and server communication, you should first check to make sure that there are no network problems. You should also check network connectivity before you call Symantec Technical Support.

You can test the communication between the client and the management server in several ways.

Table 2-1 describes the steps that you can take to check the communication between the client computer and the management server.

Table 2-1 Checking the communication between the management server and the client

What to check	Description
Check the client status icon.	You can check the status icon in the client and in the management console.
Check the policy serial number in the client and in the management console.	The serial number should match if the client can communicate with the server and receives regular policy updates. You can perform a manual policy update and then check the policy serial numbers against each other.
Test the connectivity between the client and the management server.	You can issue several commands on the client to test the connectivity to the management server. You can do the following tests: ■ Ping the management server from the client computer. ■ Telnet to the management server from the client computer. ■ Use a Web browser on the client computer to connect to the management server.

Table 2-1 Checking the communication between the management server and the client *(continued)*

What to check	Description
Check for any network problems.	You should verify that there are no network problems by checking the following items: ■ Test the connectivity between the client and management server first. If the client computer cannot ping or Telnet to the management server, you should verify the DNS service for the client. ■ Check the client's routing path. ■ Check that the management server does not have a network problem. ■ Check that the Symantec Endpoint Protection firewall (or any third-party firewall) does not cause any network problems.
Check the IIS logs on the management server.	You can check the IIS logs on the management server. The logs can help you to determine whether the client can communicate with the IIS server on the management server computer.
Check the debug logs on the client.	You can use the debug log on the client to determine if the client has communication problems.

About checking the communication between the management server and the console or the database

If you have a connection problem with the console or the database, you may see one of the following symptoms:

- The management server service (semsrv) stops.
- The management server service does not stay in a started state.
- The Home, Monitors, and Reports pages display an HTTP error.
- The Home, Monitors, and Reports pages are blank.
- The Home, Monitors, and Reports pages display a continuously loading progress bar, without displaying any content.
- A message appears, stating that too many users are connected.

All of these issues display a Java -1 error in the Windows Event log. To find the specific cause for the Java -1 error, look in the scm-server log. The scm-server log is typically located in the following location:

C:\Program Files\Symantec\Symantec Endpoint Protection Manager\tomcat\logs\scm-server-0.log

Table 2-2 describes the actions that you can take in response to the communication errors with the console or database.

Table 2-2 Checking the communication with the console or database

What to check	Description
Test the connectivity between the database and the management server.	You can verify that the management server and the database communicate properly. See "Verifying the connection with the database" on page 26.
Check that the management server heap size is correct.	You may need to adjust the heap size that is appropriate for the management server's operating system. If you cannot log in to the management server's remote console, or if you see an out-of-memory message in the smc-server log, you may need to increase the heap size. The default heap size for Symantec Endpoint Protection Manager is 256 MB. For more information on system requirements, see the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control.*
Check that the management server is not running multiple versions of PHP.	You can check whether the management server runs multiple software packages that use different versions of PHP. PHP checks for a global configuration file (php.ini). If there are multiple configuration files, you must force each product to use its own interpreter. When each product uses the correct version of PHP associated with it, the management server operates properly.

Table 2-2 Checking the communication with the console or database *(continued)*

What to check	Description
Check the number of concurrent connections to the client.	You can check that you do not have more than ten concurrent connections with the client. You may have too many connections if the management server displays the following error messages: ■ `Too many users connected.` ■ `No more connections can be made to this remote computer at this time already as many connections as the computer can accept.` Your Microsoft's End User Licensing Agreement (EULA) lists the number of connections you are allowed. The Windows XP Professional Edition and Windows 2000 Professional Edition are limited to a maximum of ten concurrent connections. You can increase the number of connections by doing one of the following actions: ■ Install the management server on a different version of Windows, such as Windows Server 2003. ■ Switch the client to pull mode and increase the interval at which the client downloads the security policy. In pull mode, the management server maintains the connection with the client. In pull mode, the management server does not maintain the connection. The longer the pull mode interval, the more concurrent connections the management server can have.
Check the system requirements.	You can check whether both the client and the management server run the minimum or recommended system requirements. For more information, see the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control*.
Check that the appropriate rights are configured for IIS.	You can check that the Internet Information Services (IIS) is configured with the appropriate rights. If the IIS is configured incorrectly, the management server displays an HTTP error or blank pages in the Home, Monitors, or Reports pages. See "Configuring the rights for IIS" on page 28.

Viewing the client status in the management console

You can check the client status icon in the management console as well as on the client directly to determine client status.

Table 2-3 shows the various icons that might appear in the management console for the client status.

Table 2-3 Client status icons in the management console

Icon	Description
	This icon indicates the following status: ■ The client can communicate with Symantec Endpoint Protection Manager. ■ The client is in computer mode.
	This icon indicates the following status: ■ The client cannot communicate with Symantec Endpoint Protection Manager. ■ The client is in computer mode. ■ The client may have been added from the console, and may not have any Symantec client software installed.
	This icon indicates the following status: ■ The client can communicate with Symantec Endpoint Protection Manager. ■ The client is in computer mode. ■ The client is an unmanaged detector.
	This icon indicates the following status: ■ The client cannot communicate with Symantec Endpoint Protection Manager. ■ The client is in computer mode. ■ The client is an unmanaged detector.
	This icon indicates the following status: ■ The client can communicate with Symantec Endpoint Protection Manager. ■ The client is in user mode.

Table 2-3 Client status icons in the management console *(continued)*

Icon	Description
👤	This icon indicates the following status: ■ The client cannot communicate with Symantec Endpoint Protection Manager. ■ The client is in user mode. ■ The client may have been added from the console, and may not have any Symantec client software installed.
🖥	This icon indicates the following status: ■ The client can communicate with Symantec Endpoint Protection Manager at another site. ■ The client is in computer mode.
🕒	This icon indicates the following status: ■ The client can communicate with Symantec Endpoint Protection Manager at another site. ■ The client is in computer mode. ■ The client is an unmanaged detector.
👤	This icon indicates the following status: ■ The client can communicate with Symantec Endpoint Protection Manager at another site. ■ The client is in computer mode.

To view the client status in the management console

1. In the management console, on the Clients page, under View Clients, select the group in which the client belongs.
2. Look on the Clients tab.

   The client name should appear in the list next to an icon that shows the client status.

About the client status icon in the client

You can find the client status icon in the notification area on the client computer. The icon appears as a yellow shield icon with a green dot when the client can communicate with the management server. For the Symantec Network Access Control client, the icon appears as a yellow key.

For more information on the client status icons, see the *Client Guide for Symantec Endpoint Protection and Symantec Network Access Control*.

Viewing the policy serial number

You should check the policy serial number on the client to see if it matches the serial number that appears in the management console. If the client communicates with the management server and receives regular policy updates, the serial numbers should match.

If the policy serial numbers do not match, you can try to manually update the policies on the client computer and check the troubleshooting logs.

To view the policy serial number in the management console

1. On the management server, in the console, click **Clients**.
2. Under View Clients, select the relevant group, and then click **Details**.

   The policy serial number and the policy date appear at the bottom of the details list.

To view the policy serial number on the client

1. On the client computer, in the client, on the Help and Support menu, click **Troubleshooting**.
2. On the Management tab, look at the policy serial number.

   The serial number should match the serial number of the policy that the management server pushes to the client.

About performing a manual policy update to check the policy serial number

You can perform a manual policy update to check whether or not the client receives the latest policy update. If the client does not receive the update, there might be a problem with the client and server communication.

You can try a manual policy update by doing any of the following actions:

- In the client on the Help and Support menu, in the Troubleshooting dialog box, under Policy Profile, you can click Update. You can use this method if you want to perform a manual update on a particular client.
- For the clients that are configured for pull mode, the management server downloads policies to the client at regular intervals (heartbeat). You can change the heartbeat interval so that policies are downloaded to the client group more

quickly. After the heartbeat interval, you can check to see if the policy serial numbers match. (For the clients that are configured for push mode, the clients receive any policy updates immediately.)

After you run a manual policy update, make sure that the policy serial number that appears in the client matches the serial number that appears in the management console.

Using the ping command to test the connectivity to the management server

You can try to ping the management server from the client computer to test connectivity.

To use the ping command to test the connectivity to the management server

1. On the client, open a command prompt.
2. Type the ping command. For example:

   ping *name*

   where *name* is the computer name of the management server. You can use the server IP address in place of the computer name. In either case, the command should return the server's correct IP address.

   If the ping command does not return the correct address, verify the DNS service for the client and check its routing path.

Using a browser to test the connectivity to the management server

You can use a Web browser to test the connectivity to the management server.

To use a browser to test the connectivity to the management server

1. On the client computer open a Web browser, such as Internet Explorer.
2. In the browser command line, type a command that is similar to either of the following commands:

   http://*management server IP address*/reporting/index.php

   If the reporting logon Web page appears, the client can communicate with the management server.

   http://*management server name*:9090

   If the Symantec Endpoint Protection Manager Console page appears, the client can communicate with the management server.
3. If a Web page does not appear, check for any network problems. Verify the DNS service for the client and check its routing path.

Using Telnet to test the connectivity to the management server

You can use Telnet to test the connectivity to the IIS server on the management server. If the client can Telnet to the management server's HTTP or HTTPS port, the client and the server can communicate. The default HTTP port is 80; the default HTTPS port is 443.

Note: You might need to adjust your firewall rules so that the client computer can Telnet into the management server.

For more information about the firewall, see the *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control*.

To use Telnet to test the connectivity to the management server

1. On the client computer, make sure the Telnet service is enabled and started.
2. Open a command prompt and enter the Telnet command. For example:

   telnet *ip address*:80

   where *ip address* is the IP address of the management server.

   If the Telnet connection fails, verify the client's DNS service and check its routing path.

Checking the inbox logs on the management server

You can use a registry key to generate logs about activity in the management server inbox.

When you modify the registry key, the management server generates the logs (ersecreg.log and exsecars.log). You can view these logs to troubleshoot client and server communication. You can find the logs in the log directory of the inbox on the management server.

To check the inbox logs on the management server

- On the management server, under HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SEPM, set the DebugLevel value to 3.

  Typically, the inbox appears in the following location on the management server computer:

  ```
  \Program Files\Symantec\Symantec Endpoint Protection Manager\data\
  inbox\log
  ```

  You can open the logs with a text application such as Notepad.

Checking the IIS logs on the management server

You can check the IIS logs on the management server. The logs show GET and POST commands when the client and the server communicate.

To check the IIS logs on the management server

1. On the management server, go to the IIS log files directory. A typical path to the directory is:

   \WINDOWS\system32\LogFiles\W3SVC1

2. Open the most recent log file with a text application such as Notepad. For example, the log file name might be ex070924.log.

3. Review the log messages.

   The file should include both GET and POST messages.

About checking the debug log on the client computer

You can check the debug log on the client. If the client has communication problems with the management server, status messages about the connection problem appear in the log.

You can check the debug log by using the following methods:

- In the client, on the Help and Support menu, in the Troubleshooting dialog box, you can click Edit Debug Log Settings and type a name for the log. You can then click View Log.
- You can use the registry to turn on debugging in the client.
  You can find the registry key in the following location:
  HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\smc_debuglog_on

Verifying the connection with the database

The management server and the database may not communicate properly. You should verify that the database runs and then test the connection between the server and the database.

If the management server runs the embedded Sybase database, perform the following steps:

- Verify that the Symantec Embedded Database service runs and that the dbsrv9.exe process listens to TCP port 2638.
- Test the ODBC connection.

If the management server runs the remote SQL database, perform the following actions:

- Verify that you have specified a named instance when you installed and configured the Symantec Endpoint Protection Manager.
- Verify that SQL Server runs and is properly configured.
- Verify that the network connection between Symantec Endpoint Protection Manager and the SQL database is correct.
- Test the ODBC connection.

To verify communication with the embedded database

1. On the management server, click **Start > Control Panel > Administrative Tools**.
2. In the Administrative Tools dialog box, double-click **Data Sources (ODBC)**.
3. In the ODBC Data Source Administrator dialog box, click **System DSN**.
4. On the System DSN tab, double-click **SymantecEndpointSecurityDSN**.
5. On the ODBC tab, verify that the Data source name drop-down list is `SymantecEndpointSecurityDSN` and type an optional description.

6 Click **Login**.

7 On the Login tab, in the User ID text box, type `dba`.

8 In the Password text box, type the password for the database.

This password is the one that you entered for the database when you installed the management server.

9 Click **Database**.

10 On the Database tab, in the Server name text box, type <\\*servername**instancename*>.

If you use the English version of Symantec Endpoint Protection Manager, type the default, `sem5`. Otherwise, leave the Server name text box blank.

11 On the ODBC tab, click **Test Connection** and verify that it succeeds.

12 Click **OK**.

13 Click **OK**.

To verify communication to the SQL database

1 On the management server, click **Start > Control Panel > Administrative Tools**.

2 In the Administrative Tools dialog box, double-click **Data Sources (ODBC)**.

3 In the ODBC Data Source Administrator dialog box, click **System DSN**.

4 On the System DSN tab, double-click **SymantecEndpointSecurityDSN**.

5 In the Server drop-down list, verify that the correct server and instance is selected.

6 Click **Next**.

7 For Login ID, type `sa`.

8 In the Password text box, type the password for the database.

This password is the one that you entered for the database when you installed the management server.

9 Click **Next** and make sure that `sem5` is selected for the default database.

10 Click **Next**.

11 Click **Finish**.

12 Click **Test Data Source** and look for the result that states:

```
TESTS COMPLETED SUCCESSFULLY!
```

Configuring the rights for IIS

The HTTP error messages typically indicate a problem with the configuration of Internet Information Services (IIS). To diagnose the problem, check the IIS logs to get the full error code.

See “Checking the IIS logs on the management server” on page 25.

You can check the following items to see if the IIS is configured properly:

- Verify that the DefaultAppPool identity is set to Network Service.
- Verify that the user rights are correct.
- Verify that the authentication and access control settings are correct.
- Verify that the secure communications setting is not selected.
  Verify this setting only if the SSL is not implemented.

If you make any changes to the following settings, restart the IIS when you have completed any of the following tasks.

To verify that the DefaultAppPool identity is set to Network Service

1. On the management server, click **Start > Programs > Administrative Tools > Internet Information Services (IIS) Manager**.
2. Expand *server name* and then expand **Application Pools**.
3. Right-click **DefaultAppPool** and click **Properties**.
4. On the Identity tab, verify that the Predefine option is selected and displays Network Service.
5. Click **OK**.

To verify that the user rights are correct

1. On the management server, open a command line and type:

   ```
   gpedit.msc
   ```

2. In the Group Policy Object Editor, expand **Computer Configuration > Windows Settings > Security Settings > Local Policies**.
3. Click **User Rights Assignment**.
4. In the right-hand pane, double-click **Adjust memory quotas for a process**.

5. On the Local Security Setting tab, verify that NETWORK SERVICE is listed.

   If the Add User or Group button is disabled, a domain GPO (group policy object) may have locked this policy. You may need to assess the domain GPOs to unlock it.

6. Click **OK**.

To verify that the authentication and access control settings are correct

1. On the management server, click **Start > Administrative Tools > Internet Information Services (IIS) Manager**.
2. Expand *server name* and then expand **Web Sites**.
3. Right-click **Default Web Site** and click **Properties**.
4. On the Directory Security tab, under Authentication and access control, click **Edit**.
5. Verify that Enable anonymous access is checked.
6. Verify that the user name and password are correct.
7. Under Authenticated access, verify that the appropriate settings are correct.
8. Click **OK**.
9. Click **OK**.

To verify that the secure communications setting is not selected

1. On the management server, click **Start > Administrative Tools > Internet Information Services (IIS) Manager**.
2. Right-click **Default Web Site** and click **Properties**.
3. On the Directory Security tab, under Secure communications, click **Edit**.
4. Verify that Require secure channel (SSL) is unchecked.
5. Click **OK**.
6. Click **OK**.

Chapter 3

Troubleshooting when a client does not update content

This chapter includes the following topics:

- About troubleshooting content update problems on clients
- About types of content for Symantec Endpoint Protection
- About determining how a client is configured to receive content
- About network connectivity and clients
- About checking the client's connection status
- Making sure that the client can communicate with its content provider
- About determining whether a client is receiving content updates from the management server
- About comparing the content on the client to the content on the management server
- Comparing the content cache
- Using the management console to compare content versions
- Viewing the latest LiveUpdate downloads to the management server
- Checking the LiveUpdate settings on the management server
- Checking the LiveUpdate content policy settings
- About checking the LiveUpdate Settings policy

- Running a manual LiveUpdate session from the management console
- What to do if you still have problems after verifying connectivity and LiveUpdate settings

About troubleshooting content update problems on clients

LiveUpdate is the name of the technology that checks for and distributes definitions and content updates to Symantec Endpoint Protection client computers.

The client can receive content updates through several different LiveUpdate content providers. These providers include the management server itself, a group update provider, an internal LiveUpdate server, Symantec LiveUpdate, or a third-party management tool.

If you suspect that a client does not receive content updates, you can perform several troubleshooting actions.

Table 3-1 describes the troubleshooting actions and where to find information about how to perform those actions.

Table 3-1 Troubleshooting actions

Action	Where to find the information
Determine how the client is configured to receive content.	See "About determining how a client is configured to receive content" on page 34.
Check the client's connection status.	See "About checking the client's connection status" on page 35.
Make sure that the client can ping its content provider or that the client is connected to the Internet.	See "Making sure that the client can communicate with its content provider" on page 36.
Determine whether or not a client is receiving updates from the management server.	See "About determining whether a client is receiving content updates from the management server" on page 37.
Check the LiveUpdate settings that are configured on the management server.	See "Checking the LiveUpdate settings on the management server" on page 41.
Check the client's LiveUpdate policy settings.	See "About checking the LiveUpdate Settings policy" on page 42. See "Checking the LiveUpdate content policy settings" on page 41.

Table 3-1 Troubleshooting actions *(continued)*

Action	Where to find the information
Run a manual LiveUpdate session from the management console to see if the client receives updated content.	See "Running a manual LiveUpdate session from the management console" on page 42.
If you still have problems, check the LiveUpdate logs on the client and the management server. You can also use a debugging tool.	See "What to do if you still have problems after verifying connectivity and LiveUpdate settings" on page 43.

About types of content for Symantec Endpoint Protection

Symantec Endpoint Protection uses several different types of content.

Table 3-2 describes the content types.

Table 3-2 Content types

Content type	Description
Antivirus and antispyware definitions	These definitions protect against virus and spyware attacks.
Decomposer signatures	These signatures support the Antivirus and Antispyware protection engine, and are used to decompose and read the data that is stored in various formats.
TruScan™ proactive threat scan heuristic signatures	These signatures protect against zero-day attack threats.
TruScan proactive threat scan commercial application list	These application lists are the legitimate commercial applications that have generated false positives in the past.
Intrusion Prevention signatures	These signatures protect against network threats and support the intrusion prevention and detection engines.
Submission Control signatures	These signatures control the flow of submissions to Symantec Security Response.

About determining how a client is configured to receive content

Clients can receive content through several different methods.

You can determine how a client is configured to receive content in the following ways:

- View the server settings in the client's LiveUpdate policy in the management console.
- Examine the LiveUpdate registry keys on the client.

Note: For more information about how you can view the server settings in the client's LiveUpdate policy, see the *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control.*

On the client, look in the registry under HKEY_LOCAL_MACHINE\Software\Symantec\Symantec Endpoint Protection\LiveUpdate.

Check the settings for the following keys:

- UseLiveUpdateServer
  If this key is set to 1, the client uses an internal LiveUpdate server or Symantec LiveUpdate directly.
- UseManagementServer
  If this key is set to 1, the client uses the management server.
- UseMasterClient
  If this key is set to 1, the client uses a group update provider.

If you have not already set up clients to receive content, you should consider the requirements of your security network.

See “Deciding how to update content” on page 64.

About network connectivity and clients

If a client does not receive content updates, you should first check whether or not there is a connectivity problem. Clients can receive content through several different methods. You should check to make sure that the client does not have any connectivity problems that prevent content updates.

See “About checking the communication between the management server and the client” on page 16.

Table 3-3 Workflow for troubleshooting connectivity

How the client receives content	What to check
Symantec Endpoint Protection Manager	Check the following item: ■ Connectivity between the client and the management server.
Group update provider	Check the following items: ■ Connectivity between the client and the group update provider. ■ Connectivity between the group update provider and the management server.
Internal LiveUpdate server	Check the following items: ■ Connectivity between the client and the internal LiveUpdate server. ■ Connectivity between the internal LiveUpdate server and Symantec LiveUpdate.
Directly to Symantec LiveUpdate	Check the following items: ■ Make sure that the client can access the Internet. ■ Check the LiveUpdate schedule in the client's policy.
Third-party management tools, such as Microsoft SMS or IBM Tivoli	Consult your vendor's user documentation and the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control*. Using a third-party management tool requires specific directory structures. Contact Symantec Technical Support if you have problems.

About checking the client's connection status

To receive updates, the client must be connected to its content provider. You should check that the client is connected to its management server. In the management console, on the Clients page, under View Clients, select the group in which the client belongs. Look on the Clients tab.

Both of the following statements should be true:

- The client appears in the list.

- The icon next to the client name shows a green dot.

In some cases, the client icon may not appear with a green dot, but the client still has connectivity to the management server.

See "About checking the communication between the management server and the client" on page 16.

Typically if the client loses connectivity to its management server, it cannot receive updates. In certain configurations, the client might be able to receive updates from Symantec LiveUpdate or an internal LiveUpdate server.

On the client computer you can also verify connectivity and the current content definitions dates.

You can check the following items on the client computer:

- In the notification area on the client computer, there should be a yellow shield icon with a green dot.
- In the client main window, the current content definition dates are listed.

In addition to connectivity problems, there are other situations that might prevent the client from receiving updates. These include the following situations:

- The server or the client computer does not contain the server group root certificate.
- The Windows firewall settings interfere with communication.
- The client firewall settings interfere with communication.

For more information about the server group root certificate or the firewall settings, see the *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control*.

Making sure that the client can communicate with its content provider

You should make sure that the client can communicate with its content provider.

If the client uses a group update provider, you should make sure that the group update provider can communicate with the management server.

If the client gets content directly from Symantec LiveUpdate, make sure that the client can access the Internet.

If you use an internal LiveUpdate server, make sure the following is true:

- The management server has connectivity to the internal LiveUpdate server.
- The internal LiveUpdate server has connectivity to Symantec LiveUpdate.

For more information about internal LiveUpdate servers, see the *LiveUpdate Administrator's Guide*.

If the client cannot ping the management server, check for any network problems. Verify the DNS service for the client and check its routing path.

See "About checking the communication between the management server and the client" on page 16.

To make sure that the client can communicate with a management server or group update provider

◆ On the client, open a command prompt and ping the management server or group update provider. For example, type:

  ping *name*

  where *name* is the computer name of the management server or group update provider. The command should return the server or group update provider's correct IP address.

About determining whether a client is receiving content updates from the management server

You can check to see which computers might not currently receive updates from the management server.

You can perform the following checks:

- Run the Computer Status quick report Computers Not Checked into Server to see online status. You can configure and run a custom version of this report to look at the computers in a particular group or site. Clients cannot receive content if they lose connectivity to the management server (unless they are configured to pull updates from Symantec LiveUpdate).
- View the Computer Status log, which contains the client computer's IP address and the time of the last check-in. It also shows the last definitions date.

The only way to be sure whether or not clients are receiving updates is to check the content version on the management server. You should then compare it to the version on the client.

See "About comparing the content on the client to the content on the management server" on page 38.

About comparing the content on the client to the content on the management server

You can compare the version of content on the client to the version on the management server in the following ways:

- Check the content cache on the client computer and compare it to the content cache on the management server. You can use this method if you want to check the content on a few clients.
  See "Comparing the content cache" on page 38.
- In the management console, run reports to check the content versions on the clients. In Reports, under Quick Reports, you can select the Computer Status report type. Then run the Virus Definitions Distribution and Protection Content Versions reports. Then check the LiveUpdate downloads status on the management server. Use this method if you want to check the content on multiple clients.
  See "Using the management console to compare content versions" on page 39.

If the content on the client does not match the content on the management server, you should check the client's connectivity to the network. You should also check the client's communication with the management server.

Comparing the content cache

You can check the content cache on the client computer and compare it to the content on the management server.

If the client receives content updates from the management server, subfolders are created on the client in the product folder. The subfolders have dates such as 70827034. The subfolder names should be the same on the client and the server if the client is receiving updates from the management server.

Note: If the client receives content directly from LiveUpdate, the content is not cached in the product folder location.

To compare the content cache

1. On the client computer, navigate to the following folder:

   \Program Files\Symantec\Symantec Endpoint Protection\ContentCache

2. On the management server, navigate to the content folder. Typically you can find the folder in the following location:

   \Program Files\Symantec\Symantec Endpoint Protection Manager\Inetpub\content

3. Compare the folders in the client content cache to the folders on the management server. Then compare the subfolders. The folders should correspond if the client is receiving content from the management server.

   In the management server content directory, you can view the ContentInfo.txt file, which lists the name of the content types and the folders.

Using the management console to compare content versions

You can view information about the latest content on the client by running reports in the management console. You can run the Computer Status Virus Definition Distribution report to see the virus definition versions on the clients. For other content, you can run the Computer Status Protection Content Versions report. These reports show the latest content versions that run on your clients.

For more information about reports, see the *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control.*

In the management console, you can see the latest content by checking the latest LiveUpdate downloads. You can compare the revision that is listed in the Show LiveUpdate Downloads dialog box to the content versions that appear in the report.

See “Viewing the latest LiveUpdate downloads to the management server” on page 40.

To use the management console to compare content versions

1. In the management console, on the Reports page, click **Quick Reports**.
2. On the Quick Reports tab, in the Report type drop-down list, click **Computer Status**.
3. In the Select a report drop-down list, click **Virus Definitions Distribution**.
4. Select any filter settings that you want, and then click **Create Report**.

   Keep the report open.

5 In the management console, navigate to the Admin page and select the site.

6 Under Tasks, click **Show LiveUpdate Downloads**.

7 Compare the antivirus and antispyware definitions revision to the revision that is listed in the report. If the client is receiving updates, the revisions should match.

Viewing the latest LiveUpdate downloads to the management server

Clients might not receive LiveUpdate content if the management server does not receive updates. The management server receives updates directly from Symantec LiveUpdate (the default method) or from an internal LiveUpdate server that pulls content from Symantec LiveUpdate.

In the management console, you can view the most recent LiveUpdate downloads to the management server.

The server receives updates from Symantec LiveUpdate at certain intervals. The default interval is every four hours. You can configure the download schedule by using the Site Properties dialog on the Admin tab in the management console.

If the content that appears in the list on the server is older than you expect, check the LiveUpdate log.

See “Viewing the LiveUpdate log” on page 43.

You should also check the connection to Symantec LiveUpdate or the internal LiveUpdate server.

After you view the latest LiveUpdate downloads, you can compare the content to the content on the clients.

See “Using the management console to compare content versions” on page 39.

To view the latest LiveUpdate downloads to the management server

1 In the management console, on the Admin page, click **Servers**.

2 Under View Servers, select the site to which the client belongs.

3 Under Tasks, click **Show LiveUpdate Downloads**.

Checking the LiveUpdate settings on the management server

The LiveUpdate settings for the site to which the client belongs must match the settings in the client's LiveUpdate content policy.

To check LiveUpdate settings on the management server

1. In the management console, on the Admin page, click **Servers**.
2. Under View Servers, select the site to which the client belongs.
3. Under Tasks, click **Edit Site Properties**.
4. On the LiveUpdate tab, under Content Types to Download, make sure the content list matches the list in the LiveUpdate Content Policy.

Checking the LiveUpdate content policy settings

Make sure that the following settings correspond:

- The content types that you specify in the Site Properties dialog box in the management console.
- The content types that you specify in the LiveUpdate policy that the client uses.

A client does not receive a content update if the following statements are true:

- The content type is not selected in the Site Properties dialog box.
- The content type is selected in the LiveUpdate policy.

Typically, the LiveUpdate content policy should be set to use the latest available content. If the policy is configured to use a specific revision, the content does not get updated with any other revision.

To check the LiveUpdate content policy settings

1. In the management console, click **Policies**.
2. Under View Policies, click **LiveUpdate**
3. On the LiveUpdate Content tab, select the policy that the client uses.
4. Under Tasks, click **Edit the Policy**.
5. On the Security Definitions page, check the following:
   - The selected content types should match the content types that you specified in the Site Properties dialog box.

- Typically, you should select the **Use latest available** option for each content type.
  If there is a revision selected instead, the client receives only that version of the content.

About checking the LiveUpdate Settings policy

You should check settings in the LiveUpdate Settings policy to make sure that the policy settings do not cause a problem with updates.

Table 3-4 describes the LiveUpdate Settings policy settings.

Table 3-4 LiveUpdate Settings policy settings

Policy setting	What to consider
Use the default management server	This setting must be checked so that clients can use the management server to receive content updates. If you uncheck this setting, clients cannot get updates from the Symantec Endpoint Protection Manager.
Use a LiveUpdate server	If you enable this option, you should use the LiveUpdate Settings Policy to configure a schedule. If you do not configure a schedule, the client can get content only from a manual LiveUpdate session.

Running a manual LiveUpdate session from the management console

You can run a manual LiveUpdate session from the management server. You can use the Update Content command from the Clients tab or you can use the logs in the Monitors page.

For more information about how to run a manual LiveUpdate session, see the *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control*.

When you run a manual LiveUpdate session, the client receives content from Symantec LiveUpdate; it does not receive content from the management server.

Note: After you run a manual LiveUpdate session, you should wait for up to two minutes. The Symantec Endpoint Protection client performs content validation checks. After two minutes, you can check to see if the command successfully updated the client. Note that the management console automatically refreshes.

You can also run a manual LiveUpdate session directly from the client if the LiveUpdate policy permits the client to run a manual session.

For more information, see the *Client Guide for Symantec Endpoint Protection and Symantec Network Access Control*.

To run a manual LiveUpdate session from the management console

1. In the management console, on the Clients page, under View Clients, right-click the client or the group.
2. Do one of the following actions:
   - Click **Run Command on Clients > Update Content**.
   - Click **Run Command on Group > Update Content**.
3. In the Update Content message box, click **Yes**.
4. In the message box, click **OK**.

What to do if you still have problems after verifying connectivity and LiveUpdate settings

You should look at the LiveUpdate log on the management server and the client. You can also create a log of the sylink communications between the client and the management server. You can use a text application, such as Notepad, to open the log files. You can also use a shareware tool, such as DebugView, to look at the debug output messages.

Viewing the LiveUpdate log

You can view the LiveUpdate log on the client and the management server.

To view the LiveUpdate log

1 On the client computer or the management server, locate the log in the LiveUpdate directory.

For example, go to the following location:

\Documents and Settings\All Users\Application Data\Symantec\LiveUpdate\Log.LiveUpdate

2 Look for the following message in the log:

```
Progress Update: DOWNLOAD_FILE_START: URL: <url>/zip
```

The URL should match the expected address of the LiveUpdate server.

If the client or the management server failed to connect to the LiveUpdate server, you see an error similar to the following:

```
Progress Update: HOST_SELECTION_ERROR:
```

Messages also appear about possible reasons for the failure.

About viewing the debug log on the client

Look at the debug log on the client. You can look at the debug log in the following ways:

- In the client, on the Help and Support menu, in the Troubleshooting dialog box, you can click Edit Debug Log Settings and type a name for the log. You can then click View Log.
- You can also use the following registry key to turn on debugging in the client: HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\smc_debuglog_on

Creating a sylink log

The client and the management server use Sylink.xml to communicate. You can dump all sylink communication messages to a log file on the client computer.

To create a sylink log

1 On the client computer, in the registry, under HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SYLINK\SyLink, add a string value that is called DumpSylink.

2 You should specify the location for the dump file (such as c:\sylink.log).

You can then view the Sylink.log file on the client computer.

About using the DebugView tool

DebugView is a shareware tool that you can use to view the strings that are written to a debug output stream on the client. The binary LiveUpdate file, Sescu.exe, handles the content updates but does not write its own log file. You can view debug output messages by using the DebugView tool.

When you run the tool, look for the following messages:

- QueryContentSeqData
- ApplyContent

If these messages appear in the output, the client receives content from a management server, a group update provider, or a third-party management tool.

You can download the tool from the following URL:

http://www.microsoft.com/technet/sysinternals/utilities/debugview.mspx

Setting up and managing mobile clients and remote clients

This chapter includes the following topics:

- About mobile clients and remote clients
- Setting up groups and locations
- About common mobile client and remote client scenarios
- About location awareness criteria
- Strengthening your security policies for remote clients
- About client notifications
- Customizing client log management settings
- Managing load balancing and roaming
- Monitoring remote clients

About mobile clients and remote clients

Today's workforce is no longer tied to a single location, because employees increasingly work remotely or from multiple locations. This situation has created a type of client that is distinct from other clients in your network. A mobile client is defined as a client that moves physically from location to location. Employees who travel in the course of their job typically use these client computers. Such client computers connect to the network intermittently and are often in an unknown state. Their users typically log in through a virtual private Network (VPN). Remote clients are defined as clients that always connect from the same location, but they are not physically located within the corporate network. Typical examples of remote clients are employees who work from their homes and log in through a VPN. Both types of clients are subject to similar risks and should be treated similarly.

Mobile clients and remote clients are more at risk than the clients that always reside within your corporate network. Mobile clients and remote clients are outside the safety of your corporate defenses. The management of these clients places an extra burden on administrators to maintain the safety of the network and its data.

You might have mobile clients and remote clients in your network for a number of different reasons, and they might exhibit different patterns of usage. For example, you may have some internal computers that periodically move outside your corporate environment. You may have some sales personnel whose computers are never inside the network. You may have some client computers that need to connect to your network but are completely outside your administrative control. For example, you may allow customers, contractors, vendors, or business partners limited access to your network. You may have employees who connect to the corporate network using their own personal computers.

Some mobile users and remote users might have a less stringent attitude toward Internet browsing than you would like, and therefore exhibit riskier behavior. The mobile users and remote users that do not work directly for your business may not be as educated about computer security as your employees. For example, they might be more likely to open email messages or attachments from unknown sources while on your network. They may be more likely to use weak passwords. Mobile users and remote users in general may be more likely to make unauthorized changes or to customize their computers. For example, they may be more likely to download and use an application that has not been approved for corporate use. Mobile users and remote users may be so focused on doing their work as quickly as possible that they fail to think about computer security.

Because it is a best practice to treat both remote clients and mobile clients similarly, we refer to both types of clients as remote clients.

Setting up groups and locations

After you determine the types of remote clients that you have, you should consider what security restrictions to apply. Should the same restrictions be applied to all your remote clients? The answer to this question determines how many groups and locations you need to create so that you can most easily manage them. Some Symantec Endpoint Protection security settings are assigned on a group basis and some are location-specific. A best practice is to enable location awareness to manage remote clients.

The hierarchical organizational structure of Symantec Endpoint Protection is based on groups, users, and computers. You add locations within a group when you need to customize any settings that are location-specific.

The condition that you use to define a location can be based on a number of criteria, including the following items:

- IP addresses
- WINS server addresses
- DHCP server addresses
- DNS server addresses
- Network connections
- Trusted Platform Modules
- Other criteria

If you intend to use the type of network connection to identify a location, you need to know what type it is. For example, the network connection may be a connection to the Symantec Endpoint Protection Manager, dial-up networking, or a particular kind of VPN server.

When you create a location, it applies to the group you created it for and any subgroups that inherit from that group. A best practice is to create the locations that any client can use at the Global group level. Locations that are specific to a particular group should be created at the subgroup level.

The smaller the number of groups and locations that you create, the simpler it is to manage your security policies and settings. The number of different security settings, log-related settings, communications settings, and policies that you want to have determines how many groups and locations you need.

Some of the configuration options that you may want to customize for your remote clients are location-independent. These options are either inherited from the parent group or are set independently for a group. If you create a single group to contain all remote clients, then these location-independent settings are the same for all those clients.

The following settings are location-independent:

- Custom intrusion prevention signatures
- System lockdown settings
- Network application monitoring settings

- LiveUpdate content policy settings
- Client log settings
- Client-server communications settings
- General security-related settings, including location awareness and Tamper Protection

To customize any of these location-independent settings, such as how client logs are handled, you need to create separate groups.

For information about how to set up groups, see the *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control*.

For information about the options, see the console context-sensitive Help.

Note: To customize the settings for any group other than the Global group, you must also turn off inheritance.

Some of the configuration options that you might want to customize for your remote clients are specific to the location.

The following settings are specific to locations:

- The control mode that the clients run in.
- The management server list that the clients use.
- The download mode that the clients run in.
- Whether or not you want a list of all the applications that are executed on clients to be collected and sent to the management server.
- The heartbeat interval that clients use for downloads.

As a best practice, you should not allow users to turn off the following protections:

- Auto-Protect
- TruScan proactive threat scans
- Tamper Protection
- The firewall rules that you have created

For information about how to set up locations, see the *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control*.

For information about the options you can use to set up locations, see the console context-sensitive Help.

About common mobile client and remote client scenarios

If you have remote clients, in the simplest case, it is a common practice to use the Global group and three locations. This is Scenario One.

To manage the security of the clients in this scenario, you can create the following locations under the Global group to use:

- Office clients that log on in the office.
- The remote clients that log on to the corporate network remotely over a VPN.
- The remote clients that log on to the Internet remotely, but not over a VPN.

Because the remote location with no VPN connection is the least secure, it is a best practice to always make this location the default location.

Note: If you turn off Global group inheritance and then you add groups, the added groups do not inherit the locations that you set up for the Global group.

In Scenario Two, you use the same two remote locations above, but add two office locations, for a total of four locations. You would have the following office locations in Scenario Two:

- Clients in the office that log on over an Ethernet connection.
- Clients in the office that log on over a wireless connection.

It simplifies management to leave all clients under the default Server control mode. If you want granular control over what your users can and cannot do, an experienced administrator can use Mixed control. A Mixed control setting gives the end user some control over security settings, but you can override their changes, if necessary. Client control allows users a wider latitude in what they can do and so constitutes a greater risk to network security.

We suggest that you use Client control only in the following situations:

- If your users are knowledgeable about computer security.
- If you have a compelling reason to use it.

About location awareness criteria

Location awareness helps to protect your network. With location awareness, you set criteria (conditions) to trigger a switch to a new location with different security settings whenever the conditions are met. The best security policies to apply typically depend on where the client is located when it connects to the network. When you have location awareness enabled, it ensures that the strictest security policy is assigned to a client when it is needed. A best practice is to enable location awareness when you manage remote clients.

On the console, you add a set of conditions to each group's location that automatically selects the correct security policy for a user's environment. These conditions are based on information, such as the network settings of the computer from which the request for network access was initiated. An IP address, a MAC address, or the address of a directory server can also function as condition.

For information about how to enable and use location awareness, see the *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control*.

Setting up Scenario One location awareness conditions

The following suggestions represent the best practices for Scenario One.

To set up the office location for the clients located in the office

1. On the Clients page, select the group that you want to add a location for.
2. Under Tasks, click **Add Location**.
3. In the Add Location Wizard, click **Next**.
4. Type a name for the location and optionally, add a description of it, and then click **Next**.
5. In the list box, click **Client can connect to management server** from the list, and then click **Next**.
6. Click **Finish**.
7. Under Tasks, click **Manage locations**, and then select the location you created.
8. Click **Add**, and then click **Criteria with AND relationship**.
9. In the Specify Location Criteria dialog box, from the Type list, click **Network Connection Type**.
10. Click **If the client computer does not use the network connection type specified below**.
11. In the bottom list box, select the name of the VPN client that your organization uses, and then click **OK**.
12. Click **OK** to exit the Manage Locations dialog box.

To set up the remote location for the clients logging in over a VPN

1 On the Clients page, select the group that you want to add a location for.

2 Under Tasks, click **Add Location**.

3 In the Add Location Wizard, click **Next**.

4 Type a name for the location and optionally, add a description of it, and then click **Next**.

5 In the list box, click **Network connection type**.

6 In the Connection Type list box, select the name of the VPN client that your organization uses, and then click **Next**.

7 Click **Finish**.

8 Click **OK**.

To set up the remote location for the clients not logging in over a VPN

1 On the Clients page, select the group that you want to add a location for.

2 Under Tasks, click **Add Location**.

3 In the Add Location Wizard, click **Next**.

4 Type a name for the location, optionally add a description of it, and then click **Next**.

5 In the list box, leave **No specific condition**, and then click **Next**.

By using these settings, this location's policies, which should be the strictest and most secure, are used as the default location policies.

6 Click **Finish**.

Setting up Scenario Two location awareness conditions

In the Scenario Two, you use the same two remote locations with the same conditions that you used for Scenario One. Instead of the single office location, you use two office locations, one for Ethernet clients and one for wireless connection clients.

See “Setting up Scenario One location awareness conditions” on page 52.

Note: You may have some clients that use Ethernet connections in the office while other clients in the office use wireless connections. For this reason, you set the last condition in the procedure for wireless clients in the office. This condition lets you create an Ethernet location Firewall policy rule to block all wireless traffic when both kinds of connections are used simultaneously.

To set up the office location for the clients that are logged on over Ethernet

1. On the Clients page, select the group that you want to add a location for.
2. Under Tasks, click **Add Location**.
3. In the Add Location Wizard, click **Next**.
4. Type a name for the location, optionally add a description of it, and then click **Next**.
5. In the list box, select **Client can connect to management server**, and then click **Next**.
6. Click **Finish**.
7. Click **OK**.
8. Under Tasks, click **Manage locations**, and then select the location you created.
9. Click **Add**, and then select **Criteria with AND relationship**.
10. In the Specify Location Criteria dialog box, from the Type list, click **Network Connection Type**.
11. Click **If the client computer does not use the network connection type specified below**.
12. In the bottom list box, select the name of the VPN client that your organization uses, and then click **OK**.
13. Click **Add** and then click **Criteria with AND relationship**.
14. In the Specify Location Criteria dialog box, from the Type list, click **Network Connection Type**.
15. Click **If the client computer uses the network connection type specified below**.
16. In the bottom list box, select **Ethernet**, and then click **OK**.
17. Click **OK** to exit the Manage Locations dialog box.

To set up the office location for the clients that are logged on over a wireless connection

1. On the Clients page, select the group that you want to add a location for.
2. Under Tasks, click **Add location**.
3. In the Add Location Wizard, click **Next**.
4. Type a name for the location, optionally add a description of it, and then click **Next**.

5 In the list box, click **Client can connect to management server**, and then click **Next**.

6 Click **Finish**.

7 Click **OK**.

8 Under Tasks, click **Manage locations**, and then select the location that you created.

9 Click **Add**, and then click **Criteria with AND relationship**.

10 In the Specify Location Criteria dialog box, from the Type list, click **Network Connection Type**.

11 Click **If the client computer does not use the network connection type specified below**.

12 In the bottom list box, select the name of the VPN client that your organization uses, and then click **OK**.

13 Click **Add**, and then click **Criteria with AND relationship**.

14 In the Specify Location Criteria dialog box, from the Type list, click **Network Connection Type**.

15 Click **If the client computer does not use the network connection type specified below**.

16 In the bottom list box, click **Ethernet**, and then click **OK**.

17 Click **Add**, and then click **Criteria with AND relationship**.

18 In the Specify Location Criteria dialog box, from the Type list, click **Network Connection Type**.

19 Click **If the client computer uses the network connection type specified below** .

20 In the bottom list box, click **Wireless**, and then click **OK**.

21 Click **OK** to exit the Manage Locations dialog box.

Strengthening your security policies for remote clients

When you manage remote users, you essentially take some form of one of the following positions:

- Leave the default policies in place, so that you do not impede remote users in the use of their computers.

- Strengthen your default security policies to provide more protection for your network, even if it restricts what remote users can do.

In most situations, the best practice is to strengthen your security policies for remote clients.

Policies may be created as shared or unshared and assigned either to groups or to locations. A shared policy is one that applies to any group and location and can be inherited. A non-shared policy is one that only applies to a specific location in a group. Typically, it is considered a best practice to create shared policies because it makes it easier to change policies in multiple groups and locations. But, when you need unique location-specific policies, you need to create them as non-shared policies or convert them to non-shared policies.

About best practices settings for a Firewall Policy

A best practice for a Firewall Policy is to assign the strictest security policies to clients that log on remotely without using a VPN. The following settings are recommended as best practice for the Firewall Policy for the remote location where users log on without a VPN:

- You can enable NetBIOS protection in the policy's Traffic Settings.

Note: Do not enable NetBIOS protection for the location where a remote client is logged on to the corporate network through a VPN. This rule is appropriate only when remote clients are connected to the Internet, not to the corporate network.

- To increase security, you can also block all local TCP traffic on the NetBIOS ports 135, 139, and 445.

The following settings are recommended as best practice for the Firewall Policy for the remote location where users log on through a VPN:

- Leave as-is all the rules that block traffic on all adapters. Do not change those rules.
- Leave as-is the rule that allows VPN traffic on all adapters. Do not change that rule.
- For all rules that use the action Allow, change the Adapter column from All Adapters to the name of the VPN adapter that you use.
- Enable the rule that blocks all other traffic.

Note: You need to make the last three changes if you want to avoid the possibility of split tunneling through the VPN.

As best practice for the Firewall policies for the office locations where users log on through Ethernet or wireless connections, use your default Firewall Policy. For the wireless connection, ensure that the rule to allow wireless EAPOL is enabled. 802.1x uses the Extensible Authentication Protocol over LAN (EAPOL) for connection authentication.

About best practices settings for an Antivirus and Antispyware Policy

The following TruScan proactive threat scan settings are recommended as best practice for your Antivirus and Antispyware Policy for the remote location where users log in without a VPN:

- Set the TruScan proactive threat scan sensitivity level for Trojan horses and worms to a high sensitivity level.
- Set the action that is taken when Trojan horses or worms are detected to Quarantine or Terminate.
- Set the sensitivity level for keyloggers to High.
- Set the action that is taken when keyloggers are detected to Quarantine or Terminate.
- If you set actions to Terminate, change the notifications setting to prompt users before processes and services are stopped.
- If you do not typically run a proactive threat scan whenever a new application is started, you should run a scan for both remote locations.

See "About managing TruScan proactive threat scans" on page 71.

About best practices settings for a LiveUpdate Policy

If you maintain strict control over Symantec content and product updates for your clients, you should consider changing your LiveUpdate Policy for your remote clients.

For the remote location where users log in without a VPN, we suggest the following best practices:

- Change the LiveUpdate Policy setting to use the default Symantec LiveUpdate server. This setting allows the remote clients to update any time they connect to the Internet.

- Change the LiveUpdate Scheduling frequency setting to one hour to make it more likely that clients update their protection when they connect to the Internet.

For all other locations, it is a best practice to use the Symantec Endpoint Protection Manager to distribute product software and content updates. An update package that is distributed through the management console are incremental rather than a complete package. The update packages are smaller than the packages that are downloaded directly from the Symantec LiveUpdate server.

About best practices settings for an Application Control Policy

You may also want to create an Application Control Policy to block certain applications or to create one that allows only certain applications. If you assign an Application Control Policy that blocks or allows, you can exercise stricter control over your mobile clients.

About client notifications

For your remote clients that are not logged on over VPN, it is a best practice to turn on client notifications for the following situations:

- Intrusion detections
  You can turn on these notifications by using the location-specific Server or Mixed control mode option in the Client User Interface Control Settings.
- Antivirus and antispyware risks
  You can turn on these notifications in the Antivirus and Antispyware policy.

Turning on notifications helps to ensure that remote users are aware when a security problem occurs.

Customizing client log management settings

You can customize some of the log management settings for remote clients, especially if clients are offline for many days. You can make one or more of the following changes to reduce the bandwidth usage and the load on your management servers:

- Change the client log settings so that clients do not upload their logs to the management server.
- Change the client log settings to upload only the client Security logs.
- Change the client log settings to retain logs for a longer period.

- In your location-specific Antivirus and Antispyware policy, filter the log events to upload only a few important events. You might want to see only definition update information, for example, or only side effect repair failures.
- If you want to see antivirus and antispyware event data from these clients' logs, change the log retention time to a longer period.

Note: Some client log settings are group-specific and some are set in the Antivirus and Antispyware policy, which can be applied to a location. If you want all remote client log and office client log settings to differ, you must use groups instead of locations to manage remote clients.

Managing load balancing and roaming

If you have multiple sites, you can use DNS along with a custom management server list for your remote clients.

You can take the following steps to set up your network for roaming clients and to balance the load on your servers:

- Configure your DNS servers as appropriate for the sites in your organization. Be sure to use the same domain name on all DNS servers. Each DNS server should be configured with the IP address of the closest management server.
- Use Symantec Endpoint Protection Manager to construct a custom management server list for your remote clients. This list should contain the fully qualified domain name of your DNS servers as its only entry. Assign this list to the group that contains your locations.

For information about how to create and assign a management server list, see the *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control*.

Monitoring remote clients

Notifications and logs are essential to maintain a secure environment. In general, you should monitor your remote clients in the same way that you monitor your other clients. You should always check to see that your protections are up to date and that your network is not currently under attack. If your network is under attack, then you want to find out who is behind the attack and how they attacked.

Even if you restrict some of the client log data that mobile clients upload, you can check the following displays:

- On the Home page, see Virus Definitions Distribution and Intrusion Prevention Signatures to see that content is up to date.
- On the Home page, see Status Summary to see if any of the protections are off on computers.
- On the Home page, see Risks Per Hour, Attacks Per Hour, and Infections Per Hour to see if your network is under attack.
- If the network is under attack, on the Monitors Summary tab, see the Network Threat Protection summary, which shows the top targets and source of attacks.

The data on the Home page in the following displays represents only the clients that connected in the past 12 hours or 24 hours:

- Virus Definitions Distribution
- Intrusion Prevention Signatures
- Status Summary

Your Home page preference settings determine the time period for which Symantec Endpoint Protection Manager displays data. If you have many clients that are frequently offline, your best monitoring option is to go to the logs and reports. In the logs and reports, filter the data to include offline clients.

Chapter 5

Symantec Endpoint Protection organization: Servers, sites, and Group Update Providers

This chapter includes the following topics:

- About the Symantec Endpoint Protection management topology
- Organizational factors to consider
- Deciding to create one site or multiple sites
- Deciding how to update content
- About high availability and failover
- About load balancing and roaming

About the Symantec Endpoint Protection management topology

A site is the primary unit of organization in the Symantec Endpoint Protection management topology. A site consists of one database and one or more management servers, and clients. Site information can be replicated across multiple sites by using the management servers.

A management server runs the Symantec Endpoint Protection software that is used to manage clients, handle policies, and to monitor and report about endpoint security. The interface to the management server is the Symantec Endpoint Protection Manager Console. The console is installed with the management server. It can also be installed and used remotely on any computer with a network connection to the management server.

You can install the Symantec Endpoint Protection embedded Sybase database, which supports up to 1,000 clients, or you can use an external MS-SQL database. An external MS-SQL database can support data for many more clients. You can place your management servers and database servers in different locations. You should be aware, however, that this situation can cause performance issues in some situations. You should ensure that you have sufficient bandwidth to support this scenario. In addition, the management server and the database should be connected over a LAN, not over a WAN.

Use the following size guidelines as best practices recommendations:

- Install as few sites as possible, up to a maximum of 20 sites.
- Connect up to ten management servers to a database.
- Connect up to 50,000 clients to a management server.

We recommend that you do not exceed these guidelines under typical circumstances.

If you have one management server and more than 45-50,000 clients, but do not want to or cannot install another server, the following strategy may help. The strategy is to add internal LiveUpdate servers and Group Update Providers to handle content updates. This strategy can help to increase the number of clients that one management server can handle.

See “Deciding how to update content” on page 64.

Note: All suggestions are intended as general guidelines only. You should modify them as necessary to fit the needs of your organization.

Organizational factors to consider

Your network architecture is the single most important thing that you should consider when designing your Symantec Endpoint Protection management structure. The following specific factors affect the number of sites, management servers, and content update servers or computers that you should use:

- The number of clients in your organization.
- The number of geographic locations in your organization and the type of communications links between them.

- The number of functional divisions or administrative groups in your organization.
- The number of datacenters in your organization.
- How frequently you want to update the security content.
- How much client log data you need to retain, how long you need to retain it, and where it should be stored.
- Any miscellaneous corporate management and IT security management considerations that are unique to your organization

Deciding to create one site or multiple sites

A small enterprise is defined here as one that has fewer than 100 clients. A medium enterprise has fewer than 1000 clients, and a large enterprise is an organization that contains more than 1000 clients.

A majority of small and medium size businesses need only a single site for central management of their network security. Since there is only one database, all data is centrally located and available. Even a large business with a single geographic location and fewer than 45-50,000 clients typically only needs one site. If you need failover capability for your management server, you can install two or more management servers. To handle additional clients, all you need to add are more management servers.

If you must have failover or high availability for your database as well, you need to cluster your databases.

Enterprises that are too complex to manage centrally can use a distributed management architecture with multiple sites. You may want to add a second site for a number of reasons. A common reason is that you have a slow WAN link between two physical locations and you want to minimize the traffic across the link. If you set up a second site with its own management server, you avoid all Symantec Endpoint Protection client-server traffic over that slow link. Another reason to add a second site is that you have more than one datacenter location in your organization. A best practice is to set up one Symantec Endpoint Protection site for each datacenter. An additional reason to add multiple sites is if you must have true high availability for your security network and security-related data.

A best practice is not to install more than 20 Symantec Endpoint Protection sites.

The following designs are common in multi-site environments:

- Distributed design

  With two sites or a few sites, each site replicates groups and policies, but logs and content are not replicated. In this model, administrators use the console to connect to a manager in the remote site to see the reports for that site. We recommend this design when you do not have a critical need to access remote data.

- Centralized logging design

  In this design, all logs are forwarded from the other sites to a central site. The central site acts as the repository for the logs from all other sites. We recommend this design when you need centralized reporting.

  A typical client stores approximately a maximum of 800 KB of entries per day in the database if all logs are uploaded to the management server. This number of entries amounts to 288 MB per client per year. To reduce this amount, consider forwarding only a few logs to your management servers, focused on security incident events. Full client logs remain available on the client when you need them to debug problems or for forensic examinations. In large organizations, you should consider the amount of storage space before you decide to forward extensive traffic data from the client firewalls.
- High availability design

  If you must have failover or high availability for your security network, you must install multiple sites and also cluster your databases.

Deciding how to update content

The default method for content and product updates is to have the management server get updates from the Symantec LiveUpdate server. After the management server gets the updates, it provides those updates to its managed clients. This method is frequently used in small or medium-sized organizations.

As an alternative, some large enterprises use one or more internal LiveUpdate servers as local update distribution points to increase performance.

Note: The average daily update size for antivirus and antispyware definitions is between 70 KB and 150 KB of data. If a site's clients can download an average update within one hour at the available bandwidth, you probably do not need an internal LiveUpdate server.

The use of an internal LiveUpdate server has the following advantages:

- If you have more than one Symantec product, you can use an internal LiveUpdate server to centrally update all your Symantec products.
- It can increase performance by reducing the traffic over WAN links. Only one server has to connect to the Symantec LiveUpdate server.

- It provides strict control over the definitions versions and content that you distribute.
- It can reduce the number of sites you need to install and configure.
- It lets you retain many different versions of definitions and content.

This method requires that you install an instance of LiveUpdate Administrator on a local server. Note that the LiveUpdate Administrator should not be installed on the same computer as a management server or on the central database server.

You can configure a LiveUpdate Administrator server to continuously check Symantec's LiveUpdate server for new definitions and content. You can configure the management servers in your network to check the internal LiveUpdate servers at a set interval. When you use an internal LiveUpdate server, the more frequently it updates, the smaller the update payload.

For information about setting up an internal LiveUpdate server, see the *LiveUpdate Administrator's Guide*.

In addition to the use of an internal LiveUpdate server or management server, enterprises may want to consider the use of Group Update Providers (GUPs). A GUP is a client that takes content updates from the management server, caches them locally, and distributes them to a group of other clients. A GUP can distribute antivirus and antispyware definitions, IPS signatures, and scan engine updates. It does not cache software update packages. Any client can act as a GUP for a group of clients, but a GUP should not serve more than 100 clients. If a GUP becomes unavailable, clients can automatically download content from the management server. Any desktop or laptop can act as a GUP. However, it is a best practice to use a permanently available computer that has a fixed IP address, such as a local file server.

A GUP reduces the amount of traffic that has to pass over the communications link from the management server to the client. The server downloads its updates only to the GUPs, which then pass the updates along to the other clients in their group.

You may want to consider using GUPs to distribute content updates for the following reasons:

- You have locations with too few clients to warrant the setup of a separate site with its own database and management server.
- Your network architecture is so complex that you might need more than 20 sites. In this situation, you can use GUPs to help to reduce the number of sites that you need for management.

Note that a GUP has the following limitations:

- In general, a GUP should update no more than 100 clients. However, you can monitor performance to see if your environment is sufficient to allow a GUP to support more than 100 clients.
- A GUP updates only definitions and content; it does not download product updates.
- A GUP maintains a cache of up to 100 files. Any files that clients have not requested in the last seven days can be purged. The GUP checks for and purges eligible files once per minute.

  If its cache contains 100 entries, a GUP does not try to download any more files until one of the files is purged. When this situation occurs, a GUP does not serve the update files and the clients must get the content directly from the management server.

For information about the use of GUPs, see the *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control*.

About high availability and failover

To attain high availability for Symantec Endpoint Protection, both the database and the management server must be constantly accessible. If you use an external database, it is a best practice to use high availability clustering for your database or databases. If you use an embedded database, there is no way to provide true high availability for the database.

Symantec Endpoint Protection does, however, support replication configuration for both embedded and Microsoft SQL Server databases. Replication configurations across sites are used for redundancy. All data from one database is periodically replicated in another database. If one database fails, you can still manage and control all clients because the second database contains the same client information.

When you select the items to replicate, you can choose logs and packages. Packages include the updates to virus definitions, client components, and client software. The size of packages and updates can grow to several gigabytes of information if you download updates in multiple languages. Consider the amount of data you replicate when you select these options, along with the bandwidth consumption. One client package is generally 55-65 MB in size when compressed.

To provide management server failover, you need to configure at least two management servers for each site and to use management server lists.

A management server list is a prioritized list of management servers that is assigned to a client group. You can install more management servers than are required to handle your clients to protect against the failure of an individual management server.

You may also want to consider failover for content updates, if you intend to use local servers. All the components that run LiveUpdate can also use a prioritized list of update sources. Your management servers can use a local LiveUpdate server and failover to LiveUpdate servers in other physical locations.

Note: The use of internal LiveUpdate servers, GUPs, and site replication does not provide true high availability, failover, disaster recovery, or load balancing functionality.

About load balancing and roaming

You should not set up multiple sites to try to balance the Symantec Endpoint Protection client load. A better practice is to add management servers to a site and use the management server list feature to automatically distribute the load among them. In a custom management server list, each server is assigned to a priority level. A client that comes onto the network selects a priority one server to connect to at random. If the first server it tries is unavailable and there are other priority one servers in the list, it randomly tries to connect to another. If no priority one servers are available, then the client tries to connect to one of the priority two servers in the list. This method of distributing client connections randomly distributes the client load among your management servers.

The following options are available for load balancing and roaming:

- To provide both load balancing and roaming, enable DNS and put a domain name as the only entry in a custom management server list.
- To provide both load balancing and roaming, enable the Symantec Endpoint Protection location awareness feature and use a custom management server list for each location. Create at least one location for each of your sites.
- Use a hardware device that provides failover or load balancing. Many of these devices also offer a setup for roaming.

Section 2

Best practices for overall security

- Managing TruScan proactive threat scans

Chapter 6

Managing TruScan proactive threat scans

This chapter includes the following topics:

- About managing TruScan proactive threat scans
- Monitoring the scan events
- Creating exceptions for detected processes
- Adjusting scan settings

About managing TruScan proactive threat scans

You can manage TruScan proactive threat scans by using two different implementation approaches. Each approach offers the advantages that relate to your network size, security features, and the workload that your technical support staff shares.

The two implementation approaches include:

- Using the Symantec default settings.
  The Symantec default settings provide a high level of protection and require a low level of management. When you first install the Symantec Endpoint Protection Manager, use the default settings.
- Adjusting the default settings.
  Use the Symantec default settings for the first two to four weeks after you set up the management server. After the initial break-in period during which you become more familiar with the technology, you may want more control. If you use this approach, you adjust the detection action and sensitivity level yourself.

With either approach, you may need to manage the events to determine which detected processes should run on the client computers.

About managing exceptions

Whether or not you use the Symantec default settings, you may need to manage the exceptions for malicious applications, legitimate applications, or both. Even when the scanning engine uses the default settings, the engine occasionally logs legitimate processes instead of ignoring them. You need to create exceptions for legitimate processes so that a scan ignores them. If you adjust the default settings, you must create exceptions so that the scanning engine quarantines or terminates the malicious applications and ignores the legitimate applications.

If you use the Symantec default settings, use the following steps:

- Monitor the scan events.
  Use the TruScan Proactive Threat Scan log to determine which processes are legitimate.
  See "Monitoring the scan events" on page 73.
- Create exceptions for the detected legitimate processes in a Centralized Exceptions Policy.
  After you determine which the legitimate processes are, add them to a Centralized Exceptions Policy and change the detection action to Ignore. The next time the scanning engine runs, it ignores these processes.
  See "Creating exceptions for detected processes" on page 74.

If you do not use the Symantec default settings, use the following steps:

- Adjust the action and the sensitivity level for Trojan horses, worms, and keyloggers.
  See "Adjusting scan settings" on page 76.
- Monitor the scan events.
  Use the TruScan Proactive Threat Scan log to determine which detected processes are legitimate and which detected processes are security risks. After you change a scan setting, you must view the TruScan Proactive Threat Scan log. The log shows you how the change affected the number of legitimate processes and security risks.
  See "Monitoring the scan events" on page 73.
- Create exceptions for the detected legitimate processes and security risks in a Centralized Exceptions Policy.
  After you identify the legitimate processes and security risks, add them to a Centralized Exceptions Policy. As you build up a Centralized Exceptions Policy with a list of the legitimate processes, the rate that the scanning engine logs legitimate processes as potential risks decreases.

See “Creating exceptions for detected processes” on page 74.

Monitoring the scan events

The client collects and uploads the scan's detection results to the management server. The results are saved in the TruScan Proactive Threat Scan log. To determine which processes are legitimate and which are security risks, look at the following columns in the log:

Event	The event type and the action that the client has taken on the process, such as cleaning it or logging it. Look for the following event types: ■ A possible legitimate process is listed as a Potential risk found event. ■ A probable security risk is listed as a Security risk found event.
Application	The process name.
Application type	The type of malware, such as Trojan horse, worm, keyloggers, or commercial application.
File/Path	The path name from where the process was launched.

The Event column tells you immediately whether a detected process is a security risk or a possible legitimate process. However, a potential risk that is found may or may not be a legitimate process, and a security risk that is found may or may not be a malicious process. Therefore, you need to look at the Application type and File/Path columns for more information. For example, you might recognize the application name of a legitimate application that a third-party company has developed.

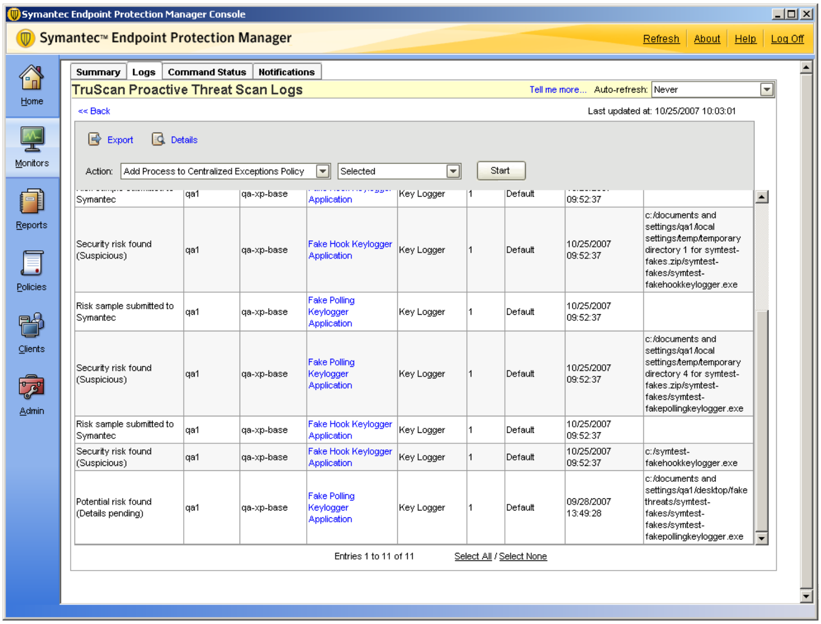
See “Creating exceptions for detected processes” on page 74.

To monitor the scan events

1. In the console, click **Monitors > Logs**.
2. On the Logs tab, in the **Log type** drop-down list, click **TruScan Proactive Threat Scan**.
3. Select a time from the **Time range** list box closest to when you last changed a scan setting.
4. Click **Advanced Settings**.
5. In the **Event type** drop-down list, select one of the following log events:
   - To view all detected processes, make sure **All** is selected.

- To view the processes that have been evaluated as security risks, click **Security risk found**.
- To view the processes that have been evaluated and logged as potential risks, click **Potential risk found**.

6 Click **View Log**.



TruScan Proactive Threat Scan Logs

Auto-refresh: Never

Last updated at: 10/25/2007 10:03:01

Action: Add Process to Centralized Exceptions Policy | Selected

Symantec	qa1	qa-xp-base	Application	Key Logger	1	Default	09:52:37	
Security risk found (Suspicious)	qa1	qa-xp-base	Fake Hook Keylogger Application	Key Logger	1	Default	10/25/2007 09:52:37	c:/documents and settings/qa1/local settings/temp/temporary directory 1 for symtest-fakes.zip/symtest-fakes/symtest-fakehookkeylogger.exe
Risk sample submitted to Symantec	qa1	qa-xp-base	Fake Polling Keylogger Application	Key Logger	1	Default	10/25/2007 09:52:37	
Security risk found (Suspicious)	qa1	qa-xp-base	Fake Polling Keylogger Application	Key Logger	1	Default	10/25/2007 09:52:37	c:/documents and settings/qa1/local settings/temp/temporary directory 4 for symtest-fakes.zip/symtest-fakes/symtest-fakepollingkeylogger.exe
Risk sample submitted to Symantec	qa1	qa-xp-base	Fake Hook Keylogger Application	Key Logger	1	Default	10/25/2007 09:52:37	
Security risk found (Suspicious)	qa1	qa-xp-base	Fake Hook Keylogger Application	Key Logger	1	Default	10/25/2007 09:52:37	c:/symtest-fakehookkeylogger.exe
Potential risk found (Details pending)	qa1	qa-xp-base	Fake Polling Keylogger Application	Key Logger	1	Default	09/28/2007 13:49:28	c:/documents and settings/qa1/desktop/fake threats/symtest-fakes/symtest-fakes/symtest-fakepollingkeylogger.exe

Entries 1 to 11 of 11

7 After you identify the legitimate applications and the security risks, you create an exception for them in a Centralized Exceptions Policy.

You can create the exception directly from the TruScan Proactive Threat Scan Logs pane.

Creating exceptions for detected processes

TruScan proactive threat scan exceptions specify a different response than the one that a scan would normally take when it detects a process. If a scan detects a process that matches an exception, the engine performs the action that the exception defines. For example, if the scan logs a legitimate application that is called `validprocess.exe`, you can create an exception so that the scan ignores `validprocess.exe`.

When you add exceptions for the detected processes, the exceptions are added to a Centralized Exceptions Policy for a specific group or a location within a group. You can first create a group that uses a specific Centralized Exceptions Policy. For example, for client computers in Group A to run a custom application that the scan might otherwise quarantine, you can create an exception to ignore the application. Then you can assign the Centralized Exception Policy with this exception to group A. Each time users in group A run that application, the scanning engine ignores the application.

If you do not use the default settings, you can set the action for Trojan horses, worms, and keyloggers to Log in the Antivirus and Antispyware Policy. Then you can use the following guidelines to create exceptions:

- For the security risks, you change the action to Quarantine or Terminate.
  You may also want to quarantine a process that might not be malicious but that you do not want the users to run.
- For the legitimate processes, you change the action to Ignore.
  You may also want to allow a particular commercial keyloggers.
- For the unknown risks, you do not create an exception because you want the scanning engine to continue to log the event. If you still cannot determine whether an unknown risk is malicious or legitimate, then you can continue to log and observe the process. You can track how frequently the client detects this process. If you eventually discover that the process is legitimate, you can create an exception and change the action to Ignore.

Note: You can create exceptions only for the processes that are not included in the Symantec-defined white list of known processes and applications.

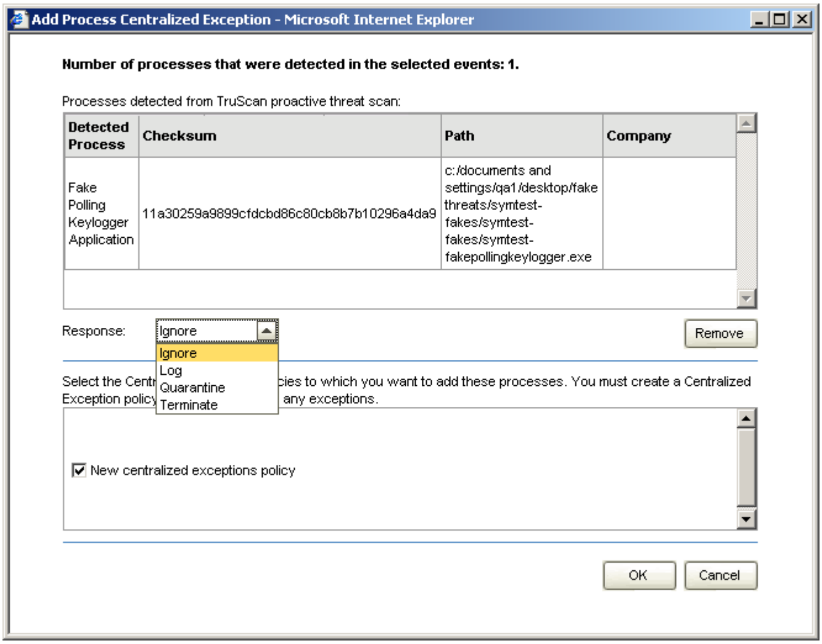
For more information on how to add processes to a Centralized Exceptions Policy, see the *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control.*

To create exceptions for detected processes

1. In the TruScan Proactive Threat Scan Logs pane, select one or more events for which you want to create a centralized exception.

   See “Monitoring the scan events” on page 73.
2. In the **Action** drop-down list, make sure **Add Process to Centralized Exceptions Policy** is selected.
3. Click **Start**.
4. In the Add Process Centralized Exception dialog box, in the **Response** drop-down list, select one of the following actions for the process.

- For a legitimate process, click **Ignore**.
- For a security risk, select either **Quarantine** or **Terminate**.



Add Process Centralized Exception - Microsoft Internet Explorer

Number of processes that were detected in the selected events: 1.

Processes detected from TruScan proactive threat scan:

Detected Process	Checksum	Path	Company
Fake Polling Keylogger Application	11a30259a9899cfdcbd86c80cb8b7b10296a4da9	c:/documents and settings/qa1/desktop/fake threats/symtest-fakes/symtest-fakes/symtest-fakepollingkeylogger.exe	

Response: Ignore

Select the Centr cies to which you want to add these processes. You must create a Centralized Exception policy any exceptions.

☑ New centralized exceptions policy

5 Select the Centralized Exceptions Policies that include this exception.

6 Click **OK**.

Adjusting scan settings

If you use the Symantec default settings to manage the detections, the client software determines the action and the sensitivity level. The scan engine that runs on the client computer automatically quarantines the security risks and logs potential risks and unknown risks.

If you do not use the Symantec default settings, you can set only a single response action for detections, whether or not they are risks. For example, a scan can quarantine all the detected processes or log all the detected processes, but a scan does not do both. You adjust the scan settings in the Antivirus and Antispyware Policy.

Table 6-1 describes the guidelines you use to adjust the detection action, sensitivity, and optionally the scan frequency.

Table 6-1 Scan settings

Setting	Description
Action	As a best practice, when you first start to manage the scans yourself, set the action to Log. This means that neither the security risks nor the legitimate processes use the action that you ultimately want. You want the scans to quarantine or terminate security risks and to ignore the legitimate processes. Therefore, you must create exceptions for all of these detections. The exceptions define the process and the action to take when a scan detects a specified process. See “Creating exceptions for detected processes” on page 74. **Note:** When you initially set up the Symantec Endpoint Protection Manager, the commercial applications use a response action of Log. With this action, you may see a lot of commercial application detections in the TruScan Proactive Threat Scan log, which can be overwhelming to users. Therefore, you may want to disable the Display a message when there is a detection feature on the Notifications tab. See “Monitoring the scan events” on page 73.

Table 6-1 Scan settings *(continued)*

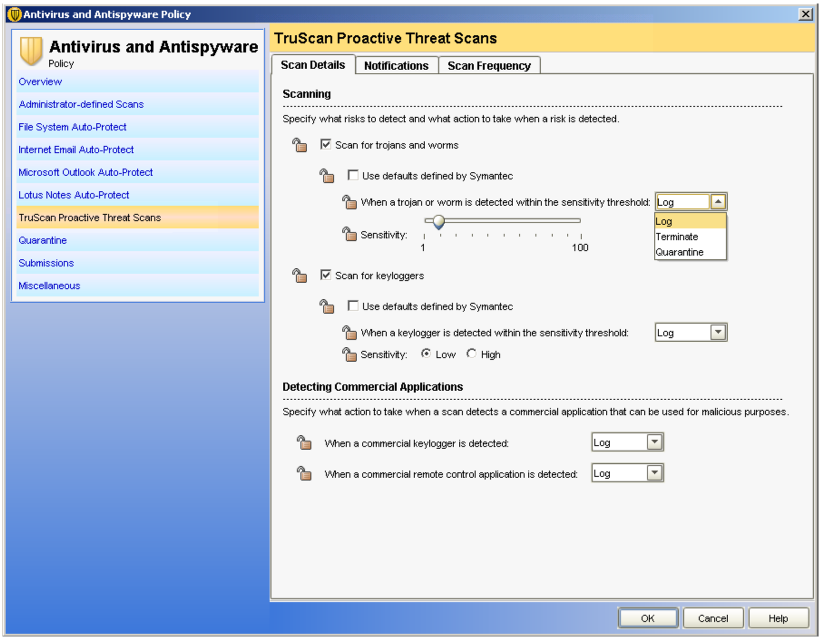
Setting	Description
Sensitivity	When you first adjust the sensitivity level for Trojan horses and worms, set the sensitivity level to 10. When the sensitivity level is low, the scans detect fewer processes than with the sensitivity level set higher. The rate of legitimate processes that are logged as potential risks is low. After you run the sensitivity level at 10 for a few days and monitor the log for any legitimate applications, you can raise the sensitivity level to 20. Over a 60-day to 90-day period, you can gradually increase the sensitivity level in 10-unit increments to 100. For maximum protection, leave the sensitivity level at 100. By using this gradual break-in approach, the users on the client computers are not overwhelmed with detection notifications as soon as you deploy the client. Instead, you can allocate time to monitor the increase in notifications at each level. You can also disable the detection notifications. For keyloggers, start the sensitivity level on Low. As you increase the sensitivity level, more processes are detected, both malicious and legitimate. The sensitivity level does not appreciably affect the rate of logged legitimate processes. A higher sensitivity level means that a scan flags a higher quantity of processes that are security risks as well as legitimate processes. But the ratio of legitimate to malicious processes remains nearly constant, despite the sensitivity level. Furthermore, the sensitivity level does not indicate the level of certainty that is associated with a detection. For example, a scan may detect one process at sensitivity level 10 and detect another process at sensitivity level 90. But the sensitivity level does not mean that one process is more of a threat than the other. After you change the sensitivity level of the scans, use the TruScan Proactive Threat Scan log to determine whether the sensitivity level is too low or too high. If the client reports too many legitimate processes as security risks, then you may want to set the sensitivity level lower until you have time to create centralized exceptions for the legitimate processes. See “Monitoring the scan events” on page 73. After you have set the correct sensitivity level, look for the legitimate processes and add them to a Centralized Exceptions Policy. Then increase the sensitivity. See “Creating exceptions for detected processes” on page 74. **Note:** After you have added all the exceptions to a Centralized Exceptions Policy, it is likely that any new detections are security risks. For greater security, you can change the response action for all processes back to either Quarantine or Terminate. Continue to monitor the TruScan Proactive Threat Scan log in case the scan detects and quarantines new legitimate applications.

Table 6-1 Scan settings *(continued)*

Setting	Description
Scan frequency	The default frequency for scans is one hour. If the performance of the client computers becomes too slow, decrease the scan frequency.

To adjust scan settings

1. In the console, click **Policies > Antivirus and Antispyware**, and then open an existing Antivirus and Antispyware Policy.
2. On the Antivirus and Antispyware Policy page, click **TruScan Proactive Threat Scans**.


Antivirus and Antispyware Policy
Antivirus and Antispyware
Policy
Overview
Administrator-defined Scans
File System Auto-Protect
Internet Email Auto-Protect
Microsoft Outlook Auto-Protect
Lotus Notes Auto-Protect
TruScan Proactive Threat Scans
Quarantine
Submissions
Miscellaneous
TruScan Proactive Threat Scans
Scan Details
Notifications
Scan Frequency
OK
Cancel
Help

Scanning

Specify what risks to detect and what action to take when a risk is detected.

☑ Scan for trojans and worms

□ Use defaults defined by Symantec

When a trojan or worm is detected within the sensitivity threshold: Log (Log / Terminate / Quarantine)

Sensitivity: 1 100

☑ Scan for keyloggers

□ Use defaults defined by Symantec

When a keylogger is detected within the sensitivity threshold: Log

Sensitivity: ● Low ○ High

Detecting Commercial Applications

Specify what action to take when a scan detects a commercial application that can be used for malicious purposes.

When a commercial keylogger is detected: Log

When a commercial remote control application is detected: Log

3. On the Scan Details tab, under Scanning, make sure that you check **Scan for trojans and worms** and **Scan for keyloggers**.
4. For either risk type, uncheck **Use defaults defined by Symantec**.
5. For either risk type, set the action to **Log**.
6. Do one of the following actions:
   - For keyloggers, click **Low**.

- For Trojan horses and worms, move the slider to the right to the second crosshatch mark, which is 10.

7 Optionally, on the Scan Frequency tab, under Scan Frequency, click **At a custom scanning frequency** and specify a time interval.

8 Click **OK**.

Index

A

availability
- for databases and management servers 66

C

centralized exceptions
- for proactive threat scans 74

client connection
- checking status 35
- status icon 20

communication
- problems between the client and the server 16
- problems with the management server 16
- problems with the server and the console or the database 17

connectivity
- communication between the client and the server 16
- performing a manual policy update 22
- using a browser to test 23
- using ping to test 23
- using Telnet to test 24
- verifying communication with the database 26
- with IIS 28

content
- comparing on the client and the server 38
- comparing versions 39
- determining how a client receives 34
- determining that a client does not receive 37
- types of 33

content cache 38

content provider
- making sure client can communicate with 36

content updates
- determining how a client is configured to receive 34
- network connectivity 34
- troubleshooting problems 32

D

databases
- availability 66
- embedded 61
- external 61

debug logs. *See* logs
- DebugView tool 45

definitions
- updating 64

F

failover 66

G

group update provider 65

groups
- setting up for remote clients 49

I

inheritance 50–51

L

LiveUpdate
- checking the content policy 41
- checking the settings on the management server 41
- checking the Settings policy 42
- internal server 64
- running a manual session 42
- viewing latest downloads to the management server 40

load balancing and roaming 59, 67

location awareness
- setting up for remote clients 49, 51

logs
- checking the debug log on the client 25
- checking the inbox logs 25
- client 58, 64
- creating a sylink log 44
- IIS 25

logs *(continued)*
viewing for proactive threat scans 73
viewing the debug log on the client 44
viewing the LiveUpdate log 43

M
management server 61
managing TruScan proactive threat scans 71
mobile clients
definition 47

N
notifications
remote clients 58
TruScan proactive threat scans 78

P
policies
LiveUpdate content 41
LiveUpdate Settings 42
updating for remote clients 56–58
policy serial number
viewing on the client 22
proactive threat scans. *See* TruScan proactive threat scans

R
remote clients
definition 47
monitoring 59
replication 66
roaming and load balancing 59, 67

S
scans. *See* TruScan
serial number. *See* policy serial number
server
internal LiveUpdate 64
settings
location-independent 49
location-specific 50
proactive threat scans 76
sites
creating one or multiple 63
defined 61
status icon 20, 35. *See* client connection

T
topology
management 61
Trojan horses, worms, and keyloggers
adjusting the settings 76
TruScan proactive threat scans
adjusting the settings 76
choosing a management approach 71
managing exceptions 72, 74
monitoring scan events 73

U
updates. *See* content updates