Symantec AntiVirus™ Corporate Edition Administrator's Guide

symantec™

Symantec AntiVirus™ Corporate Edition Administrator's Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.
Documentation version 9.0

Copyright Notice

Copyright © 2004 Symantec Corporation.
All Rights Reserved.
Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.
NO WARRANTY. The technical documentation is being delivered to you AS-IS, and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.
No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec, the Symantec logo, LiveUpdate, and Norton AntiVirus are U.S. registered trademarks of Symantec Corporation. Norton Internet Security, Norton Personal Firewall, Symantec AntiVirus, Symantec Client Firewall, Symantec Client Security, and Symantec Security Response are trademarks of Symantec Corporation.
Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.
Printed in the United States of America.
10 9 8 7 6 5 4 3 2 1

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible 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 as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages for those customers enrolled in the Platinum Support Program
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.html, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group via phone or online at www.symantec.com/techsupp.

Customers with Platinum support agreements may contact Platinum Technical Support via the Platinum Web site at www-secure.symantec.com/platinum/.

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
  - Error messages/log files
  - Troubleshooting performed prior to contacting Symantec
  - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, and then choose Service and Support. 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 on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

Contents

Technical support

Section 1 Managing Symantec AntiVirus

Chapter 1 Managing Symantec AntiVirus

About managing Symantec AntiVirus 13
Managing with the Symantec System Center 14
Using console views 15
Saving console settings 16
Understanding Symantec System Center icons 17
Discovering computers and refreshing the console 19
Auditing computers 31
About clients and servers 37
About primary servers 37
About secondary servers 38
About parent servers 38
About server and client groups 38
Deciding whether to manage with server groups and/or client groups 39
Server and client group scenario 41
Managing with server groups 41
Creating server groups 41
Locking and unlocking server groups 42
Working with server group passwords 43
Renaming server groups 45
Selecting a primary server for a server group 45
Changing primary and parent servers 46
Moving a server to a different server group 46
Viewing server groups 47
Deleting server groups 48
Enhancing server group security 48
How the access list works 48
Implementing enhanced server group security 49

Managing with client groups 53
Creating new client groups 53
Adding clients to a client group 53
Configuring settings and running tasks at the client group level 54
Finding client group settings 54
Moving clients in client groups 54
Viewing client groups 54
Filtering the client group view 56
Renaming client groups 57
Deleting client groups 57
Configuring clients directly 58
Changing an unmanaged client into a managed client (and the reverse) 58
How settings propagate 60
New Grc.dat files overwrite old Grc.dat files 61

Chapter 2 Setting up the Alert Management System

About the Alert Management System 63
How Alert Management System works 64
Configuring alert actions 65
Alert configuration tasks 65
Configuring alert action messages 66
Speeding up alert configuration 68
Configuring the Message Box alert action 70
Configuring the Broadcast alert action 71
Configuring the Run Program alert action 71
Configuring the Load An NLM alert action 72
Configuring the Send Internet Mail alert action 73
Configuring the Send Page alert action 74
Configuring the Send SNMP Trap alert action 76
Configuring the Write To Event Log alert action 79
Working with configured alerts 79
Testing configured alert actions 80
Deleting an alert action from an alert 80
Exporting alert actions to other computers 80
Using the Alert Management System Alert Log 82
Viewing detailed alert information 84
Filtering the Alert Log display list 85
Forwarding alerts from unmanaged clients 86

Section 2 Configuring Symantec AntiVirus

Chapter 3 Scanning for viruses and other threats

About threats ... 91
About scans in Symantec AntiVirus ... 93
- Understanding Auto-Protect scans ... 94
- Understanding scheduled scans ... 94
- Understanding manual scans ... 94
- Selecting computers to scan ... 95

Configuring Auto-Protect scans ... 97
- Configuring Auto-Protect for files ... 98
- Configuring Auto-Protect email scanning for groupware applications ... 107
- Configuring Auto-Protect scanning for Internet email ... 108
- How to specify exclusions ... 110
- Configuring Auto-Protect settings ... 111
- How to lock and unlock Auto-Protect options ... 112

Configuring manual scans ... 112
- How to specify exclusions ... 114
- Deleting files and folders that are left on computers by threats ... 115

Configuring scheduled scans ... 115
- Scheduling scans for server groups or individual Symantec AntiVirus servers ... 115
- Scheduling scans for Symantec AntiVirus clients ... 118
- Setting options for missed scheduled scans ... 120
- Editing, deleting, or disabling a scheduled scan ... 121
- Running a scheduled scan on demand ... 122
- Deleting files and folders that are left on computers by threats ... 122

Handling Symantec AntiVirus clients with intermittent connectivity ... 123
Configuring scan options ... 124
- How to assign primary actions and secondary actions for detected viruses ... 124
- How to assign primary actions and secondary actions for other detected threats ... 125
- Controlling the user experience ... 126
- Scanning for in-memory threats ... 134
- Excluding files from scanning ... 134
- Selecting file types and extensions to scan for viruses ... 136
- Enabling expanded threat categories ... 140
- Setting options for scanning compressed files ... 142
- Configuring HSM settings ... 143
- Setting CPU utilization ... 145

Chapter 4 Updating virus definitions files

About virus definitions files 147
Virus definitions files update methods 148
Best practice: Using the Virus Definition Transport Method and LiveUpdate together 149
Best practice: Using Continuous LiveUpdate on 64-bit computers 149
Updating virus definitions files on Symantec AntiVirus servers 150
Updating and configuring Symantec AntiVirus servers using the Virus Definition Transport Method 150
Updating servers using LiveUpdate 156
Updating servers with Intelligent Updater 159
Updating servers using Central Quarantine polling 159
Minimizing network traffic and handling missed updates 160
Updating virus definitions files on Symantec AntiVirus clients 162
Updating virus definitions files on Symantec AntiVirus clients immediately 164
Configuring managed clients to use an internal LiveUpdate server 165
Enabling and configuring Continuous LiveUpdate for managed clients 166
Setting LiveUpdate usage policies 167
Controlling virus definitions files 168
Verifying the version number of virus definitions files 169
Viewing the threat list 169
Rolling back virus definitions files 169
Testing virus definitions files 170
Update scenarios 171
About scanning after updating virus definitions files 171

Chapter 5 Responding to virus outbreaks

About responding to virus outbreaks 173
Preparing for a virus outbreak 174
Creating a virus outbreak plan 174
Defining Symantec AntiVirus actions for handling suspicious files 175
Automatically purging suspicious files from local Quarantines 176
Handling a virus outbreak on your network 177
Using virus alerts and messages 177
Running a virus sweep 178
Tracking virus alerts using Event Logs and Histories 178
Tracking submissions to Symantec Security Response with Central Quarantine Console 179

Chapter 6 Managing roaming clients

About roaming clients 181
Roaming client components 182
How roaming works 183
Implementing roaming 183
Analyzing and mapping your Symantec AntiVirus network 184
Identifying servers for each hierarchical level 185
Creating a list of 0 level Symantec AntiVirus servers 185
Creating a hierarchical list of Symantec AntiVirus servers 186
Configuring roaming client support options from the Symantec System Center console 186
Configuring additional roaming client support for roam servers 189
Configuring additional server types for roaming clients 191
Command-line options 191
Registry values 193

Chapter 7 Working with Histories and Event Logs

About Histories and Event Logs 195
Sorting and filtering History and Event Log data 197
Viewing Histories 199
Working with Threat Histories 200
Working with Scan Histories 202
Understanding Event Log icons 204
Forwarding client logs to parent servers 205
Configuring log forwarding options 205
Configuring log events to forward 206
Best practice: Configuring events to forward for sometimes managed clients 208
Reviewing the forwarding status file 208
Deleting Histories and Event Logs 209

Index

Section 1

Managing Symantec AntiVirus

- Managing Symantec AntiVirus
- Setting up the Alert Management System

Chapter 1

Managing Symantec AntiVirus

This chapter includes the following topics:

- About managing Symantec AntiVirus
- Managing with the Symantec System Center
- About clients and servers
- About server and client groups
- Managing with server groups
- Enhancing server group security
- Managing with client groups
- Configuring clients directly
- Changing an unmanaged client into a managed client (and the reverse)
- How settings propagate

About managing Symantec AntiVirus

Using the Symantec System Center, you can perform Symantec AntiVirus administrative operations such as installing antivirus protection on workstations and network servers, updating virus definitions, and managing Symantec AntiVirus servers and clients. In addition to the Symantec System Center, you can also use configuration files (Grc.dat) to configure Symantec AntiVirus clients. You can use configuration files if you want to use a third-party tool to perform remote configuration on your network.

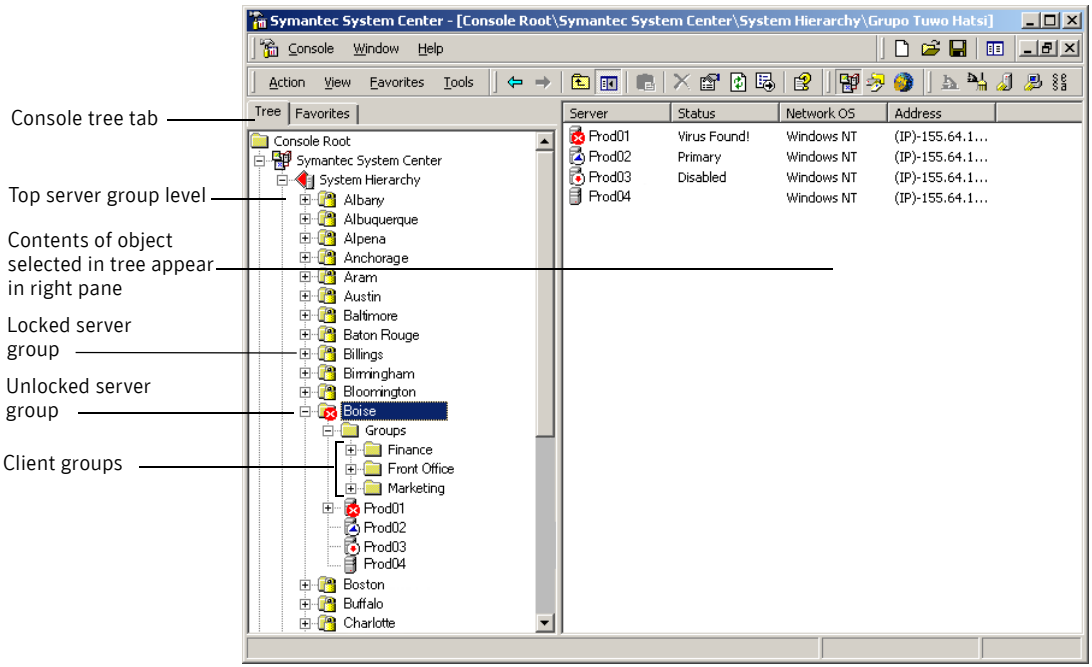
Managing with the Symantec System Center

When the Symantec System Center runs, it displays a system hierarchy of server groups, client groups, and servers displayed in an expandable/collapsible tree. The system hierarchy is the top level that contains all server groups and client groups.

Note: The system hierarchy is not populated until you install at least one Symantec AntiVirus server.

To start the Symantec System Center

- On the Windows taskbar, click **Start** > **Programs** > **Symantec System Center Console** > **Symantec System Center Console**.



Using console views

Each product management snap-in makes a new product view available within the Symantec System Center console. For example, when you install the Symantec AntiVirus management snap-in, the Symantec AntiVirus view is added, which includes fields related to Symantec AntiVirus, such as Last Scan and Definitions.

The columns that appear in the right pane change based on the selected view. When System Hierarchy is selected, the Console Default View includes the following data columns:

- Name
- Status
- Primary Server
- Valid State

Table 1-1 lists the data columns in the Symantec AntiVirus view.

Table 1-1 Data columns in the Symantec AntiVirus view

Object selected in left pane	Data columns that appear in right pane
System hierarchy icon	■ Server Group ■ Status ■ Definition Sharing ■ Newest Definitions ■ Status of server updates
Server group icon	■ Server ■ Type ■ Status ■ Last Scan ■ Definitions ■ Version ■ Scan Engine ■ Address ■ Status of client updates
Groups icon (for client groups)	■ Group Name ■ Configuration Change Date ■ Number of Clients

Table 1-1 Data columns in the Symantec AntiVirus view

Object selected in left pane	Data columns that appear in right pane
Client group icon or Server icon	■ Client ■ User ■ Status ■ Last Scan ■ Definitions ■ Version ■ Scan Engine ■ Address ■ Group ■ Server

Changing console views

Unless you change the view, the Symantec System Center console displays the Console Default View. The other views available depend upon which managed Symantec AntiVirus products you have installed.

To change console views

1. In the Symantec System Center console, in the left pane, expand **System Hierarchy**.
2. On the View menu, in the list that appears at the bottom of the menu, select a view.

Saving console settings

When you close the console, you are prompted to save console settings for the Symantec System Center.

To save console settings

◆ Do one of the following:

- Click **Yes** if you want to see the same console view the next time that you launch the Symantec System Center.
- Click **No** if you want to see the last saved view the next time you launch the Symantec System Center.

Choosing No may result in lost settings. For example, if you change settings for an attached Quarantine Server, and then choose No when exiting the console, the changes are not retained for the Quarantine Server.

Note: If a newer version of MMC is present on the system, you may need to upgrade to the newer version to save changes upon exiting the Symantec System Center console.

Understanding Symantec System Center icons

The Symantec System Center uses icons to represent the different states of computers that are running Symantec managed products. For example, if the server group icon in the server group view appears with a padlock icon, the server group must be unlocked with its password before you can configure or run scans for the computers in the server group.

Table 1-2 lists the Symantec System Center icons.

Table 1-2 Symantec System Center icons

Icon	Icon descriptions
	Highest level object representing the system hierarchy, which contains all server groups.
	Unlocked server group or client group. Compare this icon to the locked server group icon. For security reasons, all server groups default to locked when you start the Symantec System Center.
	Locked server group. You must enter a password before you can view the computers in the server group to configure and run updates and scans.
	An issue needs to be resolved in this server group. For example, there may not be a primary server assigned to the server group or a server may be infected with a threat.
	Symantec AntiVirus server running on a supported Windows or NetWare computer. Compare this icon to the next one, which is the primary server for the server group.
	Symantec AntiVirus primary server running on a supported Windows or NetWare computer.

Table 1-2 Symantec System Center icons

Icon	Icon descriptions
	Unavailable Symantec AntiVirus server. This icon appears when communication is severed between the Symantec AntiVirus server and the Symantec System Center console. The communication error may result from one of several different causes. For example, the server system is not running, the Symantec software has been removed, or there could be a network failure between the console and the system.
	A virus was detected on the computer that is running Symantec AntiVirus server.
	A threat other than a virus, such as adware or spyware, was detected on the computer that is running Symantec AntiVirus server. **Note:** If Symantec AntiVirus detects a virus and a threat other than a virus on the same computer, the virus icon appears.
	Symantec AntiVirus client running on a supported Windows computer. When you select this computer, you view options only on that computer.
	A virus was detected on the computer that is running Symantec AntiVirus client.
	A threat other than a virus, such as adware or spyware, was detected on the computer that is running Symantec AntiVirus client. **Note:** If Symantec AntiVirus detects a virus and a threat other than a virus on the same computer, the virus icon appears.
	An issue needs to be resolved with this client. For example, virus definitions files may be out-of-date or the client group to which the client was assigned is no longer valid. The status field in the Symantec System Center console indicates the actual problem.
	The computer, which runs Symantec AntiVirus client software, is not currently connected to the network. You must enable a setting for the Symantec System Center console to show when clients are not connected to the network.

Showing when clients are offline

You can configure the Symantec System Center console to show when computers running Symantec AntiVirus client software are not currently connected to the network. The icon in the last row of Table 1-2 indicates that the client is offline.

To show when clients are offline

1. In the Symantec System Center console, on the Tools menu, click **SSC Console Options Properties**.
2. In the SSC Console Options Properties dialog box, on the Client Filter tab, under Group Options, check **Indicate when clients are offline**.
   This option is unchecked by default.

Showing client Auto-Protect status

You can configure the client or server icon to appear in the Windows system tray.

The icon shows a client or server's Auto-Protect status as follows:

- When Auto-Protect is enabled, a check mark appears next to Enable Auto-Protect and the icon appears as a full shield.
- When Auto-Protect is disabled, the icon is covered by a universal no sign (a red circle with a diagonal slash).

Discovering computers and refreshing the console

At the first startup of a newly installed Symantec System Center console, the console will ping the network to find all available computers running Symantec AntiVirus servers. As soon as the servers respond, they are added to the console. Connected workstations running a managed Symantec client product are added when their *parent server* is selected in the console tree.

If you start servers that are running a manageable Symantec product while the Symantec System Center is already running, you may need to locate the server using the Find feature or Discovery Service so that it will display in the server group view.

You can also use Discovery to locate network computers on which Symantec AntiVirus is not installed.

Using the Discovery Service

The Symantec System Center console runs a single Windows NT service, the Symantec System Center Discovery Service (Nsctop.exe). This service is responsible for discovering the computers running Symantec AntiVirus server that appear in the Symantec System Center console. The Discovery service also populates the Symantec System Center console with objects.

You can choose one of the following Discovery types:

- Load from cache only
- Local Discovery
- Intense Discovery

See "Understanding Load from cache only discovery type" on page 22.

See "Understanding Local Discovery" on page 22.

See "Understanding Intense Discovery" on page 23.

How discovering computers on the network works

To discover computers on the network, a computer running Symantec AntiVirus server sends a ping packet to a computer running Symantec AntiVirus client. The ping program verifies that the remote computer exists and can accept requests. When the Ping Discovery Service (Intel PDS) hears a ping, it responds with a pong packet. Ping and pong packets are about 1 KB. A successful ping-pong discovery ensures that the computer is working.

The pong also provides valuable information, such as the following:

- Date of the computer's virus definitions files
- When the computer was last infected

Both IP and IPX pings are sent to the remote computer running Symantec AntiVirus server to determine what type of protocol it uses.

Pings are also sent that support Norton AntiVirus Corporate Edition and LANDesk Virus Protect, legacy versions of Symantec AntiVirus.

The data from the computer running Symantec AntiVirus client is stored on the computer running Symantec AntiVirus server that is the client's parent server.

The Symantec System Center console reads each parent server's registry to get the data that it displays in the console.

Following the completion of this process, Normal Discovery runs.

Normal Discovery

Following all types of Discovery, a Normal Discovery runs. In a Normal Discovery, the Symantec System Center console broadcasts to all servers that are in unlocked server groups. This additional Discovery queries the primary server of the server group for the list of secondary servers in its address cache.

The Symantec System Center console address cache stores information for all servers that have ever reported to it. The primary server address cache contains information for every server within the server group. The address cache includes the names of all secondary servers and their IP addresses.

The Symantec System Center console compares its own address cache with the address cache sent by the primary server. When a mismatch is identified, the console pings the associated server. When the pong data returns, it is added to all other servers in the list.

In this way, Normal Discovery can identify every server in the server group and attempt to resolve information conflicts between parent servers.

Discovery Service WINS or Active Directory requirement

The Discovery Service requires the use of WINS (Windows Internet Naming Service) or Active Directory name resolution. If you are attempting discovery in an environment where WINS or Active Directory is not available you will need to find at least one computer running Symantec AntiVirus server on your network first. To find the computer, you can use the Find Computer feature or the Importer tool.

See "Using the Find Computer feature" on page 27.

See the *Symantec AntiVirus Reference Guide* for information about the Importer tool.

How to find NetWare computers

The Discovery Service may not find NetWare computers that are running IP only. To find computers not located by the Discovery Service, you can use the Find Computer feature.

See "Using the Find Computer feature" on page 27.

Understanding the Discovery Cycle configuration

The Discovery Cycle time-out is configurable. Depending on how you configure your Discovery Service, you can set the time-out from 1 to 1440 minutes between discovery attempts. By default, the interval is set to 480 minutes (every 8 hours).

A new discovery is skipped if the last discovery is still running. For example, if you have discovery set to run once a minute, and discovery takes 20 minutes, 19 discovery attempts will be skipped.

Changing the Discovery Cycle interval

While the Discovery Cycle interval can be changed, be aware that increasing the interval can result in a display of outdated information from the Symantec System Center console.

To change the Discovery Cycle interval

1. In the Symantec System Center console, on the Tools menu, click **Discovery Service**.
2. Change the Interval In Minutes setting as necessary.

Understanding Load from cache only discovery type

Load from cache only offers the most basic type of discovery. It tries to refresh all of the servers for which the Symantec System Center console contains information in its address cache. Each server is then sent a series of pings to see if the server will check back in, and to refresh information on the console.

Following the Load from cache only operation, the Normal Discovery runs.

See "Normal Discovery" on page 21.

Load from cache only is the default Discovery method. This reduces unwanted traffic on the network when launching the Symantec System Center. In most cases, you may find that choosing Load from cache only finds all of the servers that you need to add to the Symantec System Center console.

Understanding Local Discovery

When you use Local Discovery, a broadcast of a ping packet is sent over the local subnet of the computer running the Symantec System Center console. Intel PDS services running on servers on the local subnet reply with pong data.

Local Discovery generates less ping noise, but is limited to working on the local subnet. Local Discovery works very well on small subnets. In very large subnets, you may experience better results using Intense Discovery.

Following a Local Discovery, the following Discovery types run:

- Load from cache only
- Normal Discovery

See "Normal Discovery" on page 21.

Understanding Intense Discovery

Intense Discovery walks My Network Places on the local Windows 2000 computer or the Network Neighborhood on the local Windows NT computer, and attempts to resolve all computers that it finds into a network address. Once it has the network address, it attempts to send ping requests. You can configure whether Intense Discovery walks the NetWare or Microsoft branches of the network tree, or both.

From the Symantec System Center console, you can select any node beneath the console root, and then choose Discovery Service from the Tools menu to perform a new discovery of servers.

Following an Intense Discovery, the following Discovery types run:

- Local Discovery
- Load from cache only
- Normal Discovery

See "Normal Discovery" on page 21.

Note: The ability of Intense Discovery to locate computers is limited by several factors: the availability of a WINS server or Active Directory, network subnet and router configuration, DNS configuration, and Microsoft domain and workgroup configuration. Searching by IP address range in most cases is not affected by these factors. For this reason, you may want to use IP Discovery.

Understanding IP Discovery

IP Discovery provides discovery by either IP address range or IP subnet range.

You may want to run IP Discovery only periodically. It can be used to discover computers across the network.

Once the computers are in the address cache, you can then rely on the Load from cache only method.

Running the Discovery Service

You manually run all forms of Discovery directly from the Symantec System Center console.

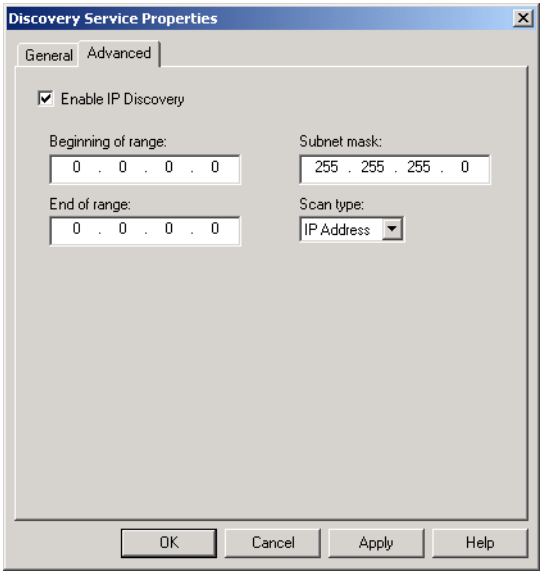
Note: The Discovery service uses WINS (Windows Internet Naming Service) or Active Directory when browsing for new computers that are running Symantec AntiVirus. If you are trying to discover new computers in an environment in which WINS or Active Directory is unavailable, you may want to run the Find Computer feature or the Importer tool first.
See "Using the Find Computer feature" on page 27.
See the *Symantec AntiVirus Reference Guide* for information about the Importer tool.

Run the Discovery Service

You can run the Discovery Service and find servers with or without including IP addresses and subnets.

To run IP Discovery

1. In the Symantec System Center console, in the left pane, select any node below the console root.
2. On the Tools menu, click **Discovery Service**.
3. In the Discovery Service Properties window, on the Advanced tab, check **Enable IP Discovery**.



Once Enable IP Discovery is checked, an IP Discovery session runs whenever you run an Intense Discovery. To run Intense Discovery without also running IP Discovery, uncheck Enable IP Discovery.

4 In the Scan Type list, select one of the following:
   - IP Subnet: The console broadcasts to each subnet.
   - IP Address: The console pings every computer in the range of IP addresses.

5 In the Beginning of range and End of range boxes, type the addresses.

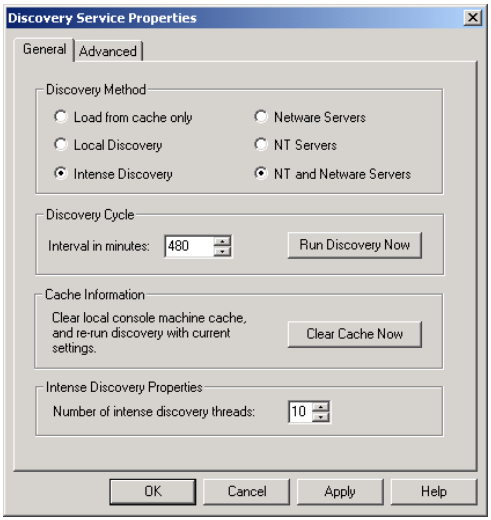
6 If you clicked IP Subnet, type the subnet mask to refine the search.
   IP Address search results appear in the Machine list box. IP Subnet search results are displayed in the Symantec System Center console status bar.

You can also access IP Discovery functionality in the Find Computer dialog box.

See "Using the Find Computer feature" on page 27.

To discover without IP

1 In the Symantec System Center console, on the Tools menu, click **Discovery Service**.



2. In the Discovery Service Properties window, on the General tab, select one of the following options:
   - Load from cache only: This is the quickest method. The Symantec System Center reads the list of servers and clients stored in the local cache.
     See "Understanding Load from cache only discovery type" on page 22.
   - Local Discovery: Broadcasts to the Symantec System Center console's local subnet. Servers respond immediately with information about themselves and their clients. Each server's server group will appear in the console (unless filtered using the View menu). Load from cache only will run as well.
     See "Understanding Local Discovery" on page 22.
   - Intense Discovery: This is the most thorough method. If you have a large network, the discovery process may take a long time. The Symantec System Center serially pings every server in the Network Neighborhood. Server names appear in the message area of the Symantec System Center console as they are found during the discovery process. Intense Discovery also performs the same local subnet broadcast as Local Discovery. Load from cache only and Local Discovery will run as well.
     For Intense Discovery, you can limit the search to NetWare or Windows NT servers only, or search for both.
     See "Understanding Intense Discovery" on page 23.
3. Under Discovery Cycle, select the Interval in minutes if necessary.
4. If you want to immediately run discovery, click **Run Discovery Now**, and then click **Close**.
   Only one discovery can run at a time.
5. Under Intense Discovery Properties, specify the number of intense discovery threads.
   You can choose any number of threads between 2 and 50. This setting affects Intense Discovery sessions only. Each discovery thread is an independent search for servers and clients. To maintain the most up-to-date discovery information, select a lower discovery interval and a higher number of discovery threads.
6. If you want to clear all server and client information out of the active memory and address cache, and immediately run Discovery based on the current discovery settings, under Cache Information, click **Clear Cache Now**.
   When you clear the cache, unlocked server groups will be locked unless the password for the server group has been saved.

Note: Rebuilding a list of servers on a large network may take a long time.

Using the Find Computer feature

If you want to quickly find a server without having to expand and browse through the tree, you can use the Find Computer feature. You can search using TCP/IP or IPX addresses, or computer names.

The Find Computer feature is also useful if you install a server and then do not see it in the tree view when you expand a server group or server. This may occur for the following reasons:

- The Symantec System Center may not automatically discover servers on LAN segments separated by routers.
- Servers may not be visible in the Network Neighborhood. For example, Windows Internet Naming Service (WINS) servers or Active Directory may not be replicated across network segments.

Servers on segments using only IPX protocol can also be skipped in the discovery process. If you cannot locate some servers on your LAN, you can locate them manually with the Find Computer feature in the Symantec System Center console. Once you use the Find Computer feature to locate a server, you can manage it from the Symantec System Center console.

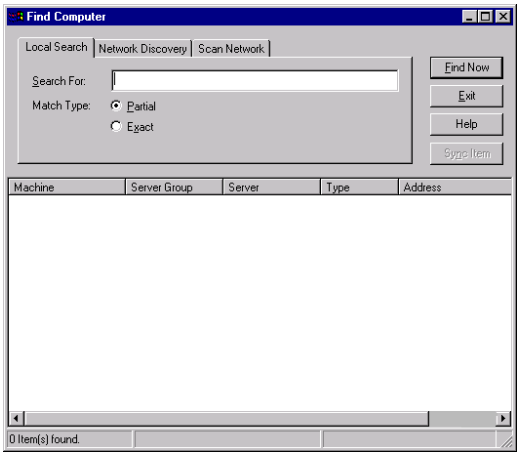
Note: If you don't have IPX installed, you may not see all NetWare computers in the console. While you will be able to find the computers using the Find Computer feature, installing IPX and TCP/IP ensures that the computers will be discovered.

Finding computers by searching the local cache

Rather than search the entire network for computers, you can restrict the search to those known to be stored in the local cache.

To find computers by searching the local cache

1 In the Symantec System Center console, on the Tools menu, click **Find Computer**.



2 In the Find Computer window, on the Local Search tab, type the network name of the server that you want to find.

3 Under Match Type, select one of the following:

- Exact: Searches for a server name that is an exact match.
- Partial: Searches for a server name that is a partial match.

If you leave the Search For text box empty and use Partial as the Match Type, all computers in the local cache will appear when you run the search.

Finding computers using a network search

You can use a network search to find individual computers running the Symantec AntiVirus server product.

Find computers

You can find computers using a network search or by specifying an IP address or subnet range.

To find computers using a network search

1 In the Symantec System Center console, on the Tools menu, click **Find Computer**.

2 In the Find Computer window, on the Network Discovery tab, specify whether you want to use a TCP/IP address, IPX address, or a computer name as the search criteria.

3 Type the server address or computer name.

4 Click **Find Now**.

To use IP addresses to find a range of computers running Symantec AntiVirus for servers

1 In the Symantec System Center console, on the Tools menu, click **Find Computer**.

2 In the Find Computer window, on the Scan Network tab, select one of the following:

- IP Subnet: Sends out a broadcast to each subnet.
- IP Address: Pings every computer in the range of IP addresses.

3 Type the addresses for Beginning of range and End of range.

4 If you clicked IP Subnet in step 2, type the subnet mask to refine the search.

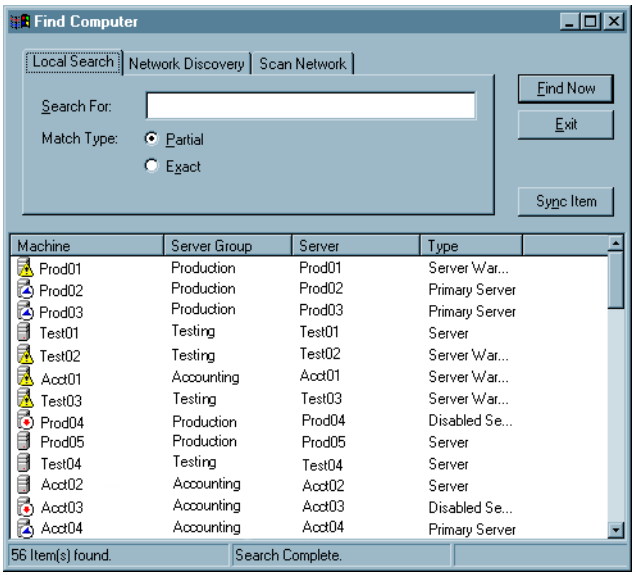
5 Click **Find Now**.
IP Address search results will appear in the Machine list box. IP Subnet search results will be displayed in the Symantec System Center console status bar.

Locating found items in the Symantec System Center console

You can match an item in a Find Computer list to the same item as it appears in the Symantec System Center console tree. To do so, the server group to which the item belongs must be unlocked.

To locate found items in the Symantec System Center console

1 In the Find Computer window, select the desired system.



2 Click **Sync Item** to locate the selected item.

Using the Refresh feature

From the Symantec System Center console, you can refresh at the system hierarchy, server group, or individual server level to validate active communication with the list of currently displayed servers. However, the Refresh feature does not find servers or server groups that may have been added since the current session of the Symantec System Center started. If the refresh determines that a server that previously appeared in the server group view is no longer communicating, the unavailable server icon appears.

To use the Refresh feature

- In the Symantec System Center console, in the left pane, right-click the system hierarchy, unlocked server group, server, or client group, and then click **Refresh**.

Auditing computers

Computers on your network that do not have Symantec AntiVirus running leave holes open in your network security. You can run a network audit of remote computers to determine the following:

- Whether a Symantec AntiVirus component is installed and running.
- The type of protection, such as server, client, or unmanaged client, that is installed.
- Whether antivirus software from other vendors or from Symantec (such as a Symantec AntiVirus consumer version), including the type and version of that software, is installed on the computer.

You must be able to log in as Administrator to the remote computers that you are auditing.

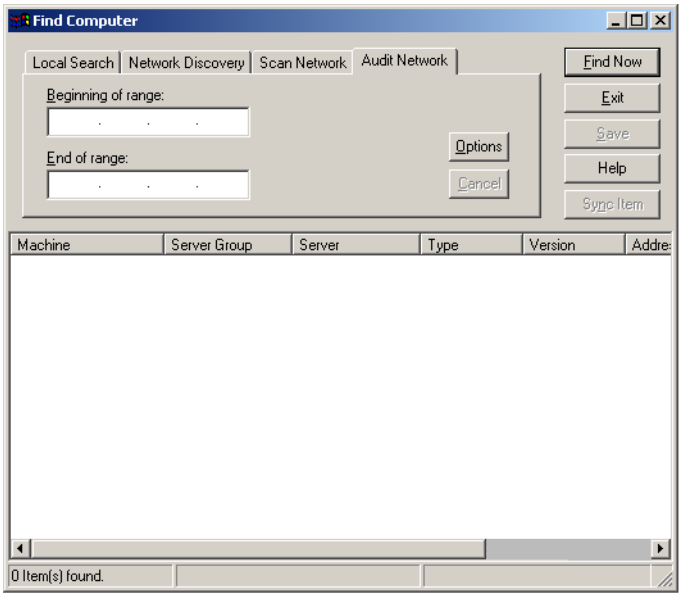
Note: If a firewall is running on the remote computer, the network audit may not be able to gather information.

Run a network audit and sync items

You can run a network audit to determine the antivirus protection status of the computers that you manage. Once the status for the computers in the range within which you searched is identified, you can locate selected computers by syncing to them.

To run a network audit

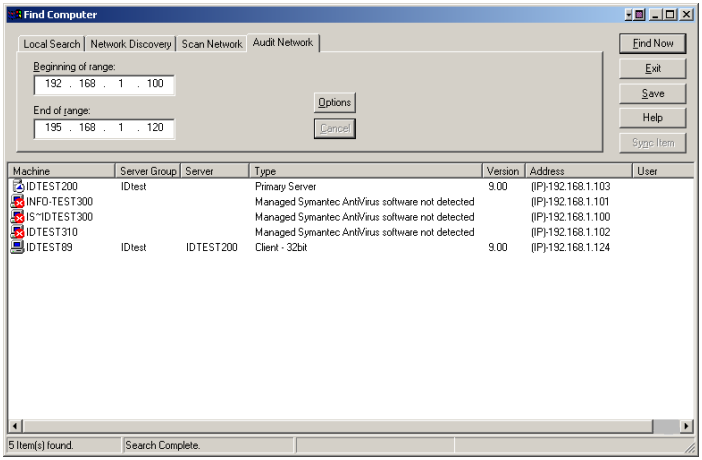
1 In the Symantec System Center console, on the Tools menu, click **Find Computer**.



2 In the Find Computer dialog box, on the Audit Network tab, type the beginning and end of the IP address range.

3 To change the default options, click **Options**.
See "Setting network audit options" on page 34.

4 Click **Find Now** to run the audit.



You can see the audit progress at the bottom of the Find Computer dialog box.
When the audit completes, the following types of information appear:

Machine	The name of the remote computer.
Server Group	The name of the server group to which the remote computer belongs.
Server	The name of the server that controls the remote computer.
Type	The server or client type. Login errors are also reported in this column.
Version	The version of the antivirus product running on the computer.
Address	The IP address of the computer.
User	The user name associated with the computer.

To sync items

1 In the Find Computer dialog box, click **Sync Item** to locate a selected computer running Symantec AntiVirus client.

2 Type the password for the server group to which the item belongs.

Labeling items and rerunning audits

You can label items such as the following:

- Computers that cannot be located or to which a connection cannot be made
- Routers and network drives
- Computers that do not have Symantec AntiVirus software installed

To label an item and rerun the audit

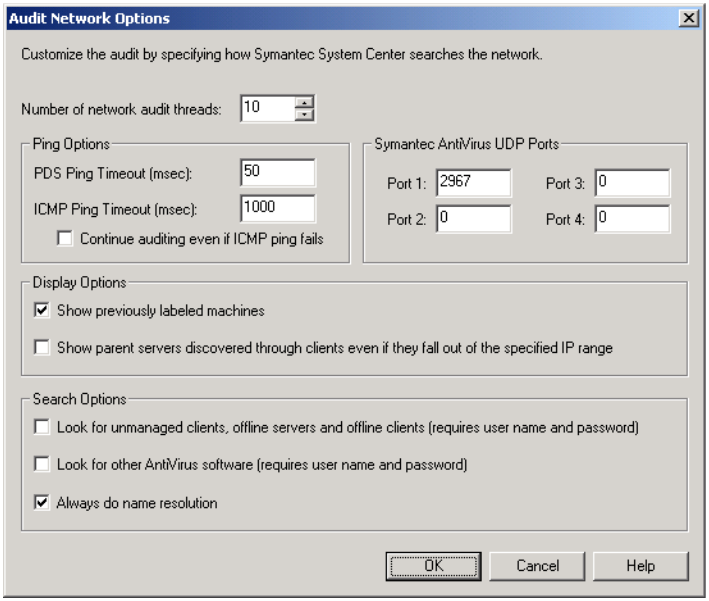
1. In the Find Computer dialog box, in the Machine column, right-click an item, and then click **Label**.
2. In the Edit description for dialog box, type a new label for the computer.
3. Click **OK**.
4. Right-click the item again, and then click **Audit again**.

Setting network audit options

You can set custom network audit options. For example, if you want to find remote computers running an unmanaged client, you can enable the related option.

To set network audit options

1 In the Find Computer dialog box, on the Audit Network tab, click **Options**.



2 In the Audit Network Options dialog box, specify the number of network audit threads to use.
A higher number yields faster results but requires more network utilization.

3 Under Ping Options, specify the timeout period in milliseconds for a Windows ICMP ping or Symantec PDS ping.

4 Check **Continue auditing even if ICMP ping fails** if you want auditing to continue if the ICMP ping fails.
For example, if you know that a firewall is set up with a rule to block an ICMP ping, you can still audit the computer for computers running Symantec AntiVirus.

5 Under Display Options, check **Show previously labeled machines** if you labeled computers during a previous audit and want the computers to appear in the results as they were previously labeled.

6 Check **Show parent servers discovered through clients even if they fall out of the specified IP range** if you want the parent servers of the computers running Symantec AntiVirus client or server out of the specified range to appear in the results.

7 Under Symantec AntiVirus UDP Ports, enter up to four port numbers that you want to ping.
Port 1 defaults to 2967, which is the default port number for RTVScan, the main Symantec AntiVirus service.

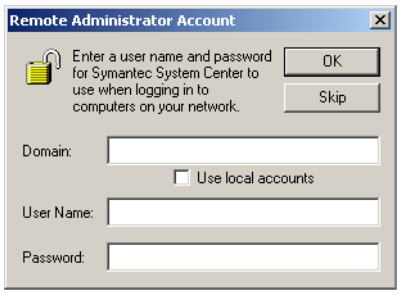
8 Under Search Options, check the appropriate boxes to find computers running unmanaged Symantec AntiVirus, offline servers and clients, or computers running antivirus software from other vendors.
You must provide valid Admin account information.
See "Setting Admin account options" on page 36.

Setting Admin account options

If you choose to find computers running unmanaged Symantec AntiVirus, offline servers and clients, or computers running antivirus software from other vendors, the Remote Administrator Account dialog box appears.

See Figure 1-1.

Figure 1-1 Remote Administrator Account dialog box



To set Admin account options

1 In the Remote Administrator Account dialog box, do one of the following:
   - Type the name of the domain that contains the computers that you want to find, followed by valid domain administrator account information.
   - Check **Use local accounts** to access a specific computer, and then type the Admin user name and password.

2 Click **OK**.

About clients and servers

The Symantec AntiVirus client program provides antivirus protection for networked and non-networked computers. The Symantec AntiVirus client program protects 32-bit and supported 64-bit computers running supported Windows versions.

The Symantec AntiVirus server program manages other computers running Symantec AntiVirus and supported legacy versions of Norton AntiVirus Corporate Edition, and can push configuration and virus definitions files updates to these clients. In addition, the Symantec AntiVirus software provides antivirus protection for the computers on which it runs. Symantec AntiVirus clients are always managed by a server.

Note: The Symantec AntiVirus server program is not supported on 64-bit computers.

When you manage with the Symantec System Center, computers running Symantec AntiVirus server can assume the following roles:

- Primary server
- Secondary server
- Parent server

About primary servers

Each server group has an administrator-designated *primary server*. The primary server is responsible for configuration functions in the server group. It can also be responsible for new virus definitions files updates.

From the Symantec System Center console, when you launch a task at the server group level, the task runs on the server group's primary server. The primary server also forwards the task on to all other servers in the server group.

If you are using Alert Management System[2], the primary server also processes all notifications.

Computers running any of the supported operating systems for servers can be made primary servers.

How the registry is affected

When you modify server options, you directly modify the registries of the selected servers. The modification is made through the transport manager, which handles communications.

The primary server acts as the repository of all server options on a group level. If you modify on a group level, the changes are recorded first in the registry of the primary server for that group in the HKLM\Software\Intel\LANDesk\VirusProtect6\CurrentVersion\DomainData key.

Then they are recorded in each of the other servers.

About secondary servers

Servers that are not assigned primary server status are called *secondary servers*. Secondary servers are children of primary servers. They retrieve information from the primary server and share it with clients.

All servers in a server group are secondary servers until you assign one as the primary server. You must designate the primary server before you can perform most tasks at the server group level.

Note: Symantec product configuration changes cannot be managed at a level higher than the server group.

About parent servers

A parent server is a computer running Symantec AntiVirus server with which a connected computer running Symantec AntiVirus client communicates to obtain configuration updates and to send alerts. Some servers may act as parent servers; others may act as primary servers. These two functions are not mutually exclusive. A primary server may also act as a parent server.

About server and client groups

Server group members can share a single Symantec AntiVirus configuration, and you can also run a Symantec AntiVirus operation on all members of a server group. From the Symantec System Center console, you can create new server groups and manage their membership. Server groups are independent of Windows domains and other products. You can combine NetWare and Windows computers into the same server groups, which allows simultaneous remote configuration of these systems.

Client groups are logical groupings of computers running Symantec AntiVirus client software. Although client groups are always attached to a server group,

each client group can be managed individually. By setting up client groups, you can set up and manage different policies under a single parent server.

- *Assigned clients* are Symantec clients that have been assigned to a client group. They receive virus definitions files from the server to which they are physically attached, but receive configuration settings and updates based upon the client group to which the Symantec AntiVirus policies are applied.
- *Unassigned clients* are Symantec clients that have not been assigned to a client group. They receive configuration settings and updates from their parent server.

Deciding whether to manage with server groups and/or client groups

Each Symantec AntiVirus server group supports a single configuration for all of the clients it manages. Each additional configuration requires adding an additional server to the server group. Server groups may provide you with all the configuration flexibility you need if all of your clients require the same configuration options. If you need more configuration flexibility, you may benefit from using client groups. When you manage using client groups, clients on the same physical server do not need to share the same configuration as other clients in the same server group. In addition, client groups can also decrease the number of servers required to manage Symantec AntiVirus. While each server group requires at least one server per unique configuration, a server group can contain any number of client groups, each with its own configuration.

Note: If you want to use client groups, Symantec recommends managing all clients with groups. While it is possible to manage in a mixed environment with some clients assigned to a group and some not assigned to a group, this adds complexity and may produce unexpected results.

Client groups and configuration priority

When you manage using client groups, clients assigned to a group receive their configuration from their group, rather than their parent server: Configuration changes made at the server level are ignored, and will only apply to unassigned clients. Configuration changes made at the server group level or system hierarchy level have priority over client group settings, and override any settings made at the client group level.

Table 1-3 lists each context you can select in the Symantec System Center, and what it configures, when selected.

Table 1-3 Configuration priority

Context	What it configures
System hierarchy	All unlocked server groups and the clients they manage (regardless of their client group membership)
Server group	All servers and clients in the server group (regardless of their client group membership)
Server	The server and its clients (regardless of their client group membership): ■ Virus Sweep ■ Update virus definitions now ■ History configuration The server and/or its unassigned clients: ■ Scheduled and manual scans ■ Virus definitions updating ■ Quarantine options ■ Client and server Auto-Protect options ■ Client administrator only options ■ Client roaming options ■ LiveUpdate ■ Auto-Protect status ■ View virus list ■ Clear virus status
Client group	Clients assigned to the client group: ■ Scheduled scans ■ Virus definitions updating ■ Quarantine options ■ History configuration ■ Client Auto-Protect options ■ Client roaming options ■ Client administrator only options ■ LiveUpdate
Client	Read only

Server and client group scenario

A company has Telemarketing and Accounting departments. These departments have staff in the company's Boston, New York, and Newark offices.

All computers in both departments have been assigned to the same server group so that they receive virus definitions updates from the same source. However, IT reports indicate that the Telemarketing department is more vulnerable to threats than the Accounting department. As a result, the system administrator creates Telemarketing and Accounting client groups. Telemarketing clients share configuration options that strictly limit how users can interact with their threat protection.

Managing with server groups

You can create as many server groups as you need to manage your servers and clients efficiently.

Creating server groups

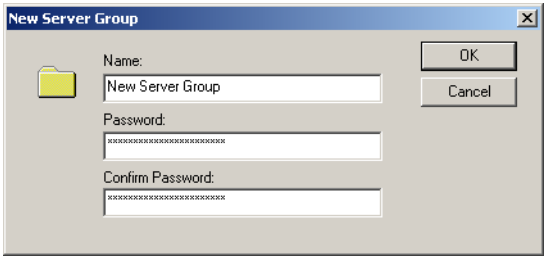
The installation program groups all of the servers that you select into one server group. This might be adequate if you want all of your managed computers running Symantec AntiVirus to use the same settings. However, if you want to make global configuration changes for groups of servers, you can create new server groups and easily use a drag-and-drop operation (or cut-and-paste) to move servers from one server group to another. When you move a server, all of its connected client computers move with it.

For example, if you have servers that require higher levels of protection, you can place all of them in the same server group and set special options to protect the server group. Note that you could also set up a new client group to achieve this same purpose.

See “About server and client groups” on page 38.

To create a server group

1 In the Symantec System Center console, in the left pane, right-click **System Hierarchy**, and then click **New** > **Server Group**.



2 In the New Server Group dialog box, type the name for the server group.

The name cannot have more than 47 characters.

3 In the Password text box, type a password for the server group.

4 In the Confirm Password text box, retype the password.

5 Click **OK**.

Each server group requires a primary server.

See "Selecting a primary server for a server group" on page 45.

Locking and unlocking server groups

You can lock a server group with a password to prevent unauthorized administrators from making configuration changes. You can add or change passwords at any time. The default password for the server group was created during installation.

Passwords are case sensitive.

Lock and unlock server groups

You can lock and unlock server groups as necessary. To unlock a server group, you must type its password correctly. Passwords are case sensitive. You can also prevent server groups from locking when you exit the console.

To lock a server group

◆ In the Symantec System Center console, in the left pane, right-click the server group that you want to lock, and then click **Lock Server Group**.

To unlock a server group

1 In the Symantec System Center console, in the left pane, right-click the server group, and then click **Unlock Server Group**.

2 Type the password to unlock the server group.

3 Check **Save This Password** if you do not want to retype the password in future sessions or for other server groups that have the same password.
If the password is correct, it will be saved.

To prevent unlocked server groups from locking when you exit the console

1 In the Symantec System Center console, in the left pane, right-click **System Hierarchy**, and then click **Properties**.

2 Uncheck **Lock All Server Groups When Exiting Console**.

Working with server group passwords

You can save, unsave, and change the server group password as necessary. To do so, the server group must have a primary server assigned to it. Empty passwords are allowed.

Saving server group passwords

You can save passwords if you do not want to reenter them in future sessions. Once the password is saved, you will not need to enter it when opening any server group that uses the same password. Saved passwords are DES encrypted and are stored in the registry of the local computer. When you attempt to unlock a server group, the Symantec System Center tries all of the saved passwords. You will be prompted for a password only if none of the saved passwords works.

Save or unsave server group passwords

The Save this password check box saves a password so that you do not have to enter it the next time the server group is opened.

When the password is saved, any previously accessed server group is either already unlocked or it does not prompt you for a password when you attempt to unlock it.

If you unchecked Lock All Server Groups When Exiting Console on the System Hierarchy properties page, the server group remains unlocked when the Symantec System Center console is reopened.

If you do not save passwords, all server groups are automatically locked by default each time that the Symantec System Center runs, even if you unlocked them the last time that you ran the program.

To save a server group password

1. In the Symantec System Center console, in the left pane, right-click a locked server group, and then click **Unlock Server Group**.
2. Type the password for the server group.
   If the server already has a password and you checked the Save This Password checkbox, the password dialog box does not appear. Create a new password in order to use this feature.
3. Check **Save This Password**.
4. Click **OK**.

See “Changing server group passwords” on page 44.

To no longer save the server group password

1. In the Symantec System Center console, in the left pane, right-click an unlocked server group, and then click **Lock Server Group**.
2. Type the old password.
3. Press **Tab**, and then type the new password.
4. Press **Tab**, and then retype the password.
5. Click **OK**.
6. Close the Symantec System Center console.
7. When prompted to save, click **No**.

Changing server group passwords

You can change server group passwords. For example, you may want to change passwords regularly for security purposes.

To change a server group password

1. In the Symantec System Center console, in the left pane, right-click the server group, and then click **Configure Server Group Password**.
2. Type the old password.
3. Press **Tab**, and then type the new password.
4. Press **Tab**, and then retype the password.
5. Click **OK**.

Renaming server groups

You can rename server groups as necessary.

To rename a server group

1. In the Symantec System Center console, in the left pane, unlock the server group that you want to rename, if necessary.
2. Right-click the server group, and then click **Rename**.
3. Type the new server group name.

Selecting a primary server for a server group

When you select a server group object in the Symantec System Center console and set options, the settings are saved to the primary server in the server group. Other servers in the server group will also use the new configuration.

You must specify which server in the server group is the primary server. No server is specified as the primary server by default. Until you designate a primary server, you cannot perform some Symantec product management operations.

Computers that are running any of the following operating systems can be primary servers:

- Windows 2000 Server/Advanced Server/Professional
- Windows XP Professional
- Windows NT 4.0 Server/Workstation
- NetWare Server

The primary server plays an important role, so select a stable server that is always running.

To select the primary server for a server group

- In the Symantec System Center console, in the left pane, right-click the server that you want to be the primary server, and then click **Make Server A Primary Server**.

Note: When changing primary servers, you may lose the AMS^2 alerts that you have set up. You can reconfigure the alerts on the new primary server, or export the alerts to the new server before you change primary servers.

Changing primary and parent servers

You can change primary servers and parent servers easily.

Change primary and parent servers

You can demote primary servers and promote secondary servers as necessary.

To change a parent server, you must copy a configurations file (Grc.dat) from the new parent to the client, and then restart the client.

The configurations file is a text format file that acts as a repository of changes being made to a group of clients. Configurations files are the heart of the communication between computers running Symantec AntiVirus server and computers running Symantec AntiVirus client. They store important information such as parent server identity and Symantec AntiVirus product configuration settings.

To change a primary server

1. In the Symantec System Center console, in the left pane, double-click the server group icon.
2. Right-click the secondary server that you are designating as a primary server, and then click **Make Server A Primary Server**.

To change a parent server of a client

1. On the intended parent server, copy the configurations file (Grc.dat) from \Program Files\SAV\.
2. On the client, paste the configurations file into one of the following folders:
   - For Windows 98\Me: C:\Program Files\Symantec AntiVirus
   - For Windows NT: C:\Winnt\Profiles\All Users\Application Data\Symantec\Symantec AntiVirus Corporate Edition\7.5
   - For Windows 2000\XP\2003: C:\Documents and Settings\All Users\Application Data\Symantec\Symantec AntiVirus Corporate Edition\7.5
3. Restart the client.

Moving a server to a different server group

You can move a server between groups using a drag-and-drop operation.

When you move a server, a server configurations file (Grcsrv.dat) is created on the server automatically. This file synchronizes the new server group settings to the server. The new server group must have a primary server.

The server configurations file is located in the same directory to which Symantec AntiVirus was installed on the server. It has the same format as a client configurations file (Grc.dat). It is created only when synchronizing a server to a new server group's settings.

The server configurations file works only for servers that are running Norton AntiVirus Corporate Edition version 7.5 or later, and Symantec AntiVirus server. For older servers, the Symantec System Center topology service copies registry settings from the primary server to the server that is being moved.

Viewing server groups

When you run the Symantec System Center console, you see servers that are running managed Symantec AntiVirus products in a tree format. Servers are grouped under server groups.

Viewing a single server group

You can view a single server group and its contents.

To view a single server group

- In the Symantec System Center console, right-click the server group, and then click **New Window From Here**.

Filtering the server group view

You can filter which server groups display in the Symantec System Center server group list. You can monitor and administer only the server groups that display in the list. By default, the Symantec System Center console displays all server groups. To remove server groups from your console, filter the view.

You receive notifications for displayed server groups only. If you filter a server group, you will not receive notifications from that server group.

To filter the server group view

1. In the Symantec System Center console, in the left pane, right-click **System Hierarchy**, and then click **View** > **Filter Server Group View**.
2. Uncheck the server groups that you want to filter from the server group list. All server groups display by default.
3. Click **OK**.

Deleting server groups

Before you can delete a server group, you must move its members to a new or existing server group.

To delete a server group

1. In the Symantec System Center console, in the left pane, right-click the server group that you want to delete, and then click **Unlock Server Group** if necessary.
2. In the server group that you want to delete, move any existing servers using a drag-and-drop operation into another server group.
   You can only delete a server group if it is empty.
3. Right-click the empty server group, and then click **Delete**.
4. Right-click **System Hierarchy**, and then click **Refresh**.

Enhancing server group security

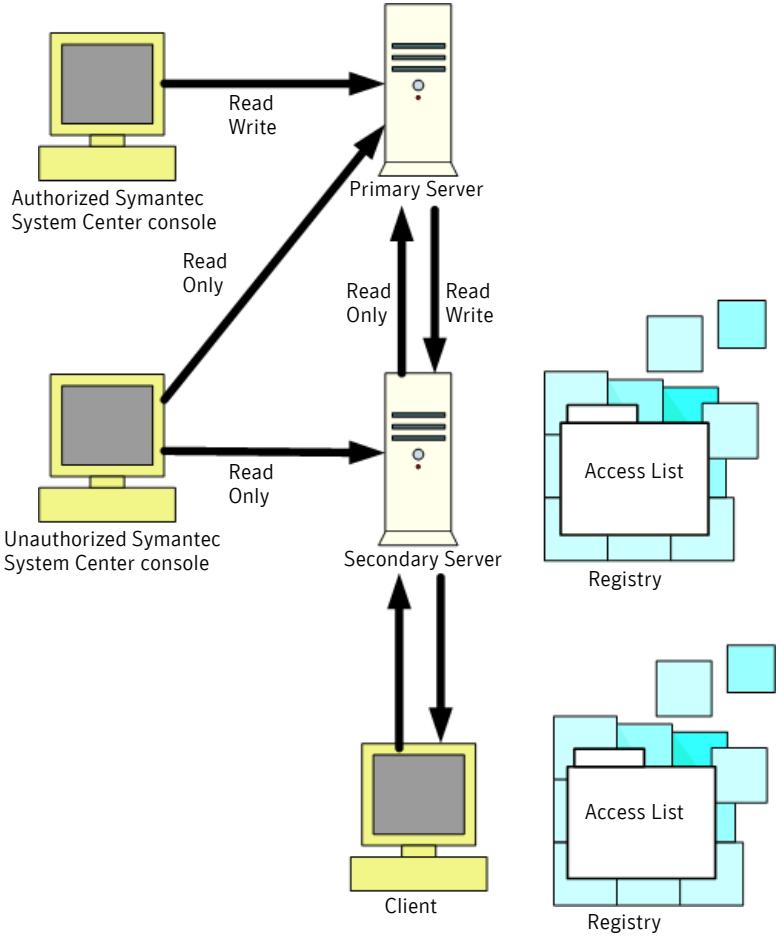
You can enhance the security that is provided by server group passwords by creating an access list that restricts inbound communication to only the IP and IPX addresses that are specified in the access list. For example, you can prevent an attacker who has access to the Symantec System Center console and a valid server group password from making unauthorized changes to the following:

- Server and client antivirus protection settings
- Auto-Protect settings
- Client group member assignments
- Primary server assignments
- Grc.dat file distribution
- Virus definitions file rollbacks

How the access list works

The access list is stored in the Windows registry on every computer that you want to protect. The address for each Symantec System Center console that communicates with the computer is validated against the access list. Symantec System Center consoles with IP or IPX addresses that are not included in the access list are limited to read-only access for antivirus protection and other settings (see Figure 1-2).

Figure 1-2 Enhanced server group security



Implementing enhanced server group security

You can perform the following tasks to implement protection and monitor unauthorized configuration changes:

- Choose which computers to protect.
- Create the access list.
- Roll out the access list.
- Log unauthorized configuration change attempts.

Choosing which computers to protect

The IP address of the computer running the Symantec System Center console should be included in the access list of every server in a server group. If you are only changing client group settings, you only need to include the address for the primary server.

You do not need to include the access list on every client. You can effectively lock down a server group and prevent IP spoofing by creating the access list on each server and leaving it empty. Add IP and IPX addresses to the access list only when you need to allow the Symantec System Center to access the server. Delete the value for an address when you no longer require access.

Creating the access list

To create an access list, you create a registry subkey and specify the authorized IP and IPX addresses.

To create the access list

1. Start a registry editor, such as Regedt32.
2. Open the HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion key.
3. Type **AccessList** as a new subkey.
4. In the AccessList subkey, add string values for IP and IPX addresses and subnet addresses of the computers that you want included in the access list. Use the following formats:

IP	Type **(IP)-<0.0.0.0>** where <0.0.0.0> is the numeric address for the computer.
IP subnet	Type **(IP)-<0.0.0.0>/<n>** where <0.0.0.0> is the numeric address for the computer and <n> is the subnet notation (for example, 16 or 24).
IPX	Type **(IPX)-<0000000:0000000000000>** where <0000000:0000000000000> is the numeric address for the computer.
IPX subnet	Type **(IPX)-<0000000>:<FFFFFFFFFFFFFFF>** where <0000000> is the numeric address for the computer and <FFFFFFFFFFFFFFF> is the subnet notation.

5. Close the registry editor.

Forcing the access list to reload

By default, the access list is refreshed every five minutes. If you want a change that you make to the list to take place immediately, you can force the reload.

To force the access list to reload

1. Start a registry editor, such as Regedt32.
2. Open the HKEY_LOCAL_MACHINE\SOFTWARE \INTEL\LANDesk\VirusProtect6\CurrentVersion\ProductControl key.
3. Type **ReadAccessList** as a new DWord.
4. Type **1** as the binary data associated with the ReadAccessList DWord value.
5. Close the registry editor.

Rolling out the access list

You can roll out the access list by performing the following tasks:

- Create a registry script with the information that you want to add to the access list, such as new values to authorize additional computers.
- Roll out the access list via your preferred distribution tool.
- Force the Symantec AntiVirus antivirus component to import the access list immediately.
  See "Forcing the access list to reload" on page 51.

Logging unauthorized configuration change attempts

When the Symantec AntiVirus antivirus component receives communication from an address that is not included in the access list, an event can be written to the Symantec AntiVirus Event Log. When the event occurs on a computer running Symantec AntiVirus, the log event is forwarded to the parent server.

Note: Unauthorized configuration change information is not written to logs by default.

Log changes and set logging frequency

You can edit the registry to log unauthorized changes. You can specify the frequency with which these items are logged.

To log unauthorized configuration changes

1. Start a registry editor, such as Regedt32.

2 Open the HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\AccessList key.

3 Type **LogAccessDenied** as a new DWord.

4 Type **1** as the binary data associated with the LogAccessDenied DWord value to enable logging.

5 Close the registry editor.

To set the frequency for logging unauthorized configuration change attempts

1 Start a registry editor, such as Regedt32.

2 Open the HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\AccessList key.

3 Type **LogAccessDeniedWindowMinutes** as a new DWord.

4 Do one of the following:

- To record every incident, type **0** as the binary data associated with the LogAccessDeniedWindowMinutes DWord value.
  The following message will appear when an unauthorized event occurs:
  Access denied to network communication from unauthorized address: <IP or IPX address> <port> where <IP or IPX address> is the IP or IPX address of the computer that was denied access and <port> is the port number that the computer attempted to use.
- To record incidents based on a frequency in minutes, type a number (in minutes) as the binary data associated with the LogAccessDeniedWindowMinutes DWord value.
  The following message will appear when an unauthorized event occurs:
  Access denied to network communication from unauthorized addresses <N> time(s) in the last <N> minute(s). Most recent address: <IP or IPX address> <port> where <N> is the frequency and the number of minutes, <IP or IPX address> is the IP or IPX address of the computer that was denied access, and <port> is the port number that the computer attempted to use.

5 Close the registry editor.

Managing with client groups

You can create as many client groups as you need to manage your clients efficiently.

Creating new client groups

All server groups contain a single Groups folder that contains all of the groups for that server group. When you create a new client group, the client group appears inside the Groups folder.

To create a new client group

1. In the Symantec System Center console, in the left pane, right-click the server group to which you want to add the client group, and then click **Unlock Server Group**.
2. Right-click the Groups folder, and then click **New Group**.
3. In the New Client Group dialog box, in the Enter name of the new client group text box, type the name for the new client group.
   The name cannot have more than 15 characters.
4. To apply the settings from an existing client group to the new client group, select the name of the existing client group from the drop-down list.
5. Click **Create**.

Adding clients to a client group

Computers that are running Symantec AntiVirus server, client, and legacy versions can be added to client groups. Both clients are treated identically. If a legacy Norton AntiVirus client does not have the feature for which a configuration option setting is set, the setting is ignored.

Note: Only Symantec AntiVirus servers support client groups; legacy versions of Norton AntiVirus Corporate Edition do not.

A client can belong to only one client group.

To add a client to a client group

1. In the Symantec System Center console, in the left pane, click the server that contains the client.
2. In the right pane, move the client to the client group using a drag-and-drop operation.

Configuring settings and running tasks at the client group level

You can set configuration options and run tasks at the client group level. The settings will be applied to, or the task run on, all clients in the client group.

To configure settings and run tasks at the client group level

1. In the Symantec System Center console, in the left pane, right-click the client group.
2. Click **All Tasks**.
3. Click the product for which you want to set options.
4. Click the type of settings that you want to configure or the task that you want to run.

Finding client group settings

Client group settings are stored in the primary server's registry. They are rolled out to each server in a client group configurations file (Grcgrp.dat). The primary server packages all client group settings into the client group configurations file, and then copies it to each secondary server in the server group. The secondary server rolls out the settings to the clients that it manages.

See the *Symantec AntiVirus Reference Guide* for information about configurations files.

Moving clients in client groups

You can move clients from one client group to another using a drag-and-drop operation. Once you move the client, it receives the new client group's configuration settings.

Viewing client groups

When you view client groups, you can do the following:

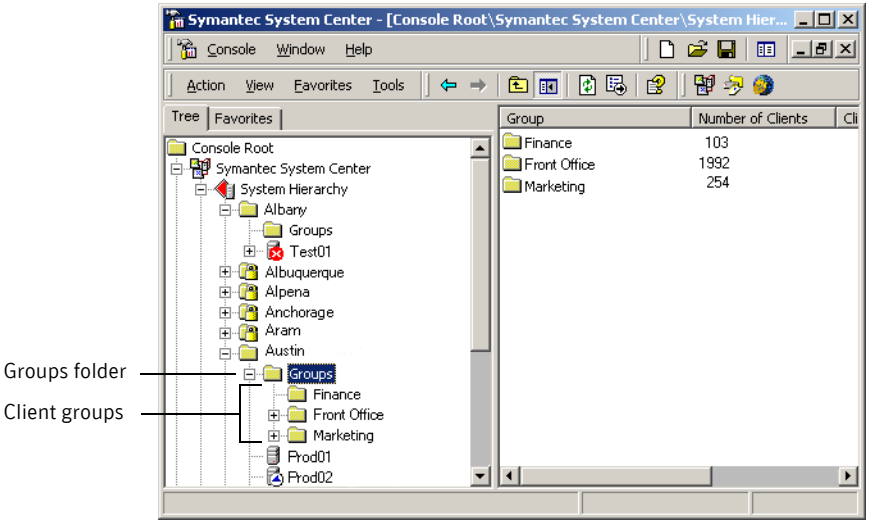
- View a single client group.
- View information about client groups.
- Filter the client group view to show only the information that interests you.

Viewing a single client group

You can view the contents of client groups one group at a time.

To view a single client group

1. In the Symantec System Center console, in the left pane, right-click the server group that contains the client group, and then click **Unlock Server Group**.
2. Double-click the server group.
3. Double-click the **Groups** folder.



The client groups appear nested beneath the Groups folder.

Viewing information about client groups

When the Groups folder is selected in the left pane and Default Console View or a Symantec product view is selected from the View menu, the client groups appear in the right pane along with information specific to the view. For example, when the Default Console View is active, the number of clients in each client group appears.

Client group filtering must be enabled for the clients to be enumerated. When you select the Groups folder, the number of clients reported for each client group may not be accurate until a client group is selected.

See "Filtering the client group view" on page 56.

Filtering the client group view

When you select a client group in the left pane, all of the clients assigned to it can appear in the right pane.

Filtering improves client viewing performance in the Symantec System Center console. However, if there are many clients and servers in the server group, filtering may have a performance impact. The clients must be enumerated to display the client groups accurately. Filtering is disabled by default.

To filter the client group view

1. In the Symantec System Center console, on the Tools menu, click **SSC Console Options**.
2. In the SSC Console Options Properties dialog box, on the Client Filter tab, under Group Options, click **Show client machines when viewing Groups**.
3. Under Server Options, click the following options as desired:
   - Build client lists when the Server Group is unlocked: Enumerates all clients in the server group when it is unlocked.
     When this option is unchecked, clients are not added to their client groups until the server is selected. The number of clients in a client group is not accurate until all the servers in the server group have been selected.
   - Cache all client info (including clients in locked Server Groups): Enumerates clients in both unlocked and locked server groups that are discovered by the Topology Service.

   These options may impact performance if there are many clients and servers in the server group.
4. Under Client Options, check **Indicate when clients are offline** to display a unique icon in the Symantec System Center console when a client is not connected to the network.
5. Click **OK**.
6. On the Action menu, click **Refresh**.

Renaming client groups

The Symantec System Center does not support renaming client groups directly. If you need to change the client group name, you must complete the following tasks:

- Create a new client group, importing settings from another client group if desired.
  See "Creating new client groups" on page 53.
- Move clients from the old client group to the new client group using a drag-and-drop operation.
- Delete the old client group.
  See "Deleting client groups" on page 57.

Deleting client groups

Before you delete a client group, you may want to reassign the clients to another client group.

When a client group is deleted, the clients that are assigned to it retain the settings of the deleted client group. The clients are not assigned new settings until one of the following actions occurs:

- The client checks in with its parent server. The client is then assigned the server's default settings for unassigned clients.
- The client is assigned to another client group. The client is then assigned the settings of the new client group.

If you delete a client group, and then recreate it before the clients check in with their parent servers or are reassigned, the clients resume membership in the group automatically. They continue to assume the settings of that group.

To delete a client group

1. In the Symantec System Center console, in the left pane, unlock the server group from which you want to delete the client group.
2. Double-click the server group.
3. Double-click the **Groups** folder.
4. Right-click the target group, and then click **Delete Group**.
5. Click **Yes**.
6. Click **Delete**.

Configuring clients directly

You can allow for the direct configuration of Symantec AntiVirus clients. The options that you set directly remain in force until a new configurations file (Grc.dat) is copied to the client.

To allow direct client configuring

- In the SSC Console Options Properties dialog box, on the Client Filter tab, under Group Options, click **Allow direct configuration of individual clients**.
  This option is unchecked by default.

Changing an unmanaged client into a managed client (and the reverse)

You can change an unmanaged client into a managed client, and a managed client into an unmanaged client.

Change a client's management mode

When you change an unmanaged client into a managed client, it will appear in and be configurable by the Symantec System Center. Similarly, changing a managed client into an unmanaged client will cause the client to disappear from the Symantec System Center.

To change an unmanaged client into a managed client

1. Decide which server is going to be the client's parent server.
2. Open Network Neighborhood or My Network Places.
3. Locate and double-click the computer that you want to act as the parent server.
   The Symantec AntiVirus server must be installed on the computer that you select.
4. Open the **VPHOME\Clt-inst\Win32** folder.
5. Copy Grc.dat to the desired location.
6. Paste the Grc.dat file to one of the following folders on the unmanaged client:
   - Windows 98/Me: C:\Program Files\Symantec AntiVirus
   - Windows NT 4.0: C:\Winnt\Profiles\All Users\Application Data\Symantec\Symantec AntiVirus Corporate Edition\7.5

- Windows 2000/XP/2003: C:\Documents and Settings\All Users\Application Data\Symantec\Symantec AntiVirus Corporate Edition\7.5

7 Restart the client.

To change a managed client into an unmanaged client

1 Uninstall Symantec AntiVirus from the client workstation.

2 Using the registry editor, delete the following subkey: HKEY_LOCAL_MACHINE\Software\Intel\LANDesk\VirusProtect6

3 Reinstall Symantec AntiVirus.

4 When prompted to make the client either managed or unmanaged, choose unmanaged.

How settings propagate

The method that Symantec AntiVirus uses to propagate settings depends upon the item that you choose in the Symantec System Center console.

Table 1-4 describes how settings propagate when you choose server groups, servers, and clients.

Table 1-4 How settings propagate from the Symantec System Center console

Object	Description
Server groups	When you set options at the server group level, and then click OK, the Symantec System Center topology service communicates directly with the primary server and only overwrites the settings that you change. If you click Cancel, no options change. The primary server updates other servers in the server group through a temporary Grcgrp.dat file, and only overwrites the settings that you change. Parent servers update their clients by rolling out a new Grc.dat file. This file replaces the existing Grc.dat file. Custom settings in the old Grc.dat file are not retained. Whenever you click Reset All, Symantec AntiVirus overwrites all settings in the dialog box.

Table 1-4 How settings propagate from the Symantec System Center console

Object	Description
Servers	When you set options at the server level, and then click OK, the Symantec System Center topology service communicates directly with the selected server. Only the selected server is affected. If you click Cancel, no options change. If you click OK without changing options, Symantec AntiVirus does not overwrite the server's current options.
Client groups	When you set options at the client group level, and then click OK, the primary server creates a Grcgrp.dat file and sends it to secondary servers. The secondary servers update their clients by rolling out a new Grc.dat file. This file replaces the existing Grc.dat file. Custom settings in the old Grc.dat file are not retained. If you click Cancel, no options change.
Clients	When you set options at the client level, and then click OK, the System Center Topology service communicates with the client directly and makes the single change in the registry. If you click Cancel, no options change.

Note: Auto-Protect scanning settings must be locked before they are propagated to clients. See "Scanning for viruses and other threats" on page 89.

New Grc.dat files overwrite old Grc.dat files

New Grc.dat files are propagated and overwrite old Grc.dat files any time that they are sent to the client. This behavior occurs even when you open a Symantec AntiVirus window or dialog box that contains options from the Symantec System Center console, and then click OK without changing options. If the earlier Grc.dat version contained custom settings that are not in the new Grc.dat, the settings are overwritten.

See the *Symantec AntiVirus Reference Guide* for additional information on using Grc.dat files.

Chapter 2

Setting up the Alert Management System

This chapter includes the following topics:

- About the Alert Management System
- How Alert Management System works
- Configuring alert actions
- Working with configured alerts
- Using the Alert Management System Alert Log
- Forwarding alerts from unmanaged clients

About the Alert Management System

Alert Management System^2 (AMS^2) provides emergency management capabilities. AMS^2 supports alerts on supported NetWare servers, Windows NT/2000 servers and workstations, Windows XP Home Edition/Professional, and Windows 98/Me workstations.

AMS^2 can generate alerts through the following means:

- Message box
- Broadcast
- Internet mail
- Page
- Run a program
- Write to the Windows NT Event Log

- Send an SNMP trap
- Load an NLM

Note: Alerts generated through SNMP traps can be sent to any third-party SNMP management console. To receive SNMP traps from Symantec AntiVirus, you must have the Symantec System Center and AMS^2 installed. (Only a primary server will run AMS^2. You must use the Symantec System Center to designate the primary server.)

See "Configuring the Send SNMP Trap alert action" on page 74.

How Alert Management System works

AMS^2 alerts are transferred from Symantec AntiVirus into AMS^2 through the Symantec AntiVirus service. On a computer running the Symantec AntiVirus client, the Symantec AntiVirus service waits for an event thread that requires an alert.

These threads can be generated by the following events:

- Configuration change
- Default Alert
- Symantec AntiVirus startup/shutdown
- Scan Start/Stop
- Virus Definitions File Update
- Threat Found

If you have configured an alert for any of these events, when the event occurs it will generate a thread. The thread prompts the Symantec AntiVirus service to create a threat information block, which it forwards to the client's parent server. When the parent server receives the threat information block, it enters it into its AMS^2 log. The threat information is then forwarded to the primary server, which makes a call to AMS^2. AMS^2 enters the information into the AMS^2 database and acts on it. The action taken depends upon how you have the alert configured.

Communication in AMS^2 is carried out through CBA, which is part of the Intel Communication Method.

Configuring alert actions

AMS^2 lets you configure many different methods of notification—such as pager, SNMP, and email—for detected threats and configuration changes.

Alert configuration tasks

AMS^2 alert configuration requires the following related tasks:

- Select an alert in the Alert Actions dialog box.
- Select the alert action that you want to configure for that alert. The alert action is the response AMS^2 sends you when an alert parameter is detected.
- Configure the alert action that you selected.

For example, you could configure the Send Page alert action to notify you if a threat was detected on a protected server. The pager message could also include information such as threat name and type, and actions taken on the infected file.

There are no default alert actions for any of the alerts. Until you configure AMS^2, no alerts are generated, though threat events are logged in the AMS^2 log file.

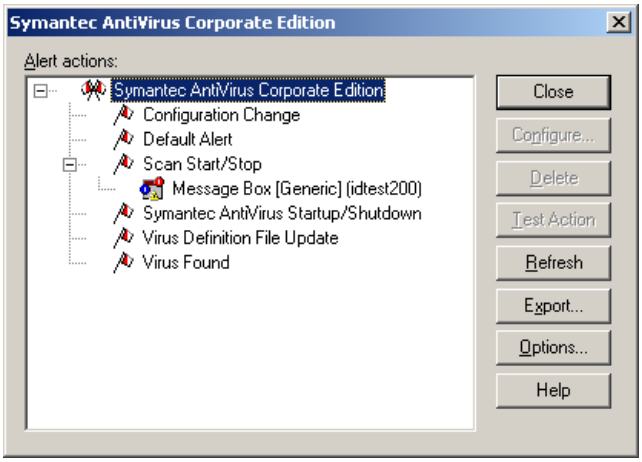
You can set up more than one action for each alert. Once you have configured alert actions for an alert, a plus (+) or minus (-) sign appears next to each configured alert, depending on whether the entry is collapsed or expanded.

Each AMS^2 alert action has its own configuration wizard. Once you have configured an alert action, the action appears in the Alert Actions dialog box under the alert for which you configured the action.

All alert actions execute on the computer that you select when you configure the action. Actions will not execute if you configure them on a computer that doesn't support that particular action. For example, any computer that you configure the Send Page action on must have a modem.

To configure an alert

1 In the Symantec System Center console, right-click the server group, and then click **All Tasks** > **AMS** > **Configure**.



2 Select an alert, and then click **Configure** to define an alert action.

Configuring alert action messages

For alert actions that generate messages (for example, Message Box, Broadcast, Send Page, and Send Internet Mail), you can include additional information from the alert that generated the message. The additional types of information appear in Table 2-1.

Table 2-1 Alert parameters

Alert parameter	Description
<Alert name>	The name of the alert; for example, Symantec AntiVirus Startup/Shutdown
<Computer>	The name of the computer where the alert originated
<Host Name>	Alert server name
<Date>	The date when the notification was generated
<Time>	The time when the notification was generated
<Severity>	The level of severity assigned to the alert; for example, Critical or Non-Critical

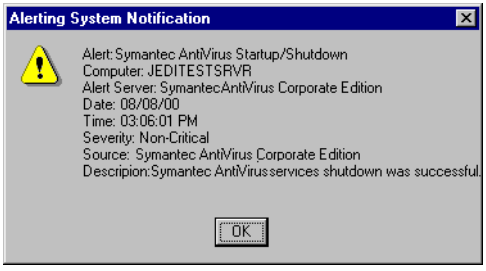
Table 2-1 Alert parameters

Alert parameter	Description
<Source>	The product source of the notification; for example, Symantec AntiVirus
<Description>	More information about the nature of the notification; for example, “Symantec AntiVirus services shutdown was successful”

The Message dialog box includes a text box in which you can enter as many as 256 characters to be used as the text of the message that you want to send. You can use the variables in Alert parameters to insert information generated by the alert. Parameters are delimited by < and > characters. Each parameter placeholder that you add to the Message text box is substituted with corresponding alert information when an alert occurs.

See Figure 2-1.

Figure 2-1 Alerting System Notification



See “Testing configured alert actions” on page 78.

If the AMS[2] alerting system detects a message larger than 1 KB, the message will not be delivered. If you have configured a default alert message, it will be delivered instead. You can configure this default alert to notify you when a message exceeds 1 KB.

To configure a default alert message

1. In the Symantec System Center console, right-click the server group, and then click **All Tasks** > **AMS** > **Configure**.
2. Click **Default Alert**, and then click **Configure**.
3. Click **Message Box**, and then click **Next**.
4. Select a computer on which to execute the action, and then click **Next**.

5 Select whether you want an error beep and whether you want the dialog box to always appear on top until it is cleared.

6 Click **Next**.

7 Type the action name that describes the message that you are configuring. The action name and the action computer name appear in the Alert Actions dialog box beside this action.

8 In the Message box, do one of the following:

- Type custom message text that you want to display and move available parameters that you want from Alert Parameters to the Message box.
- Click **Default** to use the default message information for this alert action, and then type custom message text that you want to display. Note that the default message includes the following information:

  Computer: <Host Name>

  <Host Name> is the name of the alert server. To include the name of the computer where the notification originated, you must add the <Computer> parameter to the message.

9 Click **Finish**.

Speeding up alert configuration

If you have a large network, you may be able to speed up and simplify your configuration of AMS^2 by only searching a certain segment of your network for AMS^2 computers.

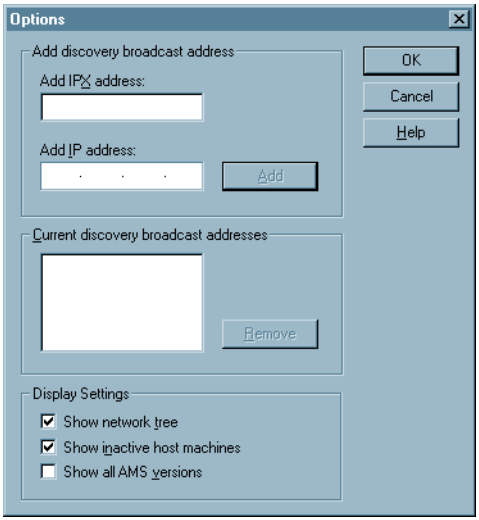
This is especially useful if you manage a large network with many different servers, and you want to confine your search to one section of the network, or one specific subnet mask. The process is faster when you limit your search, and alerts are contained in the defined network segment.

You can get a faster response across a large network if you limit the network segments. You can use this option with either IPX or TCP/IP network protocols. You can specify whether you want AMS^2 to discover clients only within a certain octet or subnet mask.

To speed up alert configuration

1 In the Symantec System Center console, right-click the server group, and then click **All Tasks** > **AMS** > **Configure**.

2 Click **Options**.



3 In the Options dialog box, do one of the following:

- If you use an IPX network, in the Add IPX address box, type the IPX network broadcast address where you want to search for AMS^2 computers.
- If you use a TCP/IP network, in the Add IP address box, type the TCP/IP network broadcast address where you want to search for AMS^2 computers.
  This is the first three segments of the computer's IP address followed by an all-inclusive segment. For example, if you enter a search broadcast address of 192.168.0.255, any of the 256 computers with AMS^2 in the subnet will receive the broadcast. So if you are searching for an AMS^2 computer that has an IP address of 192.168.0.50, you will find it.

4 Click **Add** to add this net address to the Current discovery broadcast addresses list.
Only broadcast networks listed here are searched to discover new AMS^2 computers. If you have not specified any broadcast networks, the entire network is searched each time that you start a discovery.

5 To remove a net address that is no longer needed from the Current discovery broadcast addresses list, select the address, and then click **Remove**.
When you remove a net address from this list, it doesn't disable that section of the network. Removing a net address only prevents AMS^2 from searching that section of the network for AMS^2 computers.

6 Click **OK** to save the list and return to the Alert Actions dialog box.

Configuring the Message Box alert action

The Message Box alert action displays a message box on the computer from which you configure the action. You can select whether the message box sounds a beep when it appears and whether the message box always appears on the screen until cleared.

To configure the Message Box alert action

1 In the Symantec System Center console, right-click the server group, and then click **All Tasks** > **AMS** > **Configure**.

2 Select the alert for which you want to configure alert actions.

3 Click **Configure**.

4 Click **Message Box**, and then click **Next**.

5 Select a computer to execute the action, and then click **Next**.

6 Select whether you want an error beep and whether you want the dialog box to always appear on top until it is cleared.

7 Click **Next**.

8 Type an action name.
The action name and the action computer name appear in the Alert Actions dialog box beside this action.

9 In the Message box, type any message text that you want to display and move available parameters that you want from Alert Parameters to the Message box.

10 Click **Finish**.

Configuring the Broadcast alert action

The Broadcast alert action sends a message to all computers logged on to the server that generates the alert.

To configure the Broadcast alert action

1. In the Symantec System Center console, right-click the server group, and then click **All Tasks** > **AMS** > **Configure**.
2. Select the alert for which you want to configure alert actions.
3. Click **Configure**.
4. Click **Broadcast**, and then click **Next**.
5. Select a computer to execute the action, and then click **Next**.
6. In the Message box, type any message text that you want to display and move available parameters you want from Alert Parameters to the Message box.
7. Type an action name.
   The action name and the action computer name will appear in the Alert Actions dialog box beside this action.
8. Click **Finish**.

Configuring the Run Program alert action

The Run Program alert action runs a program on the computer for which you configure the alert action. You must complete two fields in the Run Program dialog box.

The Program box should contain the full path to the program that you want to run. The Command Line box should contain any command-line options for that program. The program that you select should be on the computer's local drive to ensure that AMS^2 can find it.

If you are running the program on a remote computer, you must enter the path to the program from that computer.

If you are running a Windows program, you can select whether that program runs in a normal, minimized, or maximized state. This option has no effect on DOS programs.

To configure the Run Program alert action

1. In the Symantec System Center console, right-click the server group, and then click **All Tasks** > **AMS** > **Configure**.
2. Select the alert for which you want to configure alert actions.
3. Click **Configure**.
4. Click **Run Program**, and then click **Next**.
5. Select a computer to execute the action, and then click **Next**.
6. Type the full path name to the program that you want to run, including the program name.
7. Type any command-line options that you want the program to use.
8. Select an execution state of normal, minimized, or maximized.
9. Click **Finish**.

Configuring the Load An NLM alert action

The Load An NLM alert action loads a NetWare Loadable Module (NLM) on a selected NetWare server when the AMS^2 alert occurs. You must configure this alert to determine which NLM is loaded, and the server onto which it loads. This alert action is similar to the Run Program alert action for a Windows NT computer.

For example, if you were running the Symantec AntiVirus management snap-in, you could configure the Load An NLM alert action to load an NLM that you or a third party created on a selected NetWare server when Symantec AntiVirus detects a threat. This NLM could monitor who accesses the server and who is using the infected file. It could also back up files should the server crash because of the infection.

To configure the Load An NLM alert action

1. In the Symantec System Center console, right-click the server group, and then click **All Tasks** > **AMS** > **Configure**.
2. Select the alert for which you want to configure alert actions.
3. Click **Configure**.
4. Click **Load An NLM**, and then click **Next**.
   The first time that you configure this action, AMS^2 needs to search the network for NetWare computers that can perform this action.
   When completed, the NetWare computers appear in tree format.

5 If the computer that you are looking for does not appear in the list, click **Discover** to search for all computers again and find that computer.

6 Select the computer where the NLM will load, and then click **Next**.

7 Type or select the NLM to load.
NLMs are usually stored in the SYS:SYSTEM directory on NetWare servers.

8 Type any command-line options you want the program to use.

9 Click **Finish**.

Configuring the Send Internet Mail alert action

The Send Internet Mail alert action sends an Internet mail message to the user that you specify. When using the Send Internet Mail alert action, you need to also specify the SMTP Internet mail server through which the alert action will send the message. If you specify the mail server by name, you need to have a DNS server configured so that the Send Internet Mail alert action can resolve the server's IP address. If you do not have a DNS server, you can enter the mail server's IP address directly.

If you do not have access to an SMTP Internet mail server at your site, this alert action won't work.

To configure the Send Internet Mail alert action

1 In the Symantec System Center console, right-click the server group, and then click **All Tasks** > **AMS** > **Configure**.

2 Select the alert for which you want to configure alert actions.

3 Click **Configure**.

4 Click **Send Internet Mail**, and then click **Next**.

5 Select the computer to execute the action, and then click **Next**.

6 In the Internet Address, Sender Name, Subject, and Mail Server boxes, type or select information as appropriate.
It is preferable to provide the mail server's IP address rather than its name.
The Sender Name box must contain a valid Internet email address. Most email servers will not send a message if the server can't validate the sender's email address.

7 Click **Next**.

8 In the Message box, type any message text you need and move available parameters you want from Alert Parameters to the Message box.

9 Type an action name.
The action name and the action computer name appear in the Alert Actions dialog box beside this action.

10 Click **Finish**.

Configuring the Send Page alert action

The Send Page alert action sends a pager message to the number that you specify. Any computer that you configure a Send Page action on needs to have a modem.

See "Testing configured alert actions" on page 78.

Send Page alert action configuration is divided into the following parts:

- Configuring a modem for AMS^2 to use
- Configuring for a paging service
- Entering a pager message

To configure the Send Page alert action

1 In the Symantec System Center console, right-click the server group, and then click **All Tasks** > **AMS** > **Configure**.

2 Select the alert for which you want to configure alert actions.

3 Click **Configure**.

4 Click **Send Page**, and then click **Next**.

5 Select a computer to execute the action, and then click **Next**.

6 Type the access telephone number that you are calling to reach the paging service.
Be sure to include any numbers necessary to access an outside line from your site.

7 Type the pager ID number and password that you use to access the paging service network.
If your paging service doesn't use a password, leave the Password box blank.

8 Select your service type.
If your paging service is not listed, try one of the generic types.
See "Configuring for a paging service" on page 73.

9 Click **Next**.
If you're creating a message for an alphanumeric pager, in the Message box type any message text you want to display and move available parameters from Alert Parameters to the Message box.
If you're creating a message for a numeric pager, you can only type numbers in the Message box.

10 Type an action name.
The action name and the action computer name appear in the Alert Actions dialog box beside this action.

11 Click **Finish**.

Configuring for a paging service

You can access a paging service either directly or indirectly. Direct paging refers to dialing the service provider network access phone number and accessing the service provider's computer network directly to enter the pager identification number. The paging service network then sends the message to the pager.

AMS^2 alerting does not work with indirect paging. Indirect paging involves calling a paging service, speaking with an operator, and giving the operator the pager's identification number. The paging service operator enters the information into the paging network, and then sends the message to the pager. The indirect paging method that is often used when contacting the network directly may be a toll call, and the pager service offers toll-free service through the operator.

You need to configure the Pager alert action for your paging service. At a minimum, this information includes the paging service phone number and the name of the paging service that you are using.

Always put the paging service's phone number in the Send Page dialog box's Service Provider box. If your paging service is not in the Send Page dialog box's Service drop-down list, you can try using the Generic Beeper or the Generic Alphanumeric service (select the one that matches the type of pager that you are using). Type the password that you use to access the paging service network in the Password box.

If the generic service that you select doesn't work with your pager, you must configure the communication parameters that the Send Page alert action needs to use. This information includes the baud rate, data and stop bits, parity, and the paging protocol used by your paging service. If your paging service is in the Service drop-down list, these parameters are configured automatically when you select the service.

To configure the Send Page alert action for an unlisted paging service

1. In the Symantec System Center console, right-click the server group, and then click **All Tasks** > **AMS** > **Configure**.
2. Select the alert for which you want to configure alert actions.
3. Click **Configure**.
4. Click **Send Page**, and then click **Next**.
5. Select a computer to execute the action, and then click **Next**.
6. Click **Settings**.
7. Type the protocol, maximum message length, baud rate, data bits, stop bits, and parity that your paging service requires.
   You can get this information from your paging service.
8. Click **OK**, and then continue configuring the pager action starting with step 6 in "To configure the Send Page alert action" on page 72.

Entering a pager message

The Send Page alert action supports both alphanumeric and numeric-only pagers (numeric-only pagers are sometimes called beepers).

If you're paging an alphanumeric pager, the message can include any text that you type in and information from the alert that generated the message. This message should not exceed the maximum number of characters that your paging service supports; otherwise, you could get a truncated message.

If you're paging a numeric-only pager, you may want to create a system of server numbers and numeric error codes that correspond to alerts that you configure. For instance, you could create a system where "1" refers to your main production server and number "101" means some specific event has occurred. If you received the message "1 101," then you would know that the event had occurred on your main production server.

Configuring the Send SNMP Trap alert action

Simple Network Management Protocol (SNMP) is a message-based protocol based on a manager/agent model consisting of Get, GetNext, and Set messages and responses. SNMP uses traps to report exception conditions such as component failures and threshold violations.

AMS^2 can generate an SNMP trap when an alert occurs. You can configure systems generating alerts to send these traps to a management console, such as HP OpenView, Tivoli Enterprise Console, or Computer Associates Unicenter.

You must specify the address (either IP or IPX) of the computers to which you want SNMP traps sent.

To configure the Send SNMP Trap alert action

1. In the Symantec System Center console, right-click the server group, and then click **All Tasks** > **AMS** > **Configure**.
2. Select the alert for which you want to configure alert actions.
3. Click **Configure**.
4. Click **Send SNMP Trap**, and then click **Next**.
5. Select a computer to execute the action, and then click **Next**.
6. In the SNMP trap, type any message text that you want to display and move the parameters that you want from Alert Parameters to the Message box.
7. Type an action name.
   The action name and the action computer name appear in the Alert Actions dialog box beside this action.
8. Click **Finish**.

Configuring trap destinations for Windows NT 4.0

You can configure SNMP traps for Windows NT 4.0.

To configure trap destinations for Windows NT 4.0

1. In the Windows NT Control Panel, double-click **Network**.
2. Click **Services**.
3. Click **SNMP Service**, and then click **Properties**.
4. Click **Traps**.
5. In the Community Name box, click **Public**.
6. If there is no public entry in the list, type it in, and then click **Add**.
7. Under Trap Destinations, click **Add**.
8. Type the addresses of the computers to which you want traps sent, and then click **Add**.
9. Click **OK**, and then click **Close**.

Configuring trap destinations for Windows 2000 Server

You can configure SNMP traps for Windows 2000 Server.

To configure trap destinations for Windows 2000 Server

1. On the Windows taskbar, click **Start** > **Settings** > **Control Panel**.
2. Double-click **Administrative Tools**.
3. Double-click **Computer Management**.
4. Click **Services and Applications**.
5. Click **Services**.
6. In the right pane, click **SNMP Service**.
7. On the Action menu, click **Properties**.
8. On the Traps tab, under Community name, type the case-sensitive community name to which this computer will send trap messages, and then click **Add to List**.
9. In Trap destinations, click **Add**.
10. In Host name, IP or IPX address, type information for the host, and click **Add**.
11. Repeat steps 8 through 10 until you have added all the communities and trap destinations you want.

Configuring trap destinations for NetWare

You can configure SNMP traps for NetWare 5.x and 6.x servers.

To configure trap destinations for NetWare

1. In the NetWare server console, type:
   load inetcfg
2. Select **Protocols** and press **Enter**.
3. Select **TCP/IP** and press **Enter**.
4. Select **SNMP Manager Table**, and then press **Enter** to display the SNMP Manager Table.

5 Do one of the following:
   - To modify an existing address, select it, and then press **Enter**.
   - To add a new address, press **Insert**, type an IP address, and then press **Enter**.
   - To delete an address, select it, press **Delete**, and then press **Enter** to confirm the deletion.
6 Press the **Esc** key to close the dialog box.
7 Press **Enter** to confirm the change to the database.

Configuring the Write To Event Log alert action

The Write To Event Log alert action creates an entry in the Windows NT/2000/XP Event Log's Application Log. This entry is logged on the server from which the alert came. This alert action is available only on Windows NT/2000/XP computers.

To configure the Write To Event Log alert action

1 In the Symantec System Center console, right-click the server group, and then click **All Tasks** > **AMS** > **Configure**.
2 Select the alert for which you want to configure alert actions.
3 Click **Configure**.
4 Click **Write To Event Log**, and then click **Next**.
5 Select a computer to execute the action, and then click **Next**.
6 In the Message box, type any message text that you want to display and move parameters that you want from Alert Parameters to the Message box.
7 Type an action name.
   The action name and the action computer name appear in the Alert Actions dialog box beside this action.
8 Click **Finish**.

Working with configured alerts

Once you have configured alert actions, you can do the following:

- Test them to make sure they work as expected.
- Delete them.
- Export them to other computers.

Testing configured alert actions

After you configure alert actions, you can test them in the Alert Actions dialog box. When you select an alert and then click Test Action, all alert actions configured for that alert execute. When you select a specific alert action and click Test Action, only that alert action executes.

To test an alert

- In the Alert Actions dialog box, select an alert, and then click **Test Action**.

Deleting an alert action from an alert

You can delete actions associated with an alert as necessary.

To delete an alert action from an alert

1. In the Symantec System Center console, right-click the server group, and then click **All Tasks** > **AMS** > **Configure**.
2. Select the alert action you want to delete, and then click **Delete**.

Exporting alert actions to other computers

Each computer that generates AMS^2 alerts stores its alert information in a local AMS^2 database. Typically, the alerts and actions stored in one database are not visible to AMS^2 databases on other computers.

There may be times when you want to duplicate configurations of AMS^2 alert actions on a computer across multiple computers so you do not have to repeat your work. The AMS^2 export option lets you export alert actions to other computers that generate AMS^2 alerts.

Alert actions, such as a Send Page alert action configuration or a Message Box alert action configuration, only export if the alert for which you configured the action exists on both computers. In most cases, you can ensure this is the case by installing the same application on both computers. This way, both applications will register their alerts with their respective AMS^2 databases.

When you export alert actions from one computer to another, you have the choice of exporting a single alert action or all alert actions. Once AMS^2 exports alert actions to a computer, AMS^2 displays the Export Status dialog box to let you know the results of the export.

If the export option cannot export an alert action because the alert for which the action was configured doesn't exist on the target computer (or for any other reason), the Export Status dialog box indicates that the alert action couldn't be

exported. Alert actions also may fail to export if the target computer's AMS^2 installation is not working correctly.

To export alert actions to other computers

1. In the Symantec System Center console, right-click the server group, and then click **All Tasks** > **AMS** > **Configure**.
2. Do one of the following:
   - Click the **Symantec AntiVirus** folder if you want to export all alerts associated with Symantec AntiVirus.
   - Select either an alert (if you want to export all of that alert's actions) or a specific alert action (if you want to export only the selected alert action).
3. Click **Export**.
4. In the Available Computers list, double-click the computers that you want to receive the alert actions you selected.
   The computers will be added to the Selected Computers list.
   If the computer you want has AMS^2 active on it and it is not in the Available Computers list, click **Discover** to rediscover computers with AMS^2.
5. Click **Export**.
6. Click **Yes** in reply to the confirmation message.
7. In the Export Status dialog box, verify that the alert actions exported successfully.

Viewing export status

After AMS^2 exports alert actions to the computers that you selected in the Select Computers dialog box, AMS^2 displays the export results in the Export Status dialog box.

The Export Status dialog box displays alert actions that do not export successfully. If alerts do not export successfully, it may be for the following reasons:

- AMS^2 is not up or working correctly on the target computer. Verify AMS^2 by testing a configured alert action on that computer from the Alert Actions dialog box.
- The alert for which the action was configured doesn't exist on the target computer. Make sure that the application that registered the alert with AMS^2 on the source computer is installed on the target computer.

Using the Alert Management System Alert Log

You can use the Alert Log to view a list of all alerts generated by network computers running Symantec AntiVirus.

You can configure the Alert Log to do one of the following:

- Display only the alerts that match the conditions that you specify.
- Display a specified number of entries.

The Alert Log displays a list of alerts with the following information about each alert:

- Alert Name
- Source
- Computer
- Date
- Time
- Severity

In addition to the basic information the Alert Log dialog box displays, you can access more detailed information about each alert in the Alert Information dialog box.

Each server stores its own copy of the Alert Log locally. When you select a server and view its alert log, you're actually retrieving a copy of that server's Alert Log to your local console. Therefore, if that server is not powered on or available, you won't be able to retrieve its Alert Log for viewing.

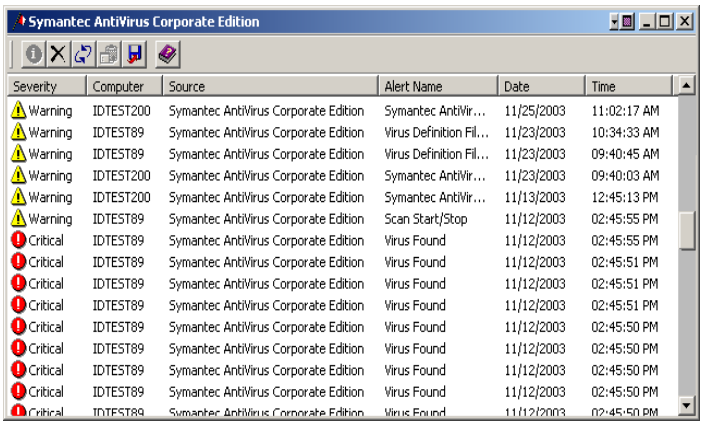
View and interact with the Alert Log

You can view the Alert Log and interact with it in the following ways:

- Change the number of entries displayed in the log
- Delete entries
- Copy the contents to the clipboard

To view the Alert Log

◆ Right-click the server group, and then click **All Tasks** > **AMS** > **View Log**.



Severity	Computer	Source	Alert Name	Date	Time
Warning	IDTEST200	Symantec AntiVirus Corporate Edition	Symantec AntiVir...	11/25/2003	11:02:17 AM
Warning	IDTEST89	Symantec AntiVirus Corporate Edition	Virus Definition Fil...	11/23/2003	10:34:33 AM
Warning	IDTEST89	Symantec AntiVirus Corporate Edition	Virus Definition Fil...	11/23/2003	09:40:45 AM
Warning	IDTEST200	Symantec AntiVirus Corporate Edition	Symantec AntiVir...	11/23/2003	09:40:03 AM
Warning	IDTEST200	Symantec AntiVirus Corporate Edition	Symantec AntiVir...	11/13/2003	12:45:13 PM
Warning	IDTEST89	Symantec AntiVirus Corporate Edition	Scan Start/Stop	11/12/2003	02:45:55 PM
Critical	IDTEST89	Symantec AntiVirus Corporate Edition	Virus Found	11/12/2003	02:45:55 PM
Critical	IDTEST89	Symantec AntiVirus Corporate Edition	Virus Found	11/12/2003	02:45:51 PM
Critical	IDTEST89	Symantec AntiVirus Corporate Edition	Virus Found	11/12/2003	02:45:51 PM
Critical	IDTEST89	Symantec AntiVirus Corporate Edition	Virus Found	11/12/2003	02:45:51 PM
Critical	IDTEST89	Symantec AntiVirus Corporate Edition	Virus Found	11/12/2003	02:45:50 PM
Critical	IDTEST89	Symantec AntiVirus Corporate Edition	Virus Found	11/12/2003	02:45:50 PM
Critical	IDTEST89	Symantec AntiVirus Corporate Edition	Virus Found	11/12/2003	02:45:50 PM
Critical	IDTEST89	Symantec AntiVirus Corporate Edition	Virus Found	11/12/2003	02:45:50 PM
Critical	IDTEST89	Symantec AntiVirus Corporate Edition	Virus Found	11/12/2003	02:45:50 PM

To change the number of entries displayed in the Alert Log

1 In the Alert Log window, right-click, and then click **Options**.

2 Specify the number of log entries that you want the log to hold.

Note: You can independently configure the number of entries that an Alert Log holds on each server.

To delete a single entry

◆ Right-click the log entry, and then click **Delete** > **Selected Entries**.

To delete multiple log entries

1 Press **Ctrl** and select the multiple log entries.

2 In the Alert Log window, right-click, and then click **Delete** > **Selected Entries**.
To select a range, click the first entry, and then press **Shift** and click the last entry.

To delete all visible log entries

- In the Alert Log window, right-click, and then click **Delete** > **Filtered Entries**.

To copy Alert Log contents to the Clipboard

1. Press and hold the **Ctrl** key, and then select the multiple log entries.
2. In the Alert Log window, right-click, and then click **Copy**.
   Only the alerts visible in the log are copied. If you want to limit the number of entries that the Alert Log copies to the Clipboard, apply filters to limit the number of visible log entries.

Viewing detailed alert information

You can view detailed information about each alert that the Alert Log displays. The Alert Information dialog box displays the detailed information and includes alerts, their values, and the action status of each alert.

The Alert Information dialog box displays a list of parameters such as Alert name, Source, Date, Severity, and Description, as well as values for the selected alert action.

The Alert Information dialog box also displays the types of status that appear in Table 2-2.

Table 2-2 Action Status types

Action Status	Description
Action Type	The type of action generated by the alert, such as Message Box, Pager, Internet Mail, Execute Program, or Broadcast.
Action Name	A name given to the specific action.
Computer	The name of the computer generating the alert.
Status	The status of the alert. The status type can include Pending, Processing Action, Error, Completed Successfully, and Failed To Complete.

To view the alert information and Action Status

1. In the Alert Log window, double-click the alert for which you want to display detailed information.
2. When you finish viewing the alert information, click **Close**.
   The computer listed in the Alert Log is the primary server that recorded the action because it records all events for the Symantec server group. To see which computer actually generated the alert, double-click the Alert Log entry about which you want more information. The Alert Information dialog box provides additional alert details, including the name of the computer that generated the alert.

Filtering the Alert Log display list

You can configure the Alert Log to display only those alerts that match specified criteria. You can filter which alerts display according to the parameters that appear in Table 2-3.

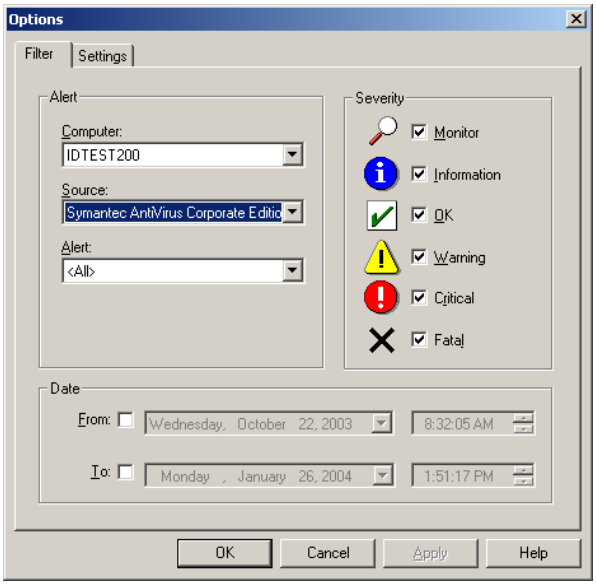
Table 2-3 Alert Log filters

Filter	Description
Computer	Displays alerts from a specific computer.
Source	Displays alerts from the same type of alert source on one or more computers.
Alert	Displays all alerts with a specific alert name.
Severity	Displays only alerts matching the severity levels that you select. You can specify the following severity levels: Monitor, Information, OK, Non-critical, Critical, and Non-recoverable.

To specify which alerts display in the Alert Log

1 In the Symantec System Center console, right-click the server group, and then click **All Tasks** > **AMS** > **View Log**.

2 In the Alert Log window, right-click, and then click **Options**.



3 Select the filters you want to apply to the Alert Log list.

4 Click **OK**.

Forwarding alerts from unmanaged clients

The AMS^2 client software is not installed as part of the client installation. If you want to use the alerting features that AMS^2 provides for unmanaged clients, you can install the AMS^2 client program that is included on the Symantec AntiVirus CD.

Unmanaged Symantec AntiVirus clients can be configured to forward their alerts to an AMS^2 server.

For the alert to be sent, the client computer must be connected to the network and must be able to connect to the AMS server.

To forward alerts to an AMS server

1. Use a text editor such as Notepad to create a new text file.
2. Add the following lines:

```
[KEYS]
!KEY!=$REGROOT$\Common
AMSServer=S<AMSServerName>
AMS=D1
!KEY!=$REGROOT$\ProductControl
LoadAMS=D1
```

3. In the <AMSServerName> line, do one of the following:
   - Type the IP or IPX address for the intended AMS^2 server.
   - Type the name of the intended AMS^2 server (make sure that the client can resolve the server name).
     Be sure to include the S preceding <SERVERNAME>. Do not include the brackets.
4. Save the file as Grc.dat to one of the following folders on the client:
   - For Windows 98\Me: C:\Program Files\Symantec AntiVirus
   - For Windows NT: C:\Winnt\Profiles\All Users\Application Data\Symantec\Symantec AntiVirus Corporate Edition\7.5
   - For Windows 2000\XP\2003: C:\Documents and Settings\All Users\Application Data\Symantec\Symantec AntiVirus

Once you have created the configurations file (Grc.dat), you can copy it to other unmanaged clients. These unmanaged clients will then forward alerts to the same AMS^2 server.

Section 2

Configuring Symantec AntiVirus

- Scanning for viruses and other threats
- Updating virus definitions files
- Responding to virus outbreaks
- Managing roaming clients
- Working with Histories and Event Logs

Chapter 3

Scanning for viruses and other threats

This chapter includes the following topics:

- About threats
- About scans in Symantec AntiVirus
- Configuring Auto-Protect scans
- Configuring manual scans
- Configuring scheduled scans
- Handling Symantec AntiVirus clients with intermittent connectivity
- Configuring scan options

About threats

Symantec AntiVirus can scan for viruses and known and emerging threats, such as spyware, adware, and other files that could put your computer at risk. Symantec AntiVirus can scan for the following threat types:

- *Viruses*: Programs or code that attach a copy of themselves to another computer program or document when it runs. Whenever the infected program runs or a user opens a document containing a macro virus, the attached virus program activates and attaches itself to other programs and documents.

  Viruses generally deliver a payload, such as displaying a message on a particular date. Some viruses specifically damage data by corrupting programs, deleting files, or reformatting disks.

- *Worms*: Programs that replicate without infecting other programs. Some worms spread by copying themselves from disk to disk, while others replicate only in memory to slow a computer down.
- *Trojan horses*: Programs that contain code that is disguised as or hiding in something benign, such as a game or utility.
- *Blended threats*: Threats that blend the characteristics of viruses, worms, Trojan horses, and code with server and Internet vulnerabilities.
- *Spyware:* Stand-alone programs that can secretly monitor system activity and detect passwords and other confidential information and relay it back to another computer.
- *Adware*: Stand-alone or appended programs that secretly gather personal information through the Internet and relay it back to another computer. Adware may track browsing habits for advertising purposes. Adware can also deliver advertising content.

  Spyware and adware can be unknowingly downloaded from Web sites (typically in shareware or freeware), email messages, and instant messenger programs. Often a user unknowingly downloads adware by accepting an End User License Agreement from a software program.
- *Dialers*: Programs that use a computer, without the user's permission or knowledge, to dial out through the Internet to a 900 number or FTP site, typically to accrue charges.
- *Joke programs*: Programs that alter or interrupt the operation of a computer in a way that is intended to be humorous or frightening. For example, a program can be downloaded from a Web site, email message, or instant messenger program. It can then move the Recycle Bin away from the mouse when the user attempts to delete it or cause the mouse to click in reverse.
- *Remote access programs*: Programs that allow access over the Internet from another computer so that they can gain information or attack or alter a user's computer. For example, a program may be installed by the user, or installed as part of some other process without the user's knowledge. The program can be used for malicious purposes with or without modification of the original remote access program.
- *Hack tools*: Programs used by a hacker to gain unauthorized access to a user's computer. For example, one hack tool is a keystroke logger, which tracks and records individual keystrokes and sends this information back to the hacker. The hacker can then perform port scans or vulnerability scans. Hack tools may also be used to create viruses.

- *Trackware*: Stand-alone or appended applications that trace a user's path on the Internet and send information to the target system. For example, the application can be downloaded from a Web site, email message, or instant messenger program. It can then obtain confidential information regarding user behavior.
- *Security risks*: Threats that do not conform to the strict definitions of viruses, Trojan horses, worms, or other expanded threat categories, but which may present a threat to a user's computer and its data.

Viruses, Trojan horses, and worms are scanned for by default. You must enable expanded threat scanning for Symantec AntiVirus to detect other types of threats.

Some threats, such as Back Orifice, were detected as viruses in earlier versions of Symantec AntiVirus. They remain detected as viruses so that Symantec AntiVirus can continue to provide protection for legacy systems.

About scans in Symantec AntiVirus

You can configure the following types of scans from the Symantec System Center console:

- File System Auto-Protect scans
- Scheduled scans
- Manual scans
- Auto-Protect email attachment scanning for Lotus Notes, and Microsoft Exchange and Outlook (MAPI)
- Auto-Protect scanning for Internet email messages and attachments that use the POP3 or SMTP communications protocols; Auto-Protect scanning for Internet email also includes outbound email heuristics scanning

File System Auto-Protect and Auto-Protect email scans detect viruses. Manual and scheduled scans detect viruses and other threats, such as adware and spyware.

You can perform scans on:

- Individual and multiple Symantec AntiVirus servers and clients
- Groups of Symantec AntiVirus servers and clients, using server groups

Understanding Auto-Protect scans

Auto-Protect scans continuously inspect files and email data for viruses as they are read from or written to a computer. Auto-Protect does not scan for other threats, such as spyware and adware. Auto-Protect is enabled by default. You can configure Auto-Protect settings for servers at the server group or server level, and clients at the server group, server, or client group level. When you configure Auto-Protect, the configuration pages look slightly different depending on whether you are setting options for servers or clients. You can lock Auto-Protect settings on clients if you want to enforce a threat policy. Users cannot change options that you lock.

Auto-Protect includes the SmartScan feature, which, when enabled, can determine a file's type even when a virus changes the file's extension.

Symantec AntiVirus scans email data on Symantec AntiVirus clients only.

Understanding scheduled scans

From the Symantec System Center console, you can schedule scans for Symantec AntiVirus servers or clients. Users can also schedule scans for their computers from Symantec AntiVirus clients, but they cannot change or disable scans that you schedule for their computers. Symantec AntiVirus runs one scheduled scan at a time. If more than one scan is scheduled at the same time, they will run sequentially.

When you create and save a scheduled scan, Symantec AntiVirus remembers the server group, server, or computer on which to run the scan and the settings that you chose for that scan.

If a computer is turned off during a scheduled scan, the scan will not run unless the computer has been configured to run missed scan events.

Scheduled scans can inspect files for viruses and other threats, such as spyware and adware.

See "Setting options for missed scheduled scans" on page 119.

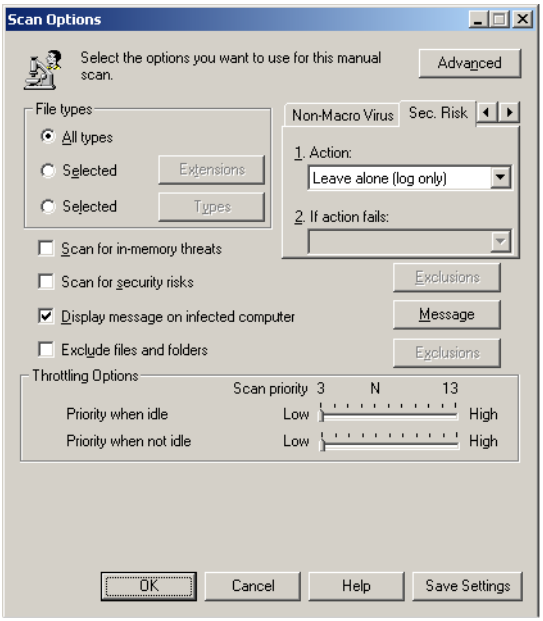
Understanding manual scans

Manual or on-demand scans inspect selected files and folders on selected computers. Manual scans provide immediate results from a scan on a small area of the network or a local hard drive.

Manual scans can inspect files for viruses and other threats, such as spyware and adware.

You can set scan options in the Scan Options dialog box shown in Figure 3-1.

Figure 3-1 Scan Options dialog box



Selecting computers to scan

In the Symantec System Center console, you select the computers that you want to scan, determine the types of scans that are available, where scans are performed, and the scan options.

Table 3-1 lists what you can scan, by object type.

Table 3-1 What you can scan

Object selected	Scans available
System Hierarchy	Virus sweep scanning of all Symantec AntiVirus servers and clients in the network
Multiple server groups	■ Virus sweep scanning of all Symantec AntiVirus servers and their clients in the selected server groups ■ Scheduled scanning for the selected Symantec AntiVirus servers
Server group	■ Virus sweep scanning of all Symantec AntiVirus servers and their clients in the selected server group ■ Scheduled scanning for the Symantec AntiVirus servers in the selected server group
Selected servers in a server group	■ Virus sweep scanning of the selected Symantec AntiVirus servers ■ Manual scanning of the selected Symantec AntiVirus servers
Single server	■ Virus sweep scanning of the Symantec AntiVirus server and all of its Symantec AntiVirus clients ■ Manual scanning of the Symantec AntiVirus server ■ Scheduled scanning of the Symantec AntiVirus server or its Symantec AntiVirus clients
Selected Symantec AntiVirus clients for a single Symantec AntiVirus server	Manual scanning of the selected Symantec AntiVirus clients that are managed by the Symantec AntiVirus server
An individual Symantec AntiVirus client	■ Manual scanning of the selected Symantec AntiVirus client ■ Scheduled scanning of the selected Symantec AntiVirus client

Note: Clients' settings must be locked before Auto-Protect options that are configured in the Symantec System Center console can be propagated to them. If you make a change but do not lock the setting, the change is not propagated to clients.

See "Configuring Auto-Protect scans" on page 96.

Determining scan options for multiple computers

When you view Auto-Protect, virus sweep, or manual scan options for multiple selected computers, the configuration check boxes and options have a tri-state feature that is apparent only when the computers have different options configured. Click the same option multiple times to see the different states:

- A solid black check mark in a check box or a solid black bullet in an option means that the option is selected for all of the computers in that group. Setting an option to a state other than the dimmed state resets that option for selected computers.
- A blank check box means that the option is not selected for any computer in that group. Setting an option to a state other than the dimmed state resets that option for selected computers.
- A dimmed check mark in a dimmed box, a blank series of options, or a blank box means that some of the computers in the group have that option selected and some do not. Setting an option to a state other than the dimmed state resets that option for selected computers.

Some options, such as excluding files and folders, are not available when you select multiple computers because the option applies only to a specific computer.

Scan option precedence

Scan configuration changes made at the server group level override any changes made at the client group or server level.

Note: Auto-Protect options work differently from the other scan options. Auto-Protect options must be locked at the server group or server level before they can be propagated to clients. If you make a change but do not lock the setting, the change is not propagated to clients.

See “Understanding Auto-Protect scans” on page 92.

Configuring Auto-Protect scans

Configuring Auto-Protect scans consists of the following tasks:

- Configuring Auto-Protect for files
- Configuring Auto-Protect email scanning
- Specifying exclusions
- Configuring Auto-Protect settings
- Locking and unlocking Auto-Protect options

Configuring Auto-Protect for files

When you configure Auto-Protect for files, you select a server group or server, configure scan settings, and configure other settings that define how Auto-Protect and its associated features behave.

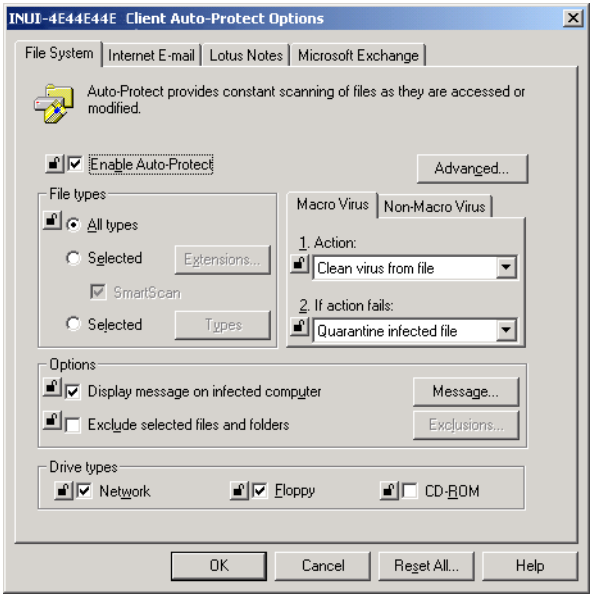
When you configure Auto-Protect options for files, specify which of the following drive types that you want Symantec AntiVirus to scan:

- Floppy drive: Symantec AntiVirus can scan files as they are read from or written to floppy disks. Floppy disks are common sources of virus infections because users may bring infected disks from home.
- Network drive: If you enable Auto-Protect on network drives, Symantec AntiVirus can scan files as they're written from a client computer to a server (or from a server to another server). This option is not necessary if you enable Auto-Protect on your servers. For example, if you enable scanning of network drives on client A and also have Auto-Protect enabled on server B, when client A writes a file to a network drive on server B, Symantec AntiVirus scans the file on client A and scans the file again on server B. This could reduce network performance on the client computer.

To configure Auto-Protect for files

1. In the Symantec System Center console, do one of the following:
   - Right-click the server group or Symantec AntiVirus servers that you want to configure, and then click **All Tasks** > **Symantec AntiVirus** > **Server Auto-Protect Options**.
     If you select a server group, the Symantec System Center will configure all of the servers that are in the server group.
   - Right-click an individual server or multiple selected servers, and then click **All Tasks** > **Symantec AntiVirus** > **Client Auto-Protect Options**.

- Right-click the server group or servers with Symantec AntiVirus clients that you want to configure, and then click **All Tasks** > **Symantec AntiVirus** > **Client Auto-Protect Options**.
  The Symantec System Center will configure all of the clients that are associated with the server or server group.
- Right-click an individual client or multiple selected clients for a server, and then click **All Tasks** > **Symantec AntiVirus** > **Client Auto-Protect Options**.



2 In the Auto-Protect Options dialog box, ensure that Enable Auto-Protect is checked.

3 Under File types, do one of the following:
   - Select file types and extensions to scan.
   - Click **Selected**, and then check **SmartScan**.

   See "About Scan all file types and SmartScan" on page 98.

4 On the Macro Virus and Non-Macro Virus tabs, assign primary actions and secondary actions for detected viruses.

5 Under Options, ensure that Display message on infected computer is checked.

6 Configure the warning message to display on infected computers.
See "Displaying and customizing a warning message on an infected computer" on page 128.

7 Exclude files or folders from Auto-Protect scans, if necessary.
See "Selecting file types and extensions to scan for viruses" on page 134.

8 Under Drive types, select drive types to scan.
See "Configuring Auto-Protect for files" on page 96.

9 Set advanced file options.
See "Configuring Advanced Auto-Protect options" on page 98.

10 Lock any client Auto-Protect options that you want to propagate to clients.
See "How to lock and unlock Auto-Protect options" on page 110.

11 If you are configuring Auto-Protect options for a server group, click **Reset All** to ensure that all of the computers are using the Auto-Protect scanning configuration that you set at this level.
See "Configuring Auto-Protect settings" on page 109.

12 Click **OK**.

About Scan all file types and SmartScan

You can configure Symantec AntiVirus to scan all file types or to use SmartScan. SmartScan scans a specific, configurable group of file extensions that contain executable code and all .exe and .doc files. SmartScan reads each file's header to determine its file type. It scans .exe and .doc files even if the file extensions for the .exe and .doc files are changed by a virus to extensions that are different from the file extensions that SmartScan has been configured to scan. SmartScan is enabled by default.

Configuring Advanced Auto-Protect options

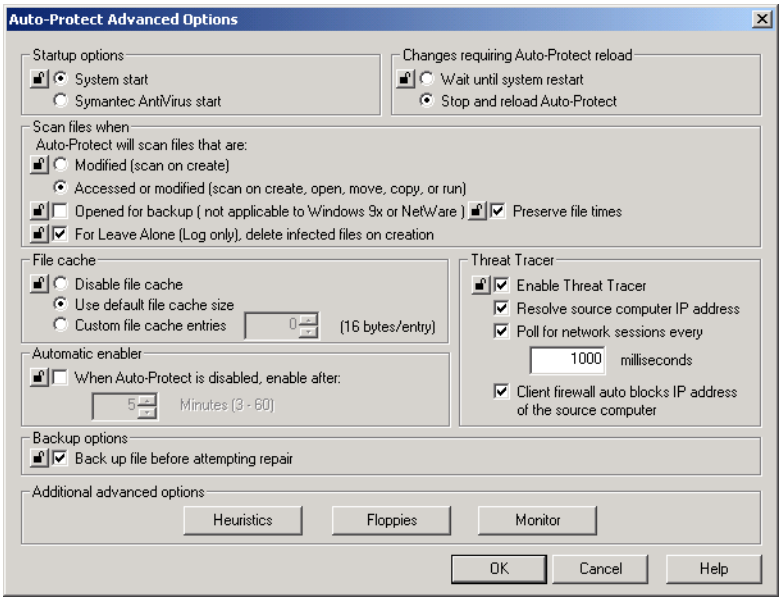
When you configure Advanced Auto-Protect options, you can define the following:

- When to start Auto-Protect
- When to reload Auto-Protect when a reload is necessary
- When to scan files with Auto-Protect
- How many entries to cache in an index of clean files
- How long to wait before enabling Auto-Protect when it is disabled
- Whether Auto-Protect backs up files before it attempts to repair them

- When the Leave alone (log only) option is enabled, whether to delete infected files delete when they are created
- Whether file times are preserved so that unchanged files are not backed up unnecessarily

To configure Advanced Auto-Protect options

1 In the Auto-Protect Options dialog box, on the File System tab, click **Advanced**.



2 In the Auto-Protect Advanced Options dialog box, under Startup options, select one of the following:

System start	Load Auto-Protect when the computer's operating system starts and unload it when the computer shuts down. This option can help protect against some viruses, such as Fun Love. If Auto-Protect detects a virus during shutdown, it places the infected file in a temporary Quarantine directory. Auto-Protect then detects the virus on startup and creates an alert notification.
Symantec AntiVirus start	Load Auto-Protect when Symantec AntiVirus starts.

3 Under Changes requiring Auto-Protect reload, select one of the following:

Wait until system restart	Stop and reload Auto-Protect when the computer restarts.
Stop and reload Auto-Protect	Stop and reload Auto-Protect immediately.

4 Under Scan files when, set Auto-Protect file monitoring options.
See "Auto-Protect file system protection options" on page 103.
See "How to bypass Auto-Protect for files that are being backed up" on page 103.

5 Under Scan files when, do the following:

For Leave Alone (Log only), delete infected files on creation	Enable this option if you want the Scan on Modify and Scan on Access and Modify file monitoring options to delete a newly created infected file when you configure Leave alone (log only) as the action. For an existing infected file, Scan on Access and Modify detects the infected file and the Leave alone action applies. The file is denied access and logged, but it is not deleted. When you disable this option, Symantec AntiVirus permits the infected file to be created.
Preserve file times	Enable this option if you do not want the file system to change the last access time. Preserving the last access time prevents backup software from backing up unchanged files.

6 Under File cache, select one of the following:

Disable file cache	Disable the file cache; for example, you may use this option during troubleshooting.
Use default file cache size	Use the default file cache size setting for desktop computers and use as close to the maximum setting as possible for servers. The default file cache size is based on the computer's operating system and the amount of available disk space. File caching decreases Auto-Protect's memory usage and can help you to track problems. Symantec AntiVirus adds a 16-byte entry to the cache index, which remains until Symantec AntiVirus detects a change to the file.

Custom file cache entries	Select the number of custom file cache entries to include. This option is useful for file servers or Web servers where you want to be able to cache a large number of files.

See "File cache options" on page 104.

7 Under Threat Tracer, to set options for tracing threats from computers running under Windows NT/2000/XP/2003 operating systems, do the following:

Enable Threat Tracer	Ensure that this option is checked to use Threat Tracer.
Resolve source computer IP address	If Resolve source computer IP address is unchecked, Symantec AntiVirus looks up and records the computer's NetBIOS name only.
Poll for network sessions every ___ milliseconds	Symantec AntiVirus polls once every second (1000 milliseconds) by default. Lower values use greater amounts of CPU and memory. Higher values decrease Threat Tracer's ability to detect infections.
Client firewall auto blocks IP address of the source computer	Enable this option if you are using Symantec Client Security firewall client and want the firewall to automatically block the IP addresses of computers that transmit infected files. The firewall automatically blocks all IP traffic to the IP address for 30 minutes by default.

See "How to trace threats" on page 104.

8 Under Automatic enabler, ensure that When Auto-Protect is disabled, enable after is checked, and then specify a length of time after which Auto-Protect is enabled on the computers for which you are configuring options.
For example, if an end user disables Auto-Protect on the desktop, you can set this option to enable it automatically after thirty minutes.

9 Under Backup options, ensure that Back up file before attempting repair is checked as a data safety precaution.
The files are encrypted and backed up to the Quarantine directory. Once a file is backed up, it must be restored before it can be accessed again.

10 Under Additional advanced options, if you want to change the level of protection that is provided by Bloodhound Heuristic Scanning, click **Heuristics**.

11 In the Heuristic Scanning dialog box, select the setting that you want, and then click **OK**.

12 In the Auto-Protect Advanced Options dialog box, under Additional advanced options, if you want to change the current settings for floppy disk scans, click **Floppies**.

13 In the Check Floppies dialog box, select one of the following:

Check floppies for boot viruses upon access	Symantec AntiVirus scans the floppy disk in the floppy drive for boot viruses when the drive is first accessed. When Symantec AntiVirus finds a boot virus, select whether to clean a virus from the boot record or leave it alone. If you click Leave alone (log only), an alert is sent when a virus is detected but no action is taken. Use this option if you want to take direct control over the virus cleaning and handling process. For example, after you receive the alert, you can decide what course of action to take.
Do not check floppies upon system shutdown	Symantec AntiVirus skips the scan of any floppy disk in the floppy drive when the computer is shut down normally.

14 Click **OK**.

15 In Windows 98 only, in the Auto-Protect Advanced Options dialog box, under Additional advanced options, if you want to disable protection monitors for virus-like activities, click **Monitor**.
Virus-like activities are activities that viruses perform when they attempt to infect your files. Any of these activities might be legitimate depending on your work context.

16 In the Monitor dialog box, to exclude activities from monitoring, select one or more of the following:

Low-Level Format Of Hard Disk	All information on the drive is erased and cannot be recovered. This type of formatting is generally performed at the factory only. If this activity is detected, it usually indicates an unknown virus at work. This is not an option for NEC PC98xx computers.
Write To Hard Disk Boot Records	Very few programs write to hard disk boot records. If this activity is detected, it could indicate an unknown virus at work.
Write To Floppy Disk Boot Records	Only a few programs (such as the operating system Format command) write to floppy disk boot records. If this activity is detected, it could indicate an unknown virus at work.

17 Click **OK**.

18 In the Auto-Protect Advanced Options dialog box, click **OK**.

Auto-Protect file system protection options

There are several file system protection options that determine the file operations that Auto-Protect monitors. Table 3-2 lists and describes these options.

Table 3-2 Auto-Protect file system protection options

Option	Description	When to use it
Modified (scan on create)	Scans files when they are written, modified, or copied.	Use this option for slightly faster performance because Auto-Protect only scans files when they are written, modified, or copied.
Accessed or modified (scan on create, open, move, copy, or run)	Scans files when they are written, opened, moved, copied, or run.	Use this option for more complete file system protection. This option may have a performance impact, because Auto-Protect scans files during all types of file operations.
Opened for backup	Scans files when they are accessed during a backup operation. Only available for computers that are running Windows NT/2000/XP/2003.	Use this option if you haven't run a virus check on files that you want to back up. Using this option can significantly slow backup operations, because Auto-Protect scans each file that is included in the backup. Do not enable this option if you want to bypass Auto-Protect for files that are being backed up. See "How to bypass Auto-Protect for files that are being backed up" on page 103.

How to bypass Auto-Protect for files that are being backed up

You can have Symantec AntiVirus bypass Auto-Protect during a backup. This allows backup software to operate without the overhead of an additional Auto-Protect scan. The setting applies only to files that are being backed up. Files that are being restored from a backup are scanned regardless of this setting.

Note: This option is available for Windows NT/2000/XP/2003 only.

File cache options

File caching decreases Auto-Protect's memory usage and can help you to track problems. The file cache includes an index of files that were scanned and determined to be clean. Symantec AntiVirus adds a 16-byte ID to the cache index, which remains until Symantec AntiVirus detects a change to the file.

How to trace threats

You can use Threat Tracer to identify the source of network share-based virus infections on computers that are running Windows NT/2000/XP/2003 operating systems.

When Auto-Protect detects an infection, it sends information to RtvScan, the main Symantec AntiVirus service. RtvScan determines if the infection originated locally or remotely. If the infection came from a remote computer, RtvScan can look up and record the computer's NetBIOS computer name and its IP address, and then display this information in the Threat Properties dialog box.

RtvScan polls every second by default for network sessions, and then caches this information as a remote computer secondary source list. This information maximizes the frequency with which Threat Tracer can successfully identify the infected remote computer. For example, a threat may close the network share before RtvScan can record the network session. Threat Tracer then uses the secondary source list to try to identify the remote computer.

When Threat Tracer cannot identify the remote computer, the source is listed as Unknown in the Threat Properties dialog box.

When Threat Tracer determines that the infection came from local host activity, it lists the local host.

The source is also listed as Unknown in the Threat Properties dialog box when the authenticated user for a file share refers to multiple computers. This can occur when a user ID is associated with multiple network sessions.

Heuristic scanning

Bloodhound can detect a high percentage of unknown viruses by isolating and locating the logical regions of a file. Bloodhound then analyzes the program logic for virus-like behavior.

Configuring Auto-Protect email scanning for groupware applications

Auto-Protect scans can scan email attachments for the following applications:

- Lotus Notes 4.5x, 4.6, and 5.0
- Microsoft Exchange 5.0 and 5.5
- Microsoft Outlook 97/98/2000/2002 (MAPI only, not Internet)

When Auto-Protect is enabled for email, attachments are immediately downloaded to the computer that is running the email client and scanned when the user opens the message. If you are downloading a large attachment over a slow connection, mail performance is affected. You may want to disable this feature for users who regularly receive large attachments.

Symantec AntiVirus supports email scanning for Symantec AntiVirus clients only.

To configure email scanning

1. In the Symantec System Center console, right-click the server group or servers to configure, and then click **All Tasks** > **Symantec AntiVirus** > **Client Auto-Protect Options**.
2. In the Client Auto-Protect Options dialog box, on the Lotus Notes or Microsoft Exchange tab, check **Enable Auto-Protect**.
   You can use the Microsoft Exchange tab to configure both Microsoft Exchange and Microsoft Outlook.
3. To set Auto-Protect options, do any of the following:
   - Select file types or extensions to scan.
   - Assign primary actions and secondary actions for detected viruses.
   - Display a warning message on infected computers.
   - Insert a warning into an email message.
   - Send email to the sender of an infected attachment.
   - Send email to selected recipients when a virus is detected.
4. Click **Advanced** to configure scanning of compressed files.
5. Set the options, and then click **OK**.
6. Lock or unlock options as desired.
7. Click **Reset All** to ensure that all of the computers are using the Auto-Protect scanning configuration that you have specified.

See "Configuring Auto-Protect scans" on page 96.

If your email program is not supported

If your email system is not one of the supported data formats, you can still protect your network by enabling Auto-Protect on your file system. For example, if you are running a Novell GroupWise email system and one of your users receives a message with an infected attachment, Symantec AntiVirus can detect the virus as soon as the user tries to open the attachment. This is because most email programs (such as GroupWise) save attachments to a temporary directory when users launch attachments from the email program. If you enable Auto-Protect on your file system, Symantec AntiVirus detects the virus as it is written to the temporary directory. Symantec AntiVirus also detects the virus if the user tries to save the infected attachment to a local drive or network drive.

Configuring Auto-Protect scanning for Internet email

Auto-Protect scanning for Internet email protects both incoming and outgoing email messages that use the POP3 or SMTP communications protocol. When Auto-Protect scanning for Internet email is enabled, Symantec AntiVirus scans both the body text of the email and any attachments that are included.

Symantec AntiVirus also provides outbound email heuristics scanning that uses Bloodhound Virus Detection to identify threats that may be contained in outgoing messages. Scanning outgoing email messages helps to prevent the spread of threats such as worms that can use email clients to replicate and distribute themselves across a network.

When Auto-Protect scanning for Internet email is enabled, attachments are immediately downloaded to the computer that is running the email client and scanned when the user opens the message. If you are downloading a large attachment over a slow connection, mail performance is affected. You may want to disable this feature for users who regularly receive large attachments.

Email scanning does not support the following email clients:

- IMAP clients
- AOL clients
- POP3 that uses SSL (Secure Sockets Layer)
- HTTP-based email such as Hotmail and Yahoo!

To configure Auto-Protect scanning for Internet email

1. In the Symantec System Center console, right-click the server group or servers to configure, and then click **All Tasks** > **Symantec AntiVirus** > **Client Auto-Protect Options**.
2. In the Client Auto-Protect Options dialog box, on the Internet E-mail tab, check **Enable Internet E-mail Auto-Protect**.
   The settings that you choose apply to both the POP3 and SMTP protocols.
3. To set Auto-Protect options, do any of the following:
   - Select file types or extensions to scan.
   - Assign primary actions and secondary actions for detected viruses.
   - Display a warning message on infected computers.
   - Insert a warning into an email message.
   - Send an email message to the sender of an infected attachment.
   - Send an email message to selected recipients when a virus is detected.
4. Click **Advanced** to configure scanning of compressed files.
5. In the Internet E-mail Advanced Options dialog box, set the scanning options that you want, and then click **OK**.
6. On the Internet E-mail tab, lock or unlock options as desired.
7. Click **Reset All** to ensure that all of the computers are using the Auto-Protect scanning configuration that you have specified.
   See "Configuring Auto-Protect scans" on page 96.

Changing the POP3 and SMTP ports that are scanned

Auto-Protect scanning for Internet email uses the standard POP3 and SMTP email ports by default. However, if you have configured your network to use a different port for either protocol, you must change the port setting in Symantec AntiVirus to match the port that you have selected.

To change the POP3 and SMTP ports that are scanned

1. In the Symantec System Center console, right-click the server group or servers to configure, and then click **All Tasks** > **Symantec AntiVirus** > **Client Auto-Protect Options**.
2. In the Client Auto-Protect Options dialog box, on the Internet E-mail tab, check **Enable Internet E-mail Auto-Protect**.
3. Click **Advanced**.

4 In the Internet E-mail Advanced Options dialog box, under Server Port Numbers, change the port number to match the port that you are using for each protocol.
If you want to reset the port numbers to the default setting, click **Use Defaults**.

5 Click **OK**.

6 Click **Reset All** to ensure that all of the computers are using the Auto-Protect scanning configuration that you have specified.
See "Configuring Auto-Protect scans" on page 96.

Enabling outbound email heuristics scanning

Auto-Protect scanning for Internet email provides outbound email protection against threats such as worms that can distribute themselves using email applications. Symantec AntiVirus utilizes Bloodhound Virus Detection technology to successfully identify threats in outbound email messages.

To enable outbound email heuristics scanning

1 In the Symantec System Center console, right-click the server group or servers to configure, and then click **All Tasks** > **Symantec AntiVirus** > **Client Auto-Protect Options**.

2 In the Client Auto-Protect Options dialog box, on the Internet E-mail tab, check **Enable Internet E-mail Auto-Protect**.

3 Click **Advanced**.

4 In the Internet E-mail Advanced Options dialog box, check **Outbound Worm Heuristics**.

5 Click **OK**.

6 Click **Reset All** to ensure that all of the computers are using the Auto-Protect scanning configuration that you have specified.
See "Configuring Auto-Protect scans" on page 96.

How to specify exclusions

Exclusions help you balance the amount of protection that your network requires with the amount of time and resources that are required to provide that protection. For example, when you scan all file types, you may want to exclude certain folders that contain only data files that are not subject to viruses. This decreases the overhead that is associated with scanning files.

Configuring Auto-Protect settings

You can configure Auto-Protect settings at the server group, server, and client group level. When you configure Auto-Protect settings, follow these rules:

- Changing server Auto-Protect settings for an individual server allows you to push a specific configuration to that server, which overrides settings that are made at the server group level. Resetting server Auto-Protect settings at the server group level allows you to reset previous settings made at the individual server level.
- Changing client Auto-Protect settings at the parent server or client group level allows you to push a specific configuration to the clients of that parent server or client group.
  - Resetting client Auto-Protect settings at the server group level resets previous settings made at the parent server or client group level, for all clients.
  - Changing client Auto-Protect settings at the parent server level changes the settings for clients not assigned to client groups; clients assigned to a client group retain their settings.
- Clicking OK in the Auto-Protect Options dialog box propagates the settings that you change. Clicking Cancel propagates the settings you visit in the Auto-Protect Options dialog box. (In this instance, visiting means changing a setting, and then changing it back to the way it was set when you opened the dialog box.) Settings that are unchanged or unvisited are not propagated.

  For example, when you change the Auto-Protect settings (but do not visit or change the settings on any other configuration tab in any other dialog box), and click OK, only the Auto-Protect options are propagated.
- Clicking Reset All propagates all settings in the dialog box, regardless of whether you change or visit them.

For more information about settings propagation, see "How settings propagate" on page 59.

To configure Auto-Protect settings

1. In the Symantec System Center console, do one of the following:
   - To change server Auto-Protect settings, right-click a server group or server, and then click **All Tasks** > **Symantec AntiVirus** > **Server Auto-Protect Options**.
   - To change client Auto-Protect settings, right-click a server-group, server, or client group, and then click **All Tasks** > **Symantec AntiVirus** > **Client Auto-Protect Options**.

2 In the Auto-Protect Options dialog box, change one or more settings.

3 Click **OK** until the main Symantec System Center console window appears.

How to lock and unlock Auto-Protect options

The lock icons in the Auto-Protect Options dialog box allow you to control user experience at the Symantec AntiVirus client. Table 3-3 lists and describes the lock icons.

Table 3-3 Auto-Protect lock icons

Icon	Description	What it does
	This is an unlocked setting.	Users can change an unlocked setting from Symantec AntiVirus client.
	This is a locked setting.	This setting is not available to users from Symantec AntiVirus client.

Configuring manual scans

Configuring a manual scan consists of the following tasks:

- Select a Symantec AntiVirus server or client.
- Select folders to scan.
- Specify scanning options.
- Specify advanced options.

If you want to scan all servers and clients in a server group, run a virus sweep or create a scheduled scan.

Symantec AntiVirus backs up viruses but does not back up other threats, such as adware or spyware, when it deletes them. Once you delete the file, Symantec AntiVirus cannot restore it.

To configure a manual scan

1. In the Symantec System Center console, do one of the following:
   - Right-click a server or client computer.
   - Select one or more servers that are in the same server group, and then right-click the servers.
   - Select one or more clients that are managed by the same server, and then right-click the clients.
2. Click **All Tasks** > **Symantec AntiVirus** > **Start Manual Scan**.
3. In the Select Items dialog box, select the folders to scan.

   If you are scanning multiple computers, this option is not available. Go to step 5.
4. Click **Save Settings** if you want Symantec AntiVirus to remember your selections for future manual scans on this computer.

   Symantec AntiVirus also remembers these settings for future scans when multiple computers are selected.
5. Click **Options**.

   See Figure 3-1, "Scan Options dialog box," on page 93.
6. In the Scan Options dialog box, you can:
   - Select file types or extensions to scan.
   - Assign primary and secondary actions for detected viruses, blended threats, and some other threats. If deleting a threat in an expanded threat category can cause a system failure, the only available action is to log it.
   - Enable scanning for threats that are in memory. See "Scanning for in-memory threats" on page 132.
   - Enable expanded threat scanning and exclude threat categories from the scan if necessary.

     When you exclude a folder, Symantec AntiVirus cannot protect the affected computer from infected files in the folder.

     When you exclude a threat category, Symantec AntiVirus cannot protect the affected computer from threats that are included in the category. See "Enabling expanded threat categories" on page 139.
   - Display a warning message on infected computers.
   - Exclude files and folders from the scan. (Not available for multiple clients or servers.)
   - Set throttling options. See "Setting CPU utilization" on page 144.
7. Click **Advanced**.

8 In the Scan Advanced Options dialog box, you can:

- Set options for scanning compressed files.
- Back up files infected by viruses or blended threats before attempting to repair them as a data safety precaution. The files are encrypted before Symantec AntiVirus backs them up. The files get backed up to the Quarantine directory. Once the file is backed up, it must be restored before it can be accessed again.

  Symantec AntiVirus does not back up threats other than viruses and blended threats; for example, Symantec AntiVirus does not back up spyware or adware files.
- Determine whether a progress dialog box appears on the computer while the scan runs. You can configure the progress dialog box to close automatically when the scan has completed. You can also display or hide a Stop button on the remote computer. When this option is disabled, the scan cannot be stopped from the remote computer.
- Set storage migration options. See "Configuring HSM settings" on page 141.
- Enable scans of compressed files on NetWare servers.

9 Click **OK** to save advanced options.

10 In the Scan Options dialog box, click **Save Settings** if you want Symantec AntiVirus to remember these options for future manual scans on this computer.

   Symantec AntiVirus will also remember these settings for future scans when multiple computers are selected.

11 Click **OK** to continue with these options.

12 Click **Start**.

See "Setting CPU utilization" on page 144.

How to specify exclusions

You can exclude files, folders, and expanded threat categories from scans.

Excluding files and folders

You may want to exclude folders that contain only data files that are not subject to viruses. You can also exclude folders that contain other allowable threats. For example, your company's security policy may allow users to run an adware program.

Note: Because excluded files and folders are not scanned, they are not protected from viruses and other threats.

Excluding expanded threat categories

You can exclude expanded threat categories for which you do not want Symantec AntiVirus to scan. For example, if you monitor user Internet behavior with a company approved trackware application that is installed on every network node, you can exclude the trackware category.

See "Enabling expanded threat categories" on page 139.

Deleting files and folders that are left on computers by threats

When Symantec AntiVirus deletes a file that is part of a threat category, such as adware or spyware, other files related to the threat may remain on the computer. The remaining files are not likely to cause a problem but you may want to delete them manually to free up disk space on the computer.

Configuring scheduled scans

Configuring scheduled scans consists of:

- Scheduling scans for Symantec AntiVirus servers and clients
- Setting options for missed scans
- Optionally editing, deleting, or disabling a scan, or running a scheduled scan on demand

Scheduled scans have settings that are similar to Auto-Protect scan settings, but each type of scan is configured separately. For example, exclusions settings that are set for Auto-Protect scanning only affect Auto-Protect scanning, and do not affect scheduled scanning.

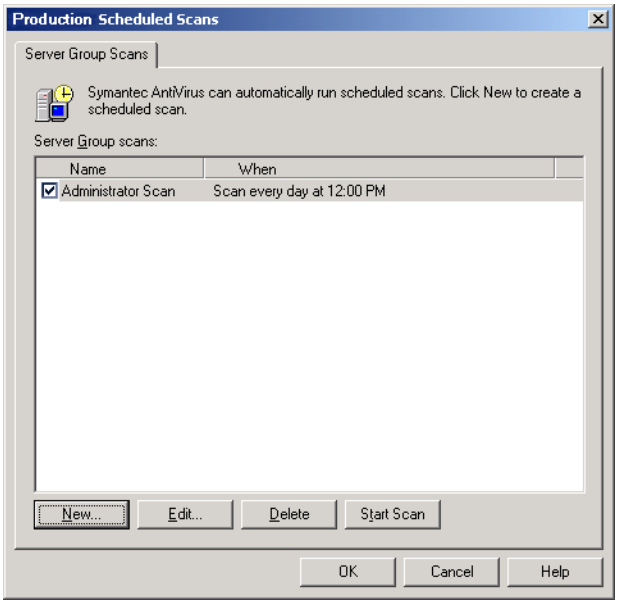
Scheduling scans for server groups or individual Symantec AntiVirus servers

You can schedule scans for one or more server groups as well as for individual Symantec AntiVirus servers.

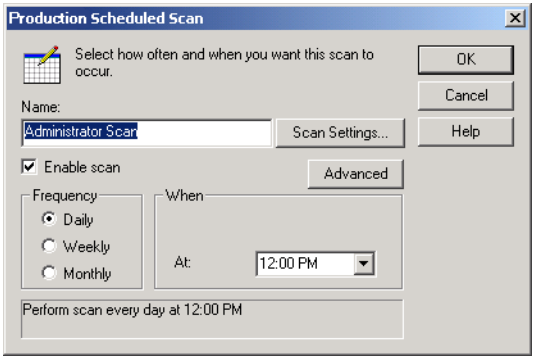
To schedule a scan for a server group

1 In the Symantec System Center console, do one of the following:
   - In the console tree, click **System Hierarchy**. In the right pane, Shift+click or Ctrl+click to select multiple server groups, and then right-click the selection.
   - Right-click a server group.
   - Right-click a server.

2 Click **All Tasks** > **Symantec AntiVirus** > **Scheduled Scans**.



3 In the Scheduled Scans dialog box, on the Server Group Scans tab, click **New**.



4 In the Scheduled Scan dialog box, under Name, type a name for the scan.

5 Ensure that Enable scan is checked.

6 Set a frequency for the scan.

7 Set a time for the scan.
You can type any time in increments of 1 minute or use the drop-down list to select a time in 15-minute increments.

8 Click **Advanced**.

9 In the Advanced Schedule Options dialog box, check **Handle Missed Events Within**, and then set the time limit within which you want the scan to run.
For example, you may want a weekly scan to run only if it is within three days after the scheduled time for the missed event.

10 Click **OK**.

11 In the Scheduled Scan dialog box, click **Scan Settings**.

12 In the Select Items dialog box, click **Options**.

13 In the Scheduled Scans Options dialog box, you can:

- Select file types or extensions to scan.
- Assign primary and secondary actions for detected viruses, blended threats, and some other threats. If deleting a threat in an expanded threat category can cause a system failure, the only available action is to log it.
- Enable scanning for threats that are in memory. See "Scanning for in-memory threats" on page 132.

- Enable expanded threat scanning and exclude threat categories from the scan if necessary.

  When you exclude a folder, Symantec AntiVirus cannot protect the affected computer from infected files in the folder.

  When you exclude a threat category, Symantec AntiVirus cannot protect the affected computer from threats that are included in the category. See "Enabling expanded threat categories" on page 139.
- Display a warning message on infected computers.
- Exclude files and folders from the scan. (Not available for multiple clients or servers.)
- Set throttling options. See "Setting CPU utilization" on page 144.

14 Click **Advanced**.

15 In the Scan Advanced Options dialog box, you can:

- Display a scan progress window on a computer that is being scanned.
- Close a scan progress window on a computer when the scan completes.
- Back up infected files before you attempt to repair them as a data safety precaution. The files are encrypted and backed up to the Quarantine directory. Once the file is backed up, it must be restored before it can be accessed again.

  Symantec AntiVirus does not back up threats other than viruses, such as adware or spyware, when you delete them. Once you delete the file, Symantec AntiVirus cannot restore it.
- Set options for scanning compressed files.

16 Click **OK** until you return to the main screen in the Symantec System Center console.

See "Configuring scan options" on page 123.

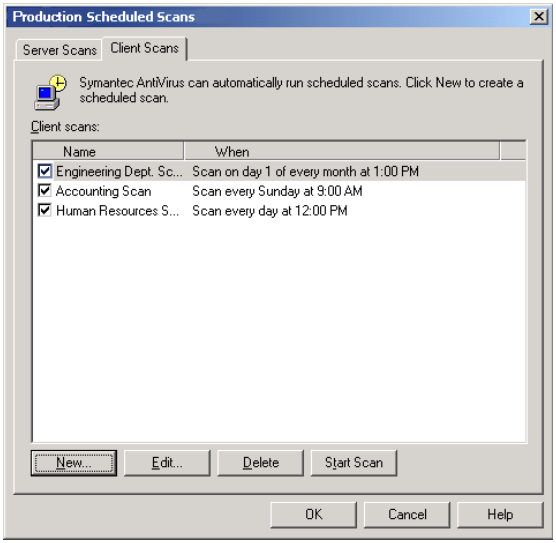
Scheduling scans for Symantec AntiVirus clients

You can schedule Symantec AntiVirus client scans at the Symantec AntiVirus server or client level.

To schedule scans for Symantec AntiVirus clients

1 In the Symantec System Center console, right-click a server or individual client, and then click **All Tasks** > **Symantec AntiVirus** > **Scheduled Scans**.

2 In the Scheduled Scans dialog box, on the Client Scans tab, click **New**.



3 In the Scheduled Scan dialog box, under Name, type a name for the scan.

4 Set a frequency for the scan.

5 Set a time for the scan.
You can type any time in increments of 1 minute or use the drop-down list to select a time in 15-minute increments.

6 Click **Advanced**.

7 In the Advanced Schedule Options dialog box, check **Handle missed events within**, and then set the time limit within which you want the scan to run.
For example, you may want a weekly scan to run only if it is within three days after the scheduled time for the missed event.

8 Click **OK**.

9 In the Scheduled Scan dialog box, click **Scan Settings**.

10 Select the folders to scan.
This option is not available if you are scanning multiple computers because folders are specific to each computer.

11 Click **Options**.

12 In the Scheduled Scan Options dialog box, you can:
   - Select file types and extensions to scan.
   - Assign primary and secondary actions for detected viruses. If deleting a threat can cause a system failure, the only available action is to log the threat.
   - Select file types or extensions to scan.
   - Enable scanning for threats that are in memory. See "Scanning for in-memory threats" on page 132.
   - Enable expanded threat scanning and exclude threat categories from the scan if necessary.

     When you exclude a folder, Symantec AntiVirus cannot protect the affected computer from infected files in the folder.

     When you exclude a threat category, Symantec AntiVirus cannot protect the affected computer from threats that are included in the category. See "Enabling expanded threat categories" on page 139.
   - Display a warning message on infected computers.
   - Exclude files and folders from the scan. (Not available for multiple clients or servers.)
   - Set throttling options. See "Setting CPU utilization" on page 144.

13 Click **Advanced**.

14 In the Scan Advanced Options dialog box, you can:
   - Set options for scanning compressed files.
   - Back up files infected by viruses or blended threats before attempting to repair them as a data safety precaution. The files are encrypted before Symantec AntiVirus backs them up. The files get backed up to the Quarantine directory. Once the file is backed up, it must be restored before it can be accessed again.

     Symantec AntiVirus does not back up threats other than viruses and blended threats; for example, Symantec AntiVirus does not back up spyware or adware files.
   - Determine whether a progress dialog box appears on the computer while the scan runs. You can configure the progress dialog box to close automatically when the scan has completed. You can also display or hide a Stop button on the remote computer. When this option is disabled, the scan cannot be stopped from the remote computer.
   - Set storage migration options. See "Configuring HSM settings" on page 141.
   - Enable scans of compressed files on NetWare servers.

15 Click **OK** until you return to the main screen in the Symantec System Center console.

See "Configuring scan options" on page 123.

Setting options for missed scheduled scans

If a computer misses a scheduled scan (for example, if it is turned off), Symantec AntiVirus will attempt the scan for a specific time interval. If Symantec AntiVirus cannot start the scan within the time interval, it will not run the scan. The default time intervals are as follows:

- Daily scans: 8 hours
- Weekly scans: 3 days
- Monthly scans: 11 days

You can specify a time interval in which to attempt a scheduled scan.

To set options for missed scheduled scans

1. In the Symantec System Center console, right click a Symantec AntiVirus server, server group, client group, or individual client, and then click **All Tasks** > **Symantec AntiVirus** > **Scheduled Scans**.
2. In the Scheduled Scans dialog box, select a scan in the list of scans.
3. Click **Edit**.
4. In the Scheduled Scan dialog box, click **Advanced**.
5. In the Advanced Schedule Options dialog box, click **Handle Missed Events Within**.
6. Specify the time interval for reattempting the scheduled scan.
7. Click **OK** until the main Symantec System Center console window appears.

Editing, deleting, or disabling a scheduled scan

If you want to modify the properties of an existing scheduled scan, you can edit it. If you want to stop a scheduled scan from occurring, you can delete or disable it.

Edit, delete, or disable a scheduled scan

You can edit, delete, or disable a scheduled scan.

To edit or delete a scheduled scan

1. In the Symantec System Center console, right-click one or more server groups, a server, or a client for which you want to edit or delete the scheduled scan, and then click **All Tasks** > **Symantec AntiVirus** > **Scheduled Scans**.
2. In the Scheduled Scans dialog box, select one of the following:
   - Server Scans: Edit or delete scans for servers. This option is not available if you selected a client computer in step 1.
   - Client Scans: Edit or delete scans for clients. This option is not available if you selected a server group in step 1.
3. Do one of the following:
   - Select an existing scan, and then click **Edit**. Change any properties that you want, and then click **OK** until you return to the Symantec System Center main window.
   - Select an existing scan, and then click **Delete**. Click **OK** until you return to the Symantec System Center main window.

To disable a scheduled scan

1. In the Symantec System Center console, right-click one or more server groups, a server, or a client for which you want to disable the scheduled scan, and then click **All Tasks** > **Symantec AntiVirus** > **Scheduled Scans**.
   The scans that you can disable depend on the object that you select.
2. In the Scheduled Scans dialog box, select one of the following:
   - Server Scans: Disable scans for servers. This option is not available if you selected a client computer in step 1.
   - Client Scans: Disable scans for clients. This option is not available if you selected a server group in step 1.
3. Uncheck the previously scheduled scan.
4. Click **OK**.

Running a scheduled scan on demand

When you create and save a scheduled scan, Symantec AntiVirus remembers the server group, server, or computer on which to run the scan and also remembers all of the settings that you chose for that specific scan.

After you configure a scheduled scan (and all of its scan properties), you might want to run it on demand at some time other than when you originally scheduled it. This can save you the effort of configuring and running a manual scan with similar properties.

To run a scheduled scan on demand

1. In the Symantec System Center console, right-click a server group or a server, and then click **All Tasks** > **Symantec AntiVirus** > **Scheduled Scans**.
2. In the Scheduled Scans dialog box, select one of the following:
   - Server Scans: Run a server scan on demand. This option is not available if you selected a server group in step 1.
   - Client Scans: Run a client scan on demand. This option is not available if you selected a server group in step 1.
3. Select an existing scheduled scan.
4. Click **Start Scan**.

Deleting files and folders that are left on computers by threats

When Symantec AntiVirus deletes a file that is part of a threat category, such as adware or spyware, other files related to the threat may remain on the computer. The remaining files are not likely to cause a problem but you may want to delete them manually to free up disk space on the computer.

Handling Symantec AntiVirus clients with intermittent connectivity

Each Symantec AntiVirus server stores a list of Symantec AntiVirus clients that it manages, and provides this data to the Symantec System Center. By default, clients check in with their parent servers once an hour, and parent servers review their lists of clients once an hour. Parent servers track client check-in times; if a client fails to check in with its parent server for more than thirty days, the parent server removes that client from its list of clients and logs that client as deleted. The next time that the Symantec System Center queries the parent server for a list of its clients, that client will not appear.

You can control this behavior by configuring the following settings:

- The client expiration interval
- The client check-in interval

Handle Symantec AntiVirus clients with intermittent connectivity

By default, the client check-in interval is set to 60 minutes. The interval may be changed with the CheckConfigMinutes registry value.

The client expiration interval must be greater than the client check-in interval or the parent server will delete and add clients continually.

If the new client configuration is not immediately received by the parent server or by the client, the information is updated during the client check-in.

To modify the client expiration interval

1. On the parent server, locate the following registry key:
   HKEY_LOCAL_MACHINE\Software\Intel\LANDesk\VirusProtect6\CurrentVersion directory
2. On the Edit menu, click **New** > **DWORD Value**.
3. Name the value as follows:
   ClientExpirationTimeout
4. Right-click the new key, and then click **Modify**.
5. In the Value Data box, replace the 0 with a number greater than 0.
   Without the use of the ClientExpirationTimeout value, the default time is 720 hours. Use a smaller value to decrease the number of minutes that it takes for the client to be removed from the console, or use a larger value to increase the time. For example, if a large number of your client computers are being removed from the Symantec System Center because people are away from the office and their computers are turned off, you can specify a larger number.
6. Click **OK**.
7. Exit Regedit.

To modify the client check-in interval

1. In the Symantec System Center console, right-click a server, server group, or client group, and then click **All Tasks** > **Symantec AntiVirus** > **Virus Definition Manager**.
2. In the Virus Definition Manager dialog box, check **Update Virus Definitions From Parent Server**.
3. Click **Settings**.
4. In the Update Settings dialog box, in the Check for updates every box, type the interval in minutes.
5. Click **OK** until the main Symantec System Center console window appears.

Configuring scan options

Many of the same scan options are available in different types of scans. For example, you can assign primary actions and secondary actions when configuring manual, scheduled, or Auto-Protect scans.

How to assign primary actions and secondary actions for detected viruses

You can assign a primary action and, in case the primary action is not possible, a secondary action for Symantec AntiVirus to take when it discovers a virus. You can assign separate actions for macro viruses and non-macro viruses.

You can assign the following actions for detected viruses:

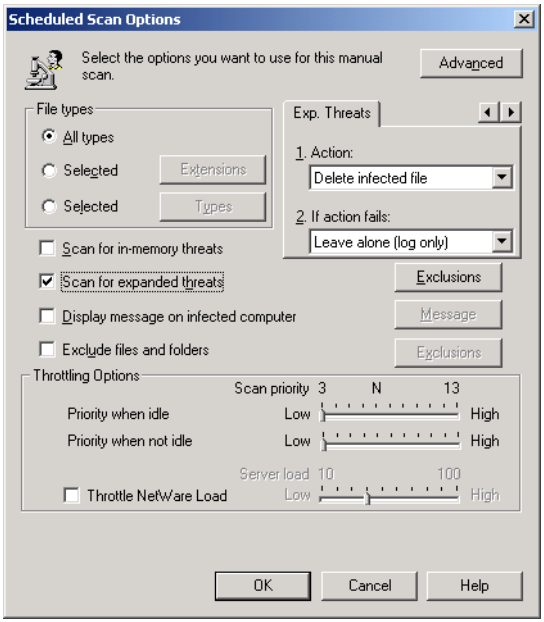
Clean virus from file	Attempts to clean an infected file upon detection.
Quarantine infected file	Attempts to move the infected file to the Quarantine on the infected computer as soon as it is detected. After an infected file is moved to the Quarantine, no user can execute it until you take an action (for example, clean or delete) and move the file back to its original location.
Delete infected file	Attempts to delete the file. Use this option only if you can replace the infected file with a virus-free backup copy because the file is permanently deleted and cannot be recovered from the Recycle Bin. If Symantec AntiVirus cannot delete the file, detailed information about the action that Symantec AntiVirus took appears in the Notification dialog box and Symantec AntiVirus Event Log.
Leave alone (log only)	Denies access to the file, displays a threat notification, and logs the event. Use this option to control how Symantec AntiVirus handles a virus. When you are notified of a virus, open the Threat History for the computer, right-click the name of the infected file, and select one of the following actions: Clean, Delete Permanently, or Move To Quarantine.

By default, Symantec AntiVirus first attempts to clean the file. If Symantec AntiVirus cannot clean the file, it moves the file to the Quarantine on the infected computer, denies access to the file, and logs the event.

How to assign primary actions and secondary actions for other detected threats

You can assign a primary action and, in case the primary action is not possible, a secondary action for Symantec AntiVirus to take when it discovers a threat other than a virus, such as adware or spyware.

Figure 3-2 Scheduled Scan Options dialog box with Exp. Threats tab



In the Scheduled Scan Options dialog box, shown in Figure 3-2, you can assign the following actions for other detected threats:

- Delete infected file: Attempts to delete the file. This action is available when deleting the file will not cause a system failure.
- Leave alone (log only): Denies access to the file, displays a virus notification, and logs the event. Use this option to control how Symantec AntiVirus handles a threat. An alert is sent when the threat is detected but no action is taken. You must then take action. For example, you may need to notify the user, and then instruct the user to uninstall the software that poses a threat.

Controlling the user experience

Symantec AntiVirus allows you to control several aspects of the Symantec AntiVirus client user experience. You can do any of the following:

- Deny or permit users the ability to unload Symantec AntiVirus.
- Require a password before permitting an uninstallation.
- Allow users to pause or stop a scheduled scan.
- Display a scan progress window.
- Display and customize a warning message on an infected computer. For example, if users have a spyware program installed on their computers, you can notify them that they have violated your corporate policy and must uninstall the application immediately.
- Add an infection warning to an infected email message.
- Notify the sender of an infected email message.
- Notify others about the receipt of an infected email message.

Denying or permitting users the ability to unload Symantec AntiVirus

You can deny or permit users the ability to unload Symantec AntiVirus.

To deny or permit users the ability to unload Symantec AntiVirus

1. In the Symantec System Center console, right-click a server, server group, or client group, and then click **All Tasks** > **Symantec AntiVirus** > **Client Administrator Only Options**.
2. Click the Security tab.
3. Change the setting for **Lock the ability of users to unload Symantec AntiVirus Services**.
4. Click **OK**.

Requiring a password before uninstalling

You can require Symantec AntiVirus to prompt for a password before permitting an uninstallation.

To require a password before uninstalling

1. In the Symantec System Center console, right-click a server, server group, or client group, and then click **All Tasks** > **Symantec AntiVirus** > **Client Administrator Only Options**.
2. Click the Security tab.
3. Check **Ask for password to allow uninstall of Symantec AntiVirus Client**.
4. Click **Change**.
5. In the Configure Password dialog box, type a new password, and then confirm by typing the password again.
6. Click **OK** until the main Symantec System Center console window appears.

Allowing users to pause, snooze, or stop a scheduled scan

You can allow users to temporarily pause or snooze a scheduled scan, as well as stop the scan entirely. The results are as follows:

- Paused scan: When a user pauses a scan, the Scan Results dialog box remains open, waiting for the user to either continue or abort the scan. If the computer is shut off, the paused scan will not continue.
- Snoozed scan: When a user snoozes a scheduled scan, the user has the option of snoozing the scan for one hour, or (depending on the configuration) for three hours. In addition, the number of snoozes is configurable. When a scan is snoozing, the Scan Results dialog box closes, and reappears when the snooze period ends and the scan resumes.

Allow users to pause, snooze, or stop a scan

A paused scan automatically restarts after a specified time interval elapses. A stopped scan will not restart.

To allow users to pause or snooze a scan

1. In the Symantec System Center console, right-click a server group, server, or client group, and then click **All Tasks** > **Symantec AntiVirus** > **Scheduled Scan**.
2. In the Scheduled Scans dialog box, do one of the following:
   - Select a scheduled scan, and then click **Edit**.
   - Click **New** to create a new scan.
3. In the Scheduled Scan dialog box, click **Scan Settings**.
4. In the Select Items dialog box, click **Options**.
5. In the Scheduled Scan Options dialog box, click **Advanced**.

6 In the Scan Advanced Options dialog box, click **Show scan progress on computer being scanned**.

7 Uncheck **Allow user to stop scan**.

8 Check **Allow user to pause/snooze scan**.

9 Click **Pause Options**.

10 In the Pause Options dialog box, do one of the following:

- Limit the number of minutes that a user may pause a scan: Check **Limit the time this scan may be paused** and type a number of minutes.
- Limit the number of times a user may pause a scan: In the Number of times it can snooze box, type a number.
- Display a three-hour snooze button: Check **Enable the 3 hour snooze**. By default, a user can pause a scan for one hour. You must enable this option to allow a user to pause a scan for three hours.

11 Click **OK** until the main Symantec System Center console window appears.

To allow users to stop a scan

1 In the Symantec System Center console, right-click a server group, server, or client group, and then click **All Tasks** > **Symantec AntiVirus** > **Scheduled Scan**.

2 In the Scheduled Scans dialog box, do one of the following:

- Select a scheduled scan, and then click **Edit**.
- Click **New** to create a new scan.

3 In the Scheduled Scan dialog box, click **Scan Settings**.

4 In the Select Items dialog box, click **Options**.

5 In the Scheduled Scan Options dialog box, click **Advanced**.

6 In the Scan Advanced Options dialog box, click **Show scan progress on computer being scanned**.

7 Check **Allow user to stop scan**.

8 Uncheck **Allow user to pause/snooze scan**.

9 If you want to automatically close the scan progress indicator after the scan completes, check **Close scan progress when done**.

10 Click **OK** until the main Symantec System Center console window appears.

Displaying and customizing a warning message on an infected computer

When you run a remote scan on a user's computer, you can immediately notify the user of a problem by displaying a warning message on the infected computer's screen. You can customize the warning message by including information such as the name of the threat, the name of the infected file, the status of the infection, and so on.

The default warning message contains message variables and text. The message variable is in brackets. Everything outside the brackets is text. You can change the text and message variables that are in the warning message to suit your needs. Table 3-4 describes the message variables.

Table 3-4 Warning message variables

Variable	Text
[LoggedBy]	Type of scan that logged the event: Auto-Protect, scheduled, or manual scan.
[Event]	Type of event, such as Threat Found.
[VirusName]	Name of detected threat.
[PathAndFilename]	Full path and file name.
[Location]	Drive location on the infected computer.
[Computer]	Name of the computer.
[User]	Network logon name of the user.
[ActionTaken]	Action that was taken on the infected file (such as cleaned, moved to the Quarantine, deleted, or left alone).
[DateFound]	Date and time that the threat was found.
[Status]	State of the file: Infected, Not Infected, or Deleted. This message variable is not used by default. If you want to display this information, you must manually add the variable to the warning message.

For example, a warning message might look as follows:

```
Scan type: Scheduled Scan
Event: Threat Found
VirusName: Stoned-C
File: C:\Autoexec.bat
Location: C:
```

```
Computer: ACCTG-2
User: JSmith
Action taken: Cleaned
```

To display and customize a warning message on an infected computer

1. In the Symantec System Center console, right-click a server group, Symantec AntiVirus server, or client group, and then click **All Tasks** > **Symantec AntiVirus** > **Client Auto-Protect Options**.
2. In the Client Auto-Protect Options dialog box, click **Display Message on infected Computer**.
3. Do one of the following:
   - Click **OK** to accept the default message.
   - Click **Message** and customize the text, and then click **OK**.
4. Click **OK** until the Client Auto-Protect Options dialog box disappears.

Adding an infection warning to an infected email message

For supported email software, you can configure Auto-Protect to automatically insert a warning into the body of an infected email message. This type of warning can be important if Symantec AntiVirus is unable to clean the virus from the message, and if an infected attachment file is moved, left alone, deleted, or renamed. The warning message tells you which virus was found and explains the action that was taken.

Symantec AntiVirus appends this text to the top of the email message that is associated with the infected attachment:

Symantec AntiVirus found a virus in an attachment from [EmailSender].

For each infected file, the following information is also added to the email message:

- Name of the file attachment
- Name of the virus
- Action taken (such as cleaned, moved to the Quarantine, deleted, or left alone)
- File status (infected or not infected)

You can customize the subject and body of the message.

The email message contains a field called [EmailSender]. All fields in brackets contain variable information. You can customize the default message by right-clicking the body of the message and selecting a field to insert into the message.

The message would look as follows to the recipient:

Symantec AntiVirus found a virus in an attachment from John.Smith@mycompany.com.

To add an infection warning to an infected email message

1. In the Symantec System Center console, right-click a server group, Symantec AntiVirus server, or client group, and then click **All Tasks** > **Symantec AntiVirus** > **Client Auto-Protect Options**.
2. In the Client Auto-Protect Options dialog box, on either the Lotus Notes or Microsoft Exchange tab, click **Insert warning into email message**.
3. Do one of the following:
   - Click **OK** to accept the default message.
   - Click **Warning** and customize the text, and then click **OK**.
4. Click **OK** until the Client Auto-Protect Options dialog box disappears.

Notifying the sender of an infected email message

For supported email software, you can configure Auto-Protect to respond automatically to the sender of an email message that contains an infected attachment.

Symantec AntiVirus sends a reply email message with the following subject:

Virus Found in message “[EmailSubject]”

The body of the message informs the sender of the infected attachment:

Symantec AntiVirus found a virus in an attachment you ([EmailSender]) sent to [EmailRecipientList].

For each infected file, the following information is also added to the email message:

- Name of the file attachment
- Name of the virus
- Action taken (such as cleaned, moved to the Quarantine, deleted, or left alone)
- File status (infected or not infected)

To notify a sender of an infected email message

1. In the Symantec System Center console, right-click a server group, Symantec AntiVirus server, or client group, and then click **All Tasks** > **Symantec AntiVirus** > **Client Auto-Protect Options**.

2. In the Client Auto-Protect Options dialog box, on either the Lotus Notes or Microsoft Exchange tab, click **Enable Lotus Notes (Microsoft Exchange) Auto-Protect**.
3. Click **Send e-mail to sender**.
4. Click **Message**.
5. Do one of the following:
   - Click **OK** to accept the default message.
   - Click **Message** and customize the text, and then click **OK**.
6. Click **OK** until the Client Auto-Protect Options dialog box disappears.

Notifying others of an infected email message

For supported email software, you can configure Auto-Protect to notify others whenever an email message that contains an infected attachment is opened.

Symantec AntiVirus sends an email message to the selected recipients with the following subject:

Virus Found in message “[EmailSubject]”

The body of the message includes information on the sender of the infected attachment:

Symantec AntiVirus found a virus in an attachment from [EmailSender].

For each infected file, the following information is also added to the email message:

- Name of the file attachment
- Name of the virus
- Action taken (such as cleaned, moved to the Quarantine, deleted, or left alone)
- File status (infected or not infected)

To notify others of an infected email message

1. In the Symantec System Center console, right-click a server group, Symantec AntiVirus server, or client group, and then click **All Tasks** > **Symantec AntiVirus** > **Client Auto-Protect Options**.
2. In the Client Auto-Protect Options dialog box, on either the Lotus Notes or Microsoft Exchange tab, click **Enable Lotus Notes (Microsoft Exchange) Auto-Protect**.
3. Click **Send e-mail to selected**.
4. Click **Addresses**.
5. In the Email Address dialog box, provide one or more email addresses to which notification will be sent.
6. Click **OK**.
7. Click **Message**.
8. Do one of the following:
   - Click **OK** to accept the default message.
   - Click **Compose** and customize the message, and then click **OK**.
9. Click **OK** until the Client Auto-Protect Options dialog box disappears.

Scanning for in-memory threats

You can configure manual and scheduled scans to scan running processes to identify and handle threats that are loaded into memory. Symantec AntiVirus can terminate the process and handle the threat-infected file based on your specified primary and secondary actions.

If the infected file is associated with an important process, you may need to shut down the computer, and then restart it.

In-memory scanning does not scan specifically for memory-resident threats, such as the SQL Slammer worm. It scans for all threats that may be in memory.

Excluding files from scanning

Exclusions help you balance the amount of protection your network requires with the amount of time and resources that are required to provide that protection. For example, when you scan all file types, you may want to exclude certain folders that contain only data files that are not subject to viruses. This decreases the overhead that is associated with needlessly scanning files.

Using the Symantec System Center, you can set exclusions for specific file extensions and folders. In addition, certain Symantec AntiVirus scans allow exclusion by named folder (for example, you can exclude scans of the path C:\Temp\Install). To maintain security, you cannot view or exclude specific files from the Symantec System Center. You can, however, exclude specific files using the Symantec AntiVirus client or server user interface. You may want to exclude files that trigger false positive alerts. For example, if you used another virus scanning program to clean infected files and the program did not completely remove the virus code, the file may be harmless but the disabled virus code might cause Symantec AntiVirus to register a false positive. Check with Symantec Technical Support if you are not sure if a file is infected.

Table 3-5 describes exclusions.

Table 3-5 Exclusions by object type

Object type	Exclusions available
Server group	Server scans: File extensions and named folders
Server	■ Server scans: File extensions, drivers, files, and folders ■ Client scans: File extensions, drivers, and named folders
Client group	Client scans: File extensions, drivers, and named folders
NetWare servers	Files by drivers and named folders; you cannot exclude files by file extension

Setting exclusions

Symantec AntiVirus exclusions behavior is as follows:

- When Symantec AntiVirus applies exclusions, the excluded items are not scanned. If the file is not excluded, it is scanned.
- For virus sweep, manual, Auto-Protect, and scheduled scans, Symantec AntiVirus takes no action on excluded files.

Enabling and disabling exclusions can improve performance depending on the situation. For example:

- If you copied a large folder that was in the exclusions list and the exclusions setting was enabled, the copying process would not take as long since the folder's contents would be excluded.
- If you copied a large folder that was not in the exclusions list, disabling exclusions would improve performance.

To set exclusions

1. In the Scan Options dialog box for the type of scan that you want to configure, click **Exclude files and folders**.
2. Click **Exclusions**.
3. In the Exclusions dialog box, check **Check file for exclusion before scanning** to enable prescan exclusions.
4. Depending on the types and numbers of computers that you are configuring, you can do the following:
   - Select file extensions to exclude by extension or wildcard.
   - Select files to exclude within specific folders by extension, wildcard, or file type.
   - Select folders to exclude from the scan.
5. Click **OK** until the Symantec System Center console appears.

Selecting file types and extensions to scan for viruses

By default, Symantec AntiVirus scans all files during a virus scan. For scans other than Auto-Protect scanning, you can select to scan only files of a specific file type or with specific extensions. Scans by file type and extension are available when you select the following objects and scan types:

- Client object: Manual scan, scheduled scan, and client Auto-Protect
- Server object: Virus sweep, manual scan, scheduled server scan, and server Auto-Protect (Windows only)

When you scan by file type, Symantec AntiVirus reads each file's header to determine the file type. For example, if you enable document scanning, Symantec AntiVirus scans all documents even if you name them with nonstandard extensions, such as Document3.mlt instead of Document3.doc.

Note: This option doesn't apply to NetWare servers; it applies only to Windows-based computers.

When you scan by file extension, Symantec AntiVirus does not read the file header to determine the file type and scans only files with the extensions that you specify. Table 3-6 describes the recommended extensions.

Table 3-6 Recommended file extensions for scanning

File extension	Description
386	Driver
ACM	Driver; audio compression manager
ACV	Driver; audio compression/decompression manager
ADT	ADT file; fax
AX	AX file
BAT	Batch
BTM	Batch
BIN	Binary
CLA	Java Class
COM	Executable
CPL	Applet Control Panel for Microsoft Windows
CSC	Corel Script
DLL	Dynamic Link Library
DOC	Microsoft Word
DOT	Microsoft Word
DRV	Driver
EXE	Executable
HLP	Help file
HTA	HTML application
HTM	HTML
HTML	HTML
HTT	HTML
INF	Installation script
INI	Initialization file

Table 3-6 Recommended file extensions for scanning

File extension	Description
JS	JavaScript
JSE	JavaScript Encoded
JTD	Ichitaro
MDB	Microsoft Access
MP?	Microsoft Project
MSO	Microsoft Office 2000
OBD	Microsoft Office binder
OBT	Microsoft Office binder
OCX	Microsoft object linking and embedding custom control
OV?	Overlay
PIF	Program information file
PL	PERL program source code (UNIX)
PM	Presentation Manager Bitmaps Graphics
POT	Microsoft PowerPoint
PPT	Microsoft PowerPoint
PPS	Microsoft PowerPoint
RTF	Rich Text Format document
SCR	Fax/screensaver/snapshot, script for Faxview/Microsoft Windows
SH	Shell Script (UNIX)
SHB	Corel Show Background file
SHS	Shell scrap file
SMM	AmiPro
SYS	Device driver
VBE	VESA BIOS (Core Functions)
VBS	VBScript
VSD	Visio
VSS	Visio

Table 3-6 Recommended file extensions for scanning

File extension	Description
VST	Visio
VXD	Virtual device driver
WSF	Windows Script File
WSH	Windows Script Host Settings File
XL?	Microsoft Excel

Select file types and extensions to scan for viruses

For all scan types, you can select files to scan by program type and extension. For scheduled and manual scans, you can also select files to scan by extension and program type at the folder level.

To select files to scan by extension

1. In the Scan Options dialog box for the scan that you want to configure, click the appropriate **Selected** button.
2. Click **Extensions**.
3. In the Selected Extensions dialog box, you can select one of the following:
   - Add: Add your own extension by typing the extension and clicking **Add**.
   - Documents: Add all document extensions.
   - Programs: Add all program extensions.
   - Use Defaults: Add all extensions and program types.
4. Click **OK** until the Symantec System Center console appears.

To select files to scan by program type

1. In the Scan Options dialog box for the scan that you want to configure, click the appropriate **Selected** button.
2. Click **Types**.
3. In the Selected Types dialog box, select one of the following:
   - Document files: Scan document files regardless of their extensions.
   - Program files: Scan MS-DOS and Windows program files.
4. Click **OK** until the Symantec System Center console appears.

To select files to scan by folder for manual scans

1. In the Symantec System Center console, right-click the object that you want to scan, and then click **All Tasks** > **Symantec AntiVirus** > **Start Manual Scan**.
2. In the Select Items dialog box, select the folders to scan.
3. Click **Options** and select the extensions and types to scan for the selected folders.
4. Click **OK** until the Symantec System Center console appears.

To select files to scan by folder for scheduled scans

1. In the Symantec System Center console, right-click the object that you want to scan, and then click **All Tasks** > **Symantec AntiVirus** > **Scheduled Scans**.
2. On the Server Scans tab, in the Server scans list, select a scan.
3. Click **Edit**.
4. In the Scheduled Scan dialog box, click **Scan Settings**.
5. In the Select Items dialog box, select the folders to scan.
6. Click **Options** and select the extensions and types to scan for the selected folders.
7. Click **OK** until the Symantec System Center console appears.

When you make selections in the tree, the icons change as listed in Table 3-7.

Table 3-7 Tree view icons

Icon	Description
	Symantec AntiVirus will scan all of the files in this folder and also all of the files in subfolders.
	Symantec AntiVirus will scan one or more items that you've selected in the folder or one of the subfolders.
	Symantec AntiVirus will scan the selected file. This is available only from the client or server interface.
	Symantec AntiVirus does not scan the folder or subitems.

Enabling expanded threat categories

You can scan client or server objects for the following threat categories during manual scan and scheduled scans:

- Spyware
- Adware
- Dialers
- Joke programs
- Remote access programs
- Hack tools
- Trackware

See "About threats" on page 89.

Enable expanded threat scanning and exclude threat categories if necessary

By default, Symantec AntiVirus does not scan for threats other than viruses and blended threats. You must enable expanded threat scanning.

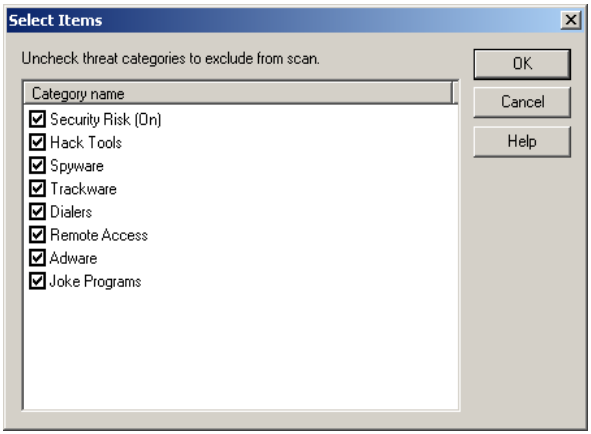
You can also exclude an expanded threat category for which you don't want Symantec AntiVirus to scan.

To enable expanded threat scanning

1. In the Symantec System Center console, do one of the following:
   - Right-click a server or client computer.
   - Select one or more servers that are in the same server group, and then right-click the servers.
   - Select one or more clients that are managed by the same server, and then right-click the clients.
2. Click **All Tasks** > **Symantec AntiVirus** > **Start Manual Scan**.
3. In the Select Items dialog box, click **Options**.
4. In the Scan Options dialog box, click **Scan for expanded threats**.
5. Click **Save Settings** if you want Symantec AntiVirus to remember these options for future manual scans on this computer.
   Symantec AntiVirus also remembers these settings for future scans when you select multiple computers.

To exclude an expanded threat category from scanning

1. In the Symantec System Center console, do one of the following:
   - Right-click a server or client computer.
   - Select one or more servers that are in the same server group, and then right-click the servers.
   - Select one or more clients that are managed by the same server, and then right-click the clients.
2. Click **All Tasks** > **Symantec AntiVirus** > **Start Manual Scan**.
3. In the Select Items dialog box, click **Options**.
4. In the Scan Options dialog box, ensure that Scan for expanded threats is enabled.
5. Click **Exclusions**.



6. In the Select Items dialog box, uncheck each threat category that you want to exclude.
7. Click **OK** until you return to the Scheduled Scans dialog box.

Setting options for scanning compressed files

Table 3-8 lists and describes the scanning options that are available for compressed files.

Table 3-8 Options for scanning compressed files

Operating system	Scanning option
Windows	Symantec AntiVirus scans compressed files during manual, email, and scheduled scans. Because of the significant processing overhead, Auto-Protect does not scan files that are within compressed files on Windows computers; however, the files are scanned as they are extracted from compressed files.
NetWare	Symantec AntiVirus scans compressed files during Auto-Protect and scheduled scans. In order to scan the contents of a compressed file, Symantec AntiVirus extracts each file, one file at a time, from the container and copies it to the SYS volume where it is scanned. The SYS volume must have enough space available on the volume to accommodate the largest file in the container.

In the Scan Advanced Options dialog box, you can set options for scanning compressed files that are nested within compressed files. If you check Scan Inside Compressed Files, Symantec AntiVirus scans the container (such as Files.zip) and the contents of the container, which are the individual, compressed files. Symantec AntiVirus supports a maximum depth of ten levels of nested compressed files; NetWare servers are limited to eight levels.

Note: You cannot stop a scan that is in progress on a compressed file. If you click Stop Scan, Symantec AntiVirus stops the scan only after it has finished scanning the compressed file.

Configuring HSM settings

Symantec AntiVirus includes settings that allow you to fine tune scans of files that are maintained by Hierarchical Storage Management (HSM) and offline backup systems. An HSM system migrates files to secondary storage such as CD-ROM, tape jukebox, SAN storage, and so on, but it may leave parts of the original file on the disk. Performance and disk space issues arise during scans if Symantec AntiVirus opens all of the stubs and the HSM system places the files back on the original disk. Consult your HSM or backup vendor to select the appropriate settings. The settings are dependent on how your HSM application operates.

Table 3-9 lists HSM scanning options for Windows 2000 and later.

Table 3-9 Storage migration options (Windows 2000 and later)

Option	Description
Skip offline files	If the offline bit is set, the file is skipped. A small clock over a file's icon in Windows Explorer indicates that the offline bit is set. Any application may set the offline bit without actually placing the file offline.
Skip offline and sparse files	Some applications set the file sparse bit to indicate that part of the file is not present on the disk. Because some HSM products set this bit and others don't, consult your HSM vendor to verify whether the sparse bit is set. With a sparse file, a stub of the file remains on the disk with the majority of the file moved to offline storage.
Skip offline and sparse files with a reparse point	Some vendors use reparse points. An application that uses reparse points will also use an appropriate device driver to manage reparse points in the files. This is the default Symantec AntiVirus setting because it is the most reliable for vendors that use reparse points. Consult your HSM vendor to determine if this setting is appropriate. With a reparse point, a portion of the file remains on disk with the remainder transparently accessed through an application filter (the device driver).
Scan resident portions of offline and sparse files	Symantec AntiVirus identifies resident portions of a file. If the file is sparse, only the resident portion is scanned; the nonresident portion remains in secondary storage. Because some vendors support this capability and others do not, consult your HSM vendor to determine if this setting is appropriate.
Scan all files, forcing demigration (fills drive)	The entire file is scanned, which forces demigration from secondary storage if necessary. Because the size of the secondary storage is usually greater than the size of the local volume, this setting may fill the local volume and cause further files that are opened for scanning to fail.

Table 3-9 Storage migration options (Windows 2000 and later)

Option	Description
Scan all files without forcing demigration (slow)	Symantec AntiVirus copies a file from secondary storage to the local hard drive as a temp file for scanning, but the HSM application leaves the original file on the secondary storage. This method is slow and not supported by all HSM vendors. Because a file is copied from secondary storage to a disk for scanning, resource demand is high. Processor and network performance may further degrade as infected content is detected when a repair or deletion is returned to secondary storage.
Scan all files recently touched without forcing demigration	To reduce some of the resource demand issues with the Scan all files without forcing demigration option, this option lets you specify that only files that have been migrated recently and may still reside on faster secondary storage are scanned. It may be appropriate to scan files if they still reside on the faster secondary disk, and skip demigration and scanning if the files reside on the slow, long-term storage. For example, files may first be migrated to a remote disk after 30 days of no access. After 60 days of no access, the file is migrated to CD-ROM or remote SAN storage. In many cases, this method may still be slow because accessing files without forcing demigration is a relatively slow operation.
Open files using backup semantics	You can allow scanning of files that, for security reasons, are normally not readable except by a specific user.

Table 3-10 lists the HSM scanning option for NetWare.

Table 3-10 Storage migration option (NetWare)

Option	Description
Scan NetWare compressed or migrated files	NetWare compressed or migrated files are scanned.

To configure HSM settings

- In the Scan Advanced Options dialog box, for the type of scan that you want to configure, select the appropriate options.

Setting CPU utilization

For scheduled and manual scans, Symantec AntiVirus allows you to control the scan's CPU priority. Giving a scan a lower priority means that the scan will take longer to complete, but also frees the CPU to work on other tasks. You may want to set a lower priority in some situations. For example, if you have scans running at lunch time during the work week, you might want to lower the scan priority to minimize the impact on user productivity.

You set scan priority using sliders in the Scan Options dialog box. You can specify scan priority for:

- Windows computers: Priority differs depending on whether the computer is idle or not idle. The idle setting specifies the priority that is assigned to scans when the computer is idle. The not idle setting specifies the priority that is assigned to scans when the computer is actively working.
- NetWare computers: Symantec AntiVirus can throttle its load on NetWare servers. A lower load setting means the server scan will take longer to complete.

Chapter 4

Updating virus definitions files

This chapter includes the following topics:

- About virus definitions files
- Virus definitions files update methods
- Updating virus definitions files on Symantec AntiVirus servers
- Updating virus definitions files on Symantec AntiVirus clients
- Controlling virus definitions files
- Testing virus definitions files
- Update scenarios
- About scanning after updating virus definitions files

About virus definitions files

Virus definitions files contain sample code for thousands of threats. When Symantec AntiVirus scans for threats, it attempts to find matches between your files and sample code that is inside of the virus definitions files. If Symantec AntiVirus finds a match, the file may be infected.

Every server and client that runs Symantec AntiVirus has a copy of the virus definitions files. These files can become outdated as new viruses and other threats are discovered. Symantec updates virus definitions files about once a week, or more frequently if needed. It's important to keep virus definitions files current to maintain the highest level of protection for your network.

Virus definitions files update methods

There are several methods that are available for downloading virus definitions and setting up servers and clients to retrieve them.

Table 4-1 describes the virus definitions files update methods.

Table 4-1 Virus definitions files update methods

Method	Description	When to use it
Virus Definition Transport Method	A push operation starts when new virus definitions are received via the Symantec FTP site or LiveUpdate server by a primary server on your network. The primary server passes a virus definitions package to all of the secondary servers in the server group. Secondary servers extract the definitions and place them in the appropriate directory. Clients receive the package from their parent servers. Clients extract the definitions and place them in the appropriate directory.	Use the Virus Definition Transport Method when you want to control virus definitions files updates from the Symantec System Center. In addition, use this method during a virus outbreak to push the latest virus definitions files to the computers on your network immediately.
LiveUpdate	A scheduled pull operation starts when a client or server on which LiveUpdate is being used requests new definitions. LiveUpdate may be configured on each computer to request the update from a designated internal LiveUpdate server or directly from the Symantec LiveUpdate server.	Use LiveUpdate when you want protected computers to pull virus definitions files updates from an internal LiveUpdate server, or directly from Symantec.
Central Quarantine polling	The Central Quarantine Server periodically polls the Symantec Digital Immune System gateway for new virus definitions files. When new definitions are available, the Central Quarantine Server can push the new definitions to the computers that need it automatically.	Use Central Quarantine when you want to automate the distribution of virus definitions files updates across your network.

Table 4-1 Virus definitions files update methods

Method	Description	When to use it
Intelligent Updater	Intelligent Updater is a self-extracting executable file that contains virus definitions files.	Use Intelligent Updater when you need to distribute virus definitions files updates to users who do not have active network connections.

Note: 64-bit computers receive virus definitions files using LiveUpdate. All other methods of updating these files are not supported.

Best practice: Using the Virus Definition Transport Method and LiveUpdate together

You can use the Virus Definition Transport Method and LiveUpdate together. Using LiveUpdate allows for updates to the software components of Symantec AntiVirus. Using the Virus Definition Transport Method allows you to schedule and push virus definitions files updates from the Symantec System Center. In addition, you can use the Virus Definition Transport Method as an emergency system for distributing new virus definitions files quickly when the network is threatened by a new virus.

Although the Virus Definition Transport Method is used more often, some large networks depend on LiveUpdate. These installations do not permit direct access to the Symantec site by a large number of servers and clients. One or more servers act as an internal LiveUpdate server to all of the other servers on the network, and in some installations, to all clients.

Best practice: Using Continuous LiveUpdate on 64-bit computers

To ensure that each managed 64-bit computer maintains the latest virus definitions, you can use Continuous LiveUpdate to require each computer to check for updates after a specified interval has expired. If you have more than one 64-bit computer on your network and you are using the Symantec System Center console, you can group these computers into a client or server group and manage the virus definitions from the console. If you are not using the console, you can enable this feature and set the interval on the client computer.

See "Enabling and configuring Continuous LiveUpdate for managed clients" on page 164.

Updating virus definitions files on Symantec AntiVirus servers

There are several methods for updating virus definitions files on servers:

- Virus Definition Transport Method
- LiveUpdate
- Intelligent Updater
- Central Quarantine polling

See "Virus definitions files update methods" on page 146.

Updating and configuring Symantec AntiVirus servers using the Virus Definition Transport Method

Update Symantec AntiVirus servers manually when you need to force an immediate update. Schedule automatic updates to handle routine virus definitions files updating without requiring further interaction.

Update servers manually or automatically using the Virus Definition Transport Method

You can update servers manually or automatically. Updates occur only when the virus definitions files on a server are older than the definitions that are available on the LiveUpdate server.

To update all unlocked servers in the system

1. In the Symantec System Center console, right-click **System Hierarchy**, and then click **Symantec AntiVirus** > **Update Virus Defs Now**.
2. Click **Yes** in the confirmation dialog box.
3. Click **OK** in the status dialog box.

To update servers manually

1. In the Symantec System Center console, right-click a server or server group, and then click **All Tasks** > **Symantec AntiVirus** > **Virus Definition Manager**.
2. Select one of the following:
   - Update The Primary Server Of This Server Group Only: To update all servers in the group from the primary server
   - Update Each Server In This Server Group Individually: To update servers individually

The option that you select affects all of the servers in the server group, whether you right-click a server group or an individual server.

3 Click **Configure**.

4 Click **Update Now**.
A message appears with information about how you can view the date of the new virus definitions file.

5 Read the information that appears, and then click **OK** until the Symantec System Center console reappears.

To update servers automatically

1 In the Symantec System Center console, right-click a server or server group, and then click **All Tasks** > **Symantec AntiVirus** > **Virus Definition Manager**.

2 Select one of the following:
- Update The Primary Server Of This Server Group Only: To update all servers in the group automatically from the primary server
- Update Each Server In This Server Group Individually: To update servers individually

The option that you select affects all servers in the server group, whether you right-click a server group or an individual server.

3 Click **Configure**.

4 Ensure that Schedule For Automatic Updates is checked, and then click **Schedule**.

5 Select options to determine when the virus definitions file will update (for example, every Tuesday at 10:00 P.M.).

6 Click **OK** until you return to the Symantec System Center main window.

Updating a master primary server

Configure a master primary server to limit your network's exposure to the Internet.

To configure a master primary server

1 In the Symantec System Center console, right-click a server, and then click **All Tasks** > **Symantec AntiVirus** > **Virus Definition Manager**.

2 In the Virus Definition Manager dialog box, click **Update the Primary Server of this Server Group only**.

3 Click **Configure**.

4 In the Configure Primary Server Updates dialog box, click **Source**.

5 In the Setup Connection dialog box, in the Update definition file via list, click **Another Protected Server**, and then click **Configure**, if necessary.

6 In the Configure Update From Server dialog box, select the master primary server from the list of servers that appears.

7 Click **OK**.

8 Click **OK**.

9 In the Configure Primary Server Updates dialog box, do one of the following:

- Click **Update Now** to retrieve the virus definitions files from the master primary server immediately.
- Click **Schedule For Automatic Updates**, and then click **Schedule** and set a frequency and time when the server will check for updates on the master primary server to schedule automatic updates.

10 Click **OK** until you return to the Symantec System Center main window.

Updating NetWare servers using the Virus Definition Transport Method

Updating a NetWare server is similar to updating other types of servers with the following differences:

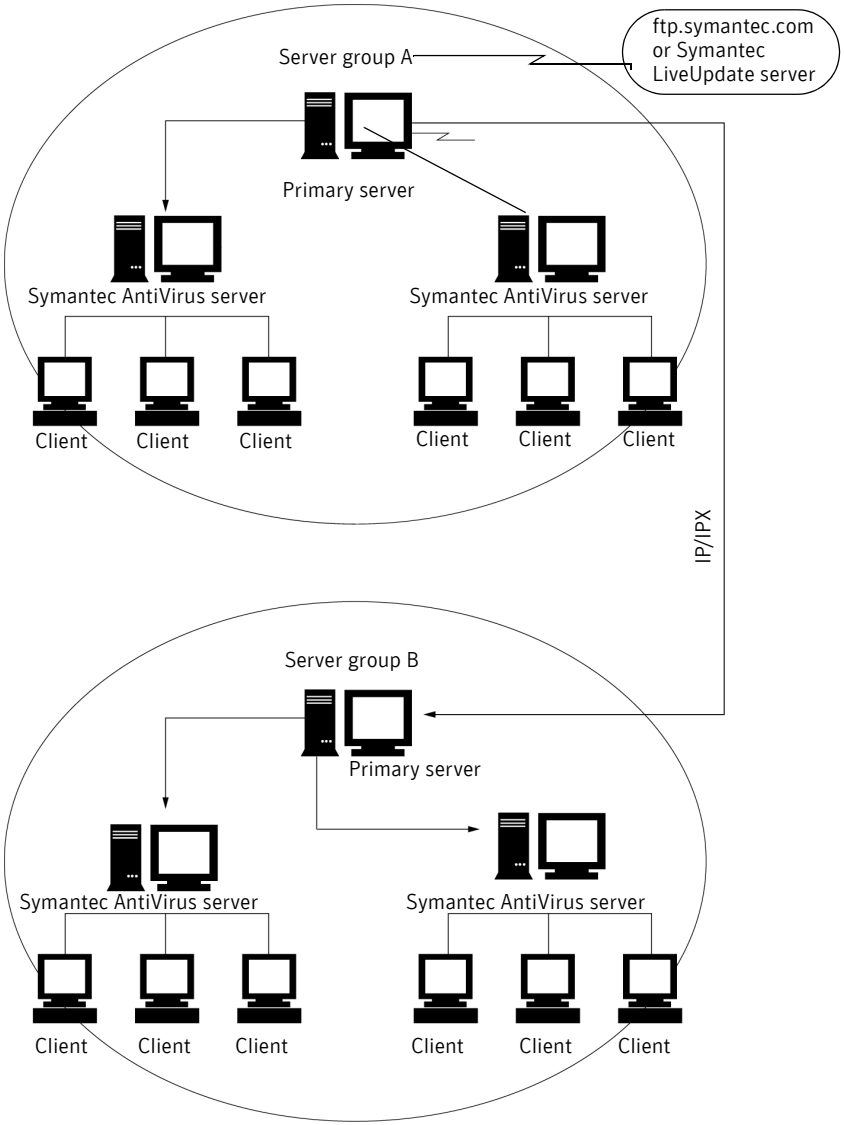
- You can designate a NetWare server as the primary server for your network, or designate a Windows NT/2000 computer as the primary server. If your NetWare servers are running on faster computers or have a higher bandwidth connection than your Windows NT/2000 servers, you can designate a NetWare server as a primary server for increased performance.
- NetWare primary servers must have TCP/IP and FTP running (FTP is not enabled by default on NetWare servers), and must be able to connect to the Internet. In addition, NetWare environments require a Windows NT/2000 computer to run the Symantec System Center console.
- NetWare servers do not store the addresses of Windows NT/2000 servers in their address caches. As a result, if your NetWare server is not running TCP/IP and is not using a domain naming system (DNS) server, you might have difficulty updating a NetWare server from a Windows NT/2000 server that resides in a different server group.

To update NetWare servers without TCP/IP

- Temporarily move the NetWare server into a server group that has a Windows NT server that is running the IPX protocol.
  After one day, you can move the NetWare server back to its original server group. This adds the Windows NT/2000 server address to the NetWare server's address cache, which lets the NetWare server locate the Windows NT/2000 server to obtain the updated virus definitions file.

Figure 4-1 shows you one way you could configure virus definitions files updates for your computer if you have a small network of six file servers divided into two server groups.

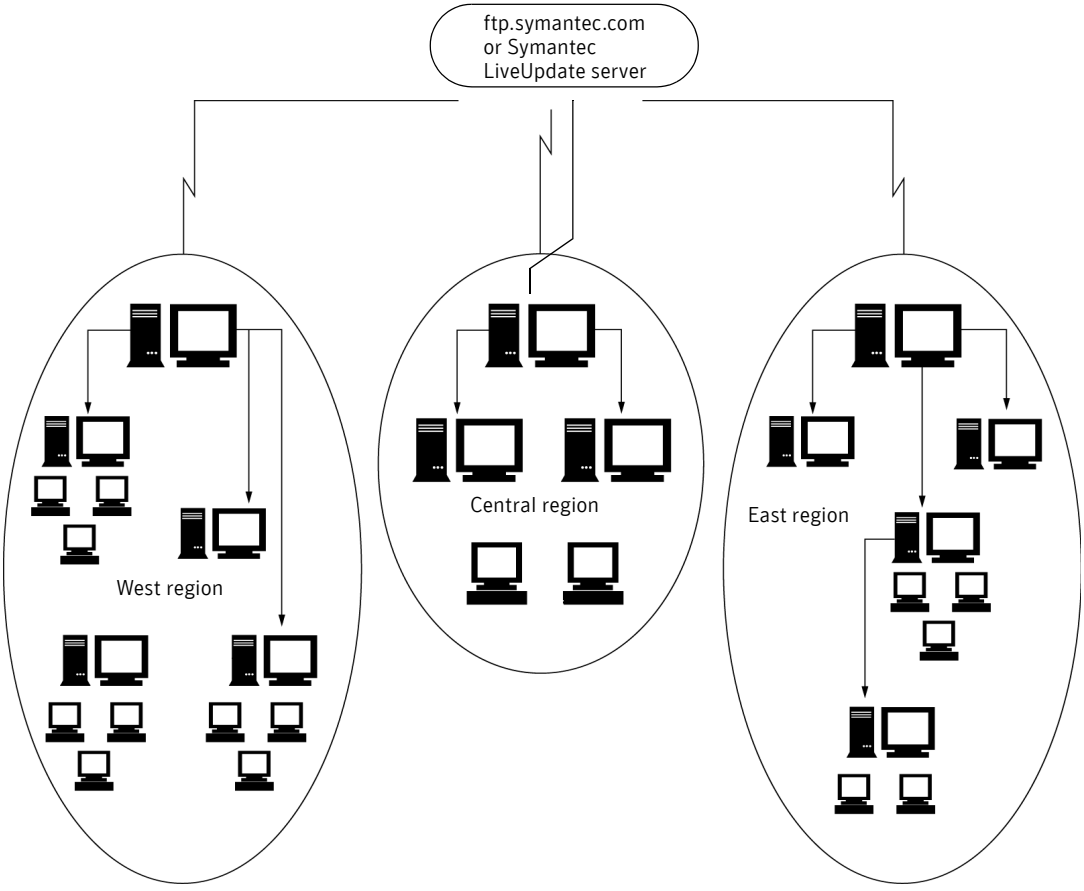
Figure 4-1 Virus definitions file updating using the Virus Definition Transport Method



Configure a primary server to retrieve the latest virus definitions files updates; you can download through FTP or another computer. Enable virus definitions file sharing so that Symantec AntiVirus servers in server group A automatically retrieve the latest updates from primary server 1. Clients automatically receive the updates from their parent servers. Configure primary server 2 to retrieve the latest update from primary server 1. This makes primary server 1 a master primary server. Symantec AntiVirus servers in server group B receive updates from their primary server. Clients automatically receive updates from their Symantec AntiVirus servers.

Figure 4-2 illustrates how you might configure virus definitions files updates if your organization has multiple sites that are linked over a wide area network (WAN).

Figure 4-2 Virus definitions file updating for multiple sites over a WAN



Server group primary servers on separate WANs retrieve the update from the Symantec FTP site or LiveUpdate server. Primary servers distribute the update to primary servers in other server groups in their local networks. The primary servers distribute the update to other protected servers and clients in their server group.

Updating servers using LiveUpdate

Depending on the size of your network, you can use LiveUpdate to update virus definitions files in the following ways:

- For smaller networks (less than 1000 nodes), configure managed servers to directly retrieve updates from the Symantec FTP site, Symantec LiveUpdate server, or an internal LiveUpdate server.
- For larger networks (greater than 1000 nodes), set up an internal LiveUpdate server, download updates to that server, and have your managed servers retrieve updates from the internal LiveUpdate server.

Updating Symantec AntiVirus servers from the Symantec FTP site or LiveUpdate server

You need to configure updating for the primary server in each server group to ensure that its virus definitions files are current. You can also configure individual servers to update directly from Symantec.

Update Symantec AntiVirus servers directly from the Symantec FTP site or LiveUpdate server

You can update all of the Symantec AntiVirus servers in a server group from a primary server, or update each server in the group individually.

To update primary servers

1. In the Symantec System Center console, right-click a server group, and then click **All Tasks** > **Symantec AntiVirus** > **Virus Definition Manager**.
2. In the Virus Definition Manager dialog box, click **Update The Primary Server Of This Server Group Only**.
3. Click **Configure**.
4. In the Configure Primary Server Updates dialog box, do one of the following:
   - Click **Update Now** to launch a LiveUpdate session immediately.
   - Click **Schedule For Automatic Updates**, and then click **Schedule** to set a frequency and time when the server will run a LiveUpdate session.
5. Click **OK**.
6. In the Configure Primary Server Updates dialog box, click **Source**.
7. In the Update definition file via list, click **LiveUpdate**.
8. Click **OK** until you return to the Symantec System Center main window.

To update individual servers from the Symantec FTP site or LiveUpdate server

1. In the Symantec System Center console, right-click a server group, and then click **All Tasks** > **Symantec AntiVirus** > **Virus Definition Manager**.
2. In the Virus Definition Manager dialog box, click **Update Each Server In This Server Group Individually**.
3. Click **Configure**.
4. In the Configure Primary Server Updates dialog box, click **Source**.
5. Click **LiveUpdate (Win32)/FTP (NetWare)**.
6. Click **OK**.
   If you are configuring a NetWare server, make sure that the server is running FTP.
7. Do one of the following:
   - Click **Update Now** to launch a LiveUpdate session immediately.
   - Click **Schedule For Automatic Updates**, and then click **Schedule** to set a frequency and time when the server will run a LiveUpdate session.
8. Click **OK** until you return to the Symantec System Center main window.

Updating servers from an internal LiveUpdate server

You can set up an internal LiveUpdate server on any computer. If you use a Symantec AntiVirus server as an internal LiveUpdate server, you can use the standard update methods that are available in the Virus Definition Manager dialog box to manually and automatically update the virus definitions files on that server. If you use a computer that does not run Symantec AntiVirus as an internal LiveUpdate server, use the LiveUpdate Administration Utility to update the virus definitions on that server.

See "Updating servers using LiveUpdate" on page 154.

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

To update servers from an internal LiveUpdate server

1. In the Symantec System Center console, right-click a server group, and then click **All Tasks** > **LiveUpdate** > **Configure**.
2. In the Configure LiveUpdate dialog box, click **Internal LiveUpdate Server**.

3 Set the following internal LiveUpdate server options:

Name	The name of the server. This name will appear when you run LiveUpdate.
Location	This box is optional. You can type descriptive information that is related to the server (for example, the name of the site).
Login Name	The logon name that is associated with the server. Leave this box blank so that users can log on and retrieve the files without typing information.
Login Password	The logon password that is associated with the server. Leave this box blank so that users can log on and retrieve the files without typing information.
URL or IP Address	■ If you are using the FTP method (recommended), under Type, you can click FTP, and then type the FTP address for the server. For example: ftp.myliveupdateserver.com ■ If you are using the HTTP method, under Type, you can click HTTP, and then type the URL for the server. For example: http:\\myliveupdateserver.com or 155.66.133.11\Export\Home\Ludepot ■ If you are using the LAN method, under Type, you can click LAN, and then type the server UNC path name. For example: \\Myserver\LUDepot In the Login box, type the name and password to access the server.

If you leave the Login Name and Login Password boxes empty, an anonymous logon will be used. This requires that anonymous logons be enabled on the FTP server. If your policy prohibits anonymous logons on FTP servers, type the logon name and password for the FTP server and directory that will be accessed.

4 Click **OK** until you return to the Symantec System Center main window.

Specifying multiple internal LiveUpdate servers for failover support

To compensate for unavailable internal LiveUpdate servers, Symantec AntiVirus supports multiple internal LiveUpdate servers.

Updating servers with Intelligent Updater

To distribute updated virus definitions, download a new Intelligent Updater, and then use your preferred distribution method to deliver the updates to your managed servers and clients. Intelligent Updater is available as a single file or as a split package, which is distributed across several smaller files. The single file is for computers with network connections. The split package can be copied to floppy disks and used to update computers that do not have network connections or Internet access.

Update servers with Intelligent Updater files

Download Intelligent Updater from the Symantec Web site, and then install Intelligent Updater to servers with the latest virus definitions files.

Note: Make sure to use Intelligent Updater files for Symantec AntiVirus rather than the consumer version of the product.

To download Intelligent Updater

1. Using your Web browser, go to:
   http://securityresponse.symantec.com
2. Click **Download Virus Definitions**.
3. Click **Download Updates (Intelligent Updater Only)**.
4. Select the appropriate language and product.
5. Click **Download Updates**.
6. Click the file with the .exe extension.
7. When you are prompted for a location in which to save the files, select a folder on your hard drive.

To install the virus definitions files

1. Locate the Intelligent Updater file that you downloaded from Symantec.
2. Double-click the file and follow the on-screen instructions.

Updating servers using Central Quarantine polling

If you use Symantec Central Quarantine, you can configure the Central Quarantine Server to periodically poll the Digital Immune System gateway for new virus definitions files. When new definitions are available, the Central Quarantine Server can automatically push the new definitions to the computers that need it, using the Virus Definition Update Method.

For more information, see the *Symantec Central Quarantine Administrator's Guide*.

Minimizing network traffic and handling missed updates

LiveUpdate provides advanced scheduling options for minimizing network traffic and handling missed updates. Table 4-2 describes LiveUpdate scheduling options.

Table 4-2 LiveUpdate scheduling options

Option	Description	When to use
Randomization options	Randomizes updates: ■ Plus or minus a specified number of minutes of the scheduled time ■ Any day of the week within a specified time interval ■ Any day of the month plus or minus a specified number of days of the scheduled date	When you want to stagger updates for multiple computers to minimize the impact on network traffic. By default, Symantec AntiVirus randomizes LiveUpdate sessions to minimize bandwidth spikes.
Missed Event options	Determines how missed LiveUpdate events will be handled. An event might be missed if a computer is turned off when the LiveUpdate session is scheduled to run. You can set options so that scheduled LiveUpdate events that were missed run at a later time.	To ensure that computers that are unavailable for a regularly scheduled LiveUpdate event will attempt to pull definitions at a later time.

Minimize network traffic and handle missed updates

You can set separate randomization schedules for Symantec AntiVirus servers and clients on your network to minimize the impact on network traffic.

You can specify separate policies for handling missed LiveUpdate events for Symantec AntiVirus servers and clients.

To randomize the LiveUpdate schedule for servers

1. In the Symantec System Center console, right-click a server or server group, and then click **All Tasks** > **Symantec AntiVirus** > **Virus Definition Manager**.
2. In the Virus Definition Manager dialog box, click **Configure**.
3. In the Configure Primary Server Updates dialog box, check **Schedule For Automatic Updates**.
4. Click **Schedule**.
5. Set the frequency and time when the server will check for updates.
6. In the Virus Definition Update Schedule dialog box, click **Advanced**.
7. In the Advanced Scheduled Options dialog box, under Randomization Options, check **Options**, and then set the minutes, day of the week, or day of the month options.
8. Click **OK** until you return to the Symantec System Center main window.

To randomize the LiveUpdate schedule for clients

1. In the Symantec System Center console, right-click a server or server group, and then click **All Tasks** > **Symantec AntiVirus** > **Virus Definition Manager**.
2. In the Virus Definition Manager dialog box, check **Schedule Client For Automatic Virus Definition Updates Using LiveUpdate**.
3. In the Virus Definition Update Schedule dialog box, click **Schedule**.
4. Set the frequency and time when the clients will check for updates.
5. Click **Advanced**.
6. In the Advanced Schedule Options dialog box, under Randomization Options, check **Options**, and then set the minutes, day of the week, or day of the month options.
7. Click **OK** until you return to the Symantec System Center main window.

To handle missed LiveUpdate events for servers

1. In the Symantec System Center console, right-click a server or server group, and then click **All Tasks** > **Symantec AntiVirus** > **Virus Definition Manager**.
2. In the Virus Definition Manager dialog box, click **Configure**.
3. Click **Schedule for Automatic Updates**.
4. In the Configure Primary Server Updates dialog box, click **Schedule**.

5 In the Virus Definition Update Schedule dialog box, click **Advanced**.

6 In the Advanced Schedule Options dialog box, check **Handle Missed Events Within**.

7 Set the time limit within which you want the scan to run.
For example, you might want a weekly LiveUpdate event to run only if it is within three days after the scheduled time for the missed event.

8 Click **OK** until you return to the Symantec System Center main window.

To handle missed LiveUpdate events for clients

1 In the Symantec System Center console, right-click a server or server group, and then click **All Tasks** > **Symantec AntiVirus** > **Virus Definition Manager**.

2 In the Virus Definition Manager dialog box, click **Schedule Client For Automatic Virus Definition Updates Using LiveUpdate**.

3 Click **Schedule**.

4 In the Virus Definition Update Schedule dialog box, click **Advanced**.

5 Check **Handle Missed Events Within**.

6 Set the time limit within which you want the scan to run.
For example, you may want a weekly LiveUpdate event to run only if it is within three days after the scheduled time for the missed event.

7 Click **OK** until you return to the Symantec System Center main window.

Updating virus definitions files on Symantec AntiVirus clients

You can update the virus definitions files on Symantec AntiVirus clients using any of the following:

- Virus Definition Transport Method
- LiveUpdate
- Intelligent Updater
  See "Specifying multiple internal LiveUpdate servers for failover support" on page 156.
- Central Quarantine polling
  See "Updating servers using Central Quarantine polling" on page 157.

See "Virus definitions files update methods" on page 146.

Update virus definitions files on Symantec AntiVirus clients

You can update Symantec AntiVirus clients using the Virus Definition Transport Method, LiveUpdate, or both.

Note: LiveUpdate is the only method for updating virus definitions files that is supported on 64-bit computers.

To update clients using the Virus Definition Transport Method

1. In the Symantec System Center console, right-click a server group, and then click **All Tasks** > **Symantec AntiVirus** > **Virus Definition Manager**.
2. In the Virus Definition Manager dialog box, check **Update Virus Definitions From Parent Server**.
3. Click **Settings**.
4. In the Update Settings dialog box, set the frequency with which the parent server will push updates.
5. Click **OK**.
6. In the Virus Definition Manager dialog box, uncheck **Schedule Client for Automatic Updates using LiveUpdate**.
7. Click **OK** until you return to the Symantec System Center main window.

To update clients using LiveUpdate

1. In the Symantec System Center console, right-click a server group, and then click **All Tasks** > **Symantec AntiVirus** > **Virus Definition Manager**.
2. In the Virus Definition Manager dialog box, check **Schedule Client For Automatic Updates Using LiveUpdate**.
3. Click **Schedule**.
4. In the Virus Definition Update Schedule dialog box, select the frequency, day, and time that you want the update to occur.
5. Click **OK** until you return to the Symantec System Center main window.

To update clients using both the Virus Definition Transport Method and LiveUpdate

1. In the Symantec System Center console, right-click a server group, and then click **All Tasks** > **Symantec AntiVirus** > **Virus Definition Manager**.
2. In the Virus Definition Manager dialog box, check **Update Virus Definitions from Parent Server**.

3 Check **Schedule Client For Automatic Updates Using LiveUpdate**.

4 Click **Schedule**.

5 In the Virus Definition Update Schedule dialog box, select the frequency, day, and time that you want the update to occur.

6 Click **OK**.

7 Click **Settings**.

8 In the Update Settings dialog box, set the frequency with which the parent server will push updates.

9 Click **OK** until you return to the Symantec System Center main window.

Updating virus definitions files on Symantec AntiVirus clients immediately

You can force clients to update virus definitions files immediately using LiveUpdate. This feature is available for clients that normally receive updates using LiveUpdate or the Virus Definition Transport Method.

This feature provides a good way to update virus definitions files when one or more clients on which LiveUpdate is installed are using outdated files for some reason (for example, when an update operation that was performed at the server group level succeeded on all but several clients).

Warning: Updating a large number of clients immediately can result in slow performance. Once you start this operation, you cannot cancel it. Do not use this feature to update virus definitions files during a virus outbreak.
See "Handling a virus outbreak on your network" on page 175.

Update virus definitions files on Symantec AntiVirus clients immediately

Before you can update virus definitions files, you must specify the number of clients to update. When the number of selected clients exceeds this number, a confirmation dialog box appears to verify that you want to exceed the administrator-specified number.

To specify the number of clients to update immediately

1. In the Symantec System Center console, on the Tools menu, click **SSC Options**.
2. In the SSC Properties window, on the Client Filter tab, select the number of multi-selected clients to update before a confirmation dialog box appears.
3. Click **OK**.

To update one or more clients immediately with LiveUpdate

1. In the Symantec System Center console, right-click one or more clients in the right pane, and then click **All Tasks** > **Symantec AntiVirus** > **Update Virus Defs Now**.
2. If you selected more than the administrator-specified number of clients, in the confirmation dialog box, select one of the following:
   - Yes
   - Cancel

   If a client is configured to update using the Virus Definition Transport Method, Symantec AntiVirus prompts you to allow LiveUpdate to run.
3. Click **OK** in the status dialog box.

Configuring managed clients to use an internal LiveUpdate server

You can configure LiveUpdate settings for managed computers running Symantec AntiVirus client from the Symantec System Center. For unmanaged Symantec AntiVirus clients, use the LiveUpdate Administration Utility to create a custom .hst file.

For information on configuring LiveUpdate for unmanaged Symantec AntiVirus clients, see the *LiveUpdate Administrator's Guide*.

To configure a managed Symantec AntiVirus client to use an internal LiveUpdate server

1. Right-click a parent server, and then click **All Tasks** > **LiveUpdate** > **Configure**.
2. In the Configure LiveUpdate dialog box, click **Internal LiveUpdate Server**.
3. If you are using an FTP or HTTP server, type the appropriate data in the Login Name and Password boxes.
4. In the Connection box, type one of the following:
   - The UNC path to your shared folder
   - The URL or IP address for your FTP or HTTP server

5 In the Type list, select one of the following:
   - LAN
   - FTP
   - HTTP
6 Click **OK** until you return to the Symantec System Center main window.
   If you are using multiple parent servers, repeat steps 1–6 for each parent server so that all Symantec AntiVirus clients and servers receive the changes. You can also configure LiveUpdate for an entire group by right-clicking the server group.

Enabling and configuring Continuous LiveUpdate for managed clients

If a managed Symantec AntiVirus client infrequently connects to its parent server (for example, a notebook computer that is used offsite), it may not receive the most current virus definitions files updates. For these computers, Continuous LiveUpdate offers a backup option for receiving updates directly from Symantec whenever the computer connects to the Internet.

With Continuous LiveUpdate, you can specify a maximum number of days that the virus definitions files on a Symantec AntiVirus computer can be out-of-date before an update is forced. When the Symantec AntiVirus client determines that its virus definitions files exceed their maximum age, it initiates a silent (no user interaction required) LiveUpdate session when it connects to the Internet.

Enable and configure Continuous LiveUpdate

You can enable Continuous LiveUpdate using the Symantec System Center, or by changing registry values on Symantec AntiVirus clients. You can then configure Continuous LiveUpdate options by adding values to the client's registry.

To enable Continuous LiveUpdate using the Symantec System Center

1 In the Symantec System Center console, right click a server group, a Symantec AntiVirus server, a client group, or an individual Symantec AntiVirus client, and then click **All Tasks** > **Symantec AntiVirus** > **Virus Definition Manager**.
2 In the Virus Definition Manager dialog box, check **Enable Continuous LiveUpdate**.
3 Click **OK** until you return to the Symantec System Center main window.

To enable Continuous LiveUpdate by changing registry values

1. Using Regedit, navigate to: HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\PatternManager
2. Add EnableAdminForcedLU as a new DWORD.
3. Set the value of the DWORD to one of the following values:
   - 1: Enable
   - 0: Disable

To configure Continuous LiveUpdate

◆ Configure Continuous LiveUpdate using the following registry values:

EnableAdminForcedLU	Set to 0 to disable Continuous LiveUpdate or set to 1 to enable it.
MaxDefsDaysOldAllowed	Specify the age (in days) that the definition can be before Symantec AntiVirus executes a silent LiveUpdate.
AdminForcedLUCheckInterval	Specify the interval (in minutes) to check for old definitions.
AFLUDelay	Set the startup delay time (between 10 and 180 minutes) of the Continuous LiveUpdate feature. This delay time is only valid if the feature is enabled. The actual delay time is a random number between 8 and N+8 where N is the value in the registry key. The default value is 30 minutes.

Note: You should set the MaxDefsDaysOldAllowed value to 8 days or higher. Lower settings may cause problems if you need to perform a virus definitions files rollback, since the age of the definitions files that you want to roll back to may exceed the maximum number of days that Continuous LiveUpdate will allow before forcing an update.

Setting LiveUpdate usage policies

You can set LiveUpdate usage policies for managed clients. When these policies are enabled, they are dimmed on the client. The policies determine whether the following activities can be performed at the client level:

- Change the LiveUpdate schedule.
- Manually launch LiveUpdate.

To set LiveUpdate usage policies

1. In the Symantec System Center console, right-click a server or server group, and then click **All Tasks** > **Symantec AntiVirus** > **Virus Definition Manager**.
2. In the Virus Definition Manager dialog box, do one of the following:
   - Check **Do Not Allow Client To Modify LiveUpdate Schedule** to prevent the LiveUpdate schedule from being modified on the client. (Schedule Client For Automatic Updates Using LiveUpdate must be checked or this box is dimmed.)
   - Uncheck **Download Product Updates Using LiveUpdate** to prevent application updates.
   - Uncheck **Do Not Allow Client To Manually Launch LiveUpdate** to prevent LiveUpdate from being manually launched on the client.

Note: When Do Not Allow Client To Modify LiveUpdate Schedule or Do Not Allow Client To Manually Launch LiveUpdate is unchecked, LiveUpdate can run on the client at any time.

Controlling virus definitions files

The Symantec System Center console provides a set of tools for controlling the deployment of virus definitions files on your network. Use these tools to do the following:

- Verify the dates of virus definitions files on servers.
- View the virus lists on servers and clients.
- Roll back to a previous virus definitions file (network-wide).

If new virus definitions files are causing false positives or other problems for a server, you can verify the version number of the virus definitions files on that computer and then deploy an earlier definitions set from the Symantec System Center console. All servers and clients in that server group will roll back to the specified virus definitions files. You can also control the version of the virus definitions files used on all servers and clients in a server group. Users who download a virus definitions file that was not approved for company use can be forced to use the virus definitions file that you specify. Because you can easily

undo a virus definitions file rollout, you can release new virus definitions files in less time.

The Symantec System Center displays a warning icon if a virus definitions file is out-of-date on one or more computers that are managed by a parent server, server group, or client group.

To find a computer with outdated definitions

- Expand the server, server group, or client group and look for more warning icons.

Verifying the version number of virus definitions files

Using the Symantec System Center console, you can view the version number of the virus definitions files at the Symantec AntiVirus server, server group, client group, and individual Symantec AntiVirus client level.

To verify the version number of the virus definitions files

- In the Symantec System Center console, right-click a server group, client group, Symantec AntiVirus server, or client, and then click **Properties**.
  On the Symantec AntiVirus tab, in the Virus Definitions box, the file version is listed as a numerical date, followed by a version number.
  Once virus definitions files are updated on a computer, it may take several minutes before the information is available from the console.

Viewing the threat list

You can view a list of viruses and other threats, such as adware and spyware, that are detectable on a selected server or client. The threat list ensures that the selected computer is protected from a specific virus.

To view the threat list

1. In the Symantec System Center console, right-click a server or client, and then click **All Tasks** > **Symantec AntiVirus** > **View Threat List**.
2. Click **Close**.

Rolling back virus definitions files

You can roll back a virus definitions file for a server group. For example, if the most recent file generated false positive virus detections you might want to roll back to a previous file.

Note: When you roll back virus definitions files, virus definitions that are newer than those in the rolled back version are deleted.

To roll back virus definitions files

1. In the Symantec System Center console, right-click a server or server group, and then click **All Tasks** > **Symantec AntiVirus** > **Virus Definition Manager**.
2. In the Virus Definition Manager dialog box, ensure that Update The Primary Server Of This Server Group Only is selected, and then click **Configure**.
3. In the Configure Primary Server Updates dialog box, click **Definition File**.
4. In the Select Virus Definition File dialog box, select the virus definitions file that you want to roll back to, and then click **Apply**.
5. Click **Yes** to change the current file.
6. Click **OK** until you return to the Symantec System Center main window.

Testing virus definitions files

Many administrators prefer to test virus definitions files on a test network before making them available on a production server. To test virus definitions files, complete the following tasks:

- Install Symantec AntiVirus server to a primary server on the test network.
- From the primary server on your test network, run LiveUpdate to download the virus definitions file.
- Go to www.eicar.org and download the antivirus test file to test the operation of the virus definitions file.
- Once testing is complete, copy the virus definitions file from the \Program files\Sav folder on the test server to a folder with the same name on the primary servers on your production network.
- Once the virus definitions files are on the primary servers, they will flow to other servers in the server group.

Note: Clients are configured to automatically retrieve virus definitions from their parent servers if Update Virus Definitions From Parent Server in the Virus Definition Manager dialog box is checked.

Update scenarios

The following scenarios show how administrators at two different companies perform updates:

- At Company A, the administrator downloads the new virus definitions file from the Symantec FTP site or Symantec LiveUpdate server to a primary server on the test network. He tests the virus definitions file. When testing is completed, he copies the virus definitions file to the master primary server on his production network. He has configured other primary servers so that they retrieve the update from the master primary server. All of the other connected computers use the Virus Definition Transport Method. Secondary servers retrieve the update from their primary server. Clients retrieve the update from their parent server.
- At Company B, the administrator downloads the new virus definitions file from the Symantec FTP site or Symantec LiveUpdate server to a test network. She tests the virus definitions file. When testing is completed, she downloads the new virus definitions file from the Symantec FTP site or Symantec LiveUpdate server to the internal LiveUpdate server on her production network. Some low risk users are allowed to go outside of the firewall. When LiveUpdate runs on their computers, virus definitions files are downloaded directly from the Symantec FTP site or Symantec LiveUpdate server.

About scanning after updating virus definitions files

If Auto-Protect is enabled, Symantec AntiVirus begins scanning with the updated virus definitions files immediately.

Once virus definitions files are updated, Symantec AntiVirus offers to attempt to repair files that are stored in Quarantine.

You can run a manual scan or schedule a scan to check for expanded threats, such as adware and spyware.

See “Scanning for viruses and other threats” on page 89.

Chapter 5

Responding to virus outbreaks

This chapter includes the following topics:

- About responding to virus outbreaks
- Preparing for a virus outbreak
- Handling a virus outbreak on your network

About responding to virus outbreaks

Responding to virus outbreaks requires preparing before an outbreak occurs, and having a strategy in place for handling an outbreak should one occur.

In addition to installing Symantec AntiVirus on the servers and workstations in your network, preparing for a virus outbreak consists of the following tasks:

- Creating and reviewing a virus outbreak plan.
- Defining Symantec AntiVirus actions for handling viruses.
- A strategy for handling virus outbreaks includes the following:
  - Enable virus alerts and messages.
  - Run a virus sweep of your network.

- Track viruses using logs.
- Use the Central Quarantine Console to track infected computers on your network, and submit suspicious file samples to Symantec Security Response for analysis and cure.

Preparing for a virus outbreak

To prepare for a virus outbreak, you should create a virus outbreak plan and define actions for handling suspicious files.

Creating a virus outbreak plan

An effective response to a virus outbreak on your network requires a plan that allows you to respond quickly and efficiently.

Table 5-1 outlines the tasks for creating a virus outbreak plan.

Table 5-1 A model virus outbreak plan

Task	Description
Ensure that virus definitions files are current.	Verify that infected computers have the latest virus definitions files, and use the Virus Definition Transport Method to push new definitions if needed. See "About virus definitions files" on page 145.
Map your network topology.	Prepare a network topology map so that you can systematically isolate and clean computers by segment before you reconnect them to your local network. Your map should contain the following information: ■ Server names and addresses ■ Client names and addresses ■ Network protocols ■ Shared resources
Identify the virus.	Symantec AntiVirus logs are a good source of information about viruses on your network. If you can identify a virus from the logs, you can use the Symantec Security Response Virus Encyclopedia to learn how to remove the virus.

Table 5-1 A model virus outbreak plan

Task	Description
Respond to unknown viruses.	If you cannot identify a suspicious file as a virus by examining the logs, and the latest virus definitions files do not clean the file, go to http://securityresponse.symantec.com and look at the Latest Virus Threats and Security Advisories areas for news.
Understand security solutions.	In addition to understanding your network topology, you need to understand your implementation of Symantec AntiVirus as well as the implementation of any other security products that are used on your network. Consider the following questions: ■ What security programs are protecting network servers and workstations? ■ What is the schedule for updating virus definitions? ■ What alternative methods of obtaining updates are available if the normal channels are under attack? ■ What log files are available for tracking viruses on your network?
Have a backup plan.	In the event of a catastrophic virus infection, you may need to restore servers and clients to be sure that your network has not been compromised. Having a backup plan in place to restore critical computers is essential.

Defining Symantec AntiVirus actions for handling suspicious files

By default, Symantec AntiVirus performs the following actions when it identifies a suspicious file:

- Symantec AntiVirus attempts to repair the file.
- If the file cannot be repaired with the current set of virus definitions files, the infected file is moved to the Quarantine on the local computer. In addition, the Symantec AntiVirus client makes a log entry of the threat event in its log. The Symantec AntiVirus client data is forwarded to a primary server. You can view log data from the Symantec System Center console.

You can perform the following additional actions to complete your virus handling strategy:

- Define different repair actions based on virus type. For example, you can have Symantec AntiVirus automatically fix macro viruses, but ask what action to take when a program file virus is detected.
- Assign a backup action for files that Symantec AntiVirus cannot repair, such as deleting the infected file.
- Receive virus alerts, such as a page or email message, if you are using AMS^2.
- Configure the local Quarantine to forward infected files to the Central Quarantine. You can configure the Central Quarantine to attempt a repair based on its set of virus definitions files (which may be more up-to-date than the definitions on the local computer), or automatically forward samples of infected files to Symantec Security Response for analysis.

See "About the Alert Management System" on page 61.

For more information, see the *Symantec Central Quarantine Administrator's Guide*.

Automatically purging suspicious files from local Quarantines

When Symantec AntiVirus scans a suspicious file, it places the file in the local Quarantine folder on the affected computer. The Quarantine purge feature automatically deletes files in the Quarantine that exceed a specified age.

Registry settings for Quarantine purge are located in this registry key:

\\HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\Quarantine

Table 5-2 lists the possible Quarantine purge settings.

Table 5-2 Quarantine purge settings

Value	Settings	Description
QuarantinePurgeEnabled	0/1	Disables/enables purge
QuarantinePurgeAgeLimit	X	Specifies the maximum number of days to keep a file in the Quarantine directory
QuarantinePurgeFrequency	X	Sets the frequency value for purging: 0=Days, 1=Months, 2=Years
BackupItemPurgeEnabled	0/1	Disables/enables purging backup files
BackupItemPurgeAgeLimit	X	Specifies the maximum number of days to keep a backup file in Quarantine
BackupItemPurgeFrequency	X	Sets the frequency value for purging backup files: 0=Days, 1=Months, 2=Years
RepairedItemPurgeEnabled	0/1	Disables/enables purging repaired files
RepairedItemPurgeFrequency	X	Sets the frequency value for purging repaired files: 0=Days, 1=Months, 2=Years

Handling a virus outbreak on your network

Symantec AntiVirus provides the following tools for handling a virus outbreak on your network:

- Alerts: Sends AMS[2] and built-in alerts
- Virus sweep: Forces a virus scan at the system hierarchy, server group, or individual server level
- Event Logs and Histories: Track viruses and Central Quarantine submissions at the server group, individual server, or client level
- Central Quarantine Console: Tracks submissions to Symantec Security Response
- Emergency Disk: Cleans boot sector viruses

Using virus alerts and messages

You can use alerts and messages to learn about suspicious files that Symantec AntiVirus discovers on your network. Symantec AntiVirus offers the following notification mechanisms:

- AMS^2: If configured, Symantec AntiVirus clients can send threat events to an AMS^2 server. You can configure AMS^2 servers to send alerts to a pager, email address, and other notification mechanisms.
  See "About the Alert Management System" on page 61.
- Custom messages: From the Symantec System Center console, you can have a custom message appear on Symantec AntiVirus clients when they encounter a suspicious file.
  See "Displaying and customizing a warning message on an infected computer" on page 128.

Running a virus sweep

If you discover several suspicious files, you might not know if the problem is on the computer or server on which the suspicious files were detected, or if the problem has spread to other areas of the network. You might want to begin a virus sweep using the Symantec System Center. The number of computers that you scan depends on how you start the sweep.

If a Symantec AntiVirus client is not accessible during a virus sweep, Symantec AntiVirus will do one of the following:

- On 32-bit operating systems: Scan the computer as soon as it is turned on. The computer does not have to log on to the network.
- On 16-bit operating systems: Scan the computer as soon as it is turned on and logged on to the network.

Depending on the object that you select in the Symantec System Center console, you can run a virus sweep on your entire network, a server group, or an individual server.

Warning: A virus sweep can create considerable network traffic, the amount and duration of which depend on the size of your network. Once you start a virus sweep it must complete; you cannot stop it.

To run a virus sweep

1. In the Symantec System Center console, right-click the network, a server group, or a server, and then click **All Tasks** > **Symantec AntiVirus** > **Start Virus Sweep**.
2. In the Name box, type a name for the sweep.
3. Click **Start**.
   See "Configuring scan options" on page 123.

Tracking virus alerts using Event Logs and Histories

You can track Threat Found alerts from the Symantec System Center console. By default, Threat Found alerts appear for three days. You can change the number of days for which Threat Found alerts appear.

See "About Histories and Event Logs" on page 193.

Tracking submissions to Symantec Security Response with Central Quarantine Console

The Symantec System Center logs an event when a Symantec AntiVirus client submits a suspicious file to Symantec Security Response. In addition to the logged event, you can track the Auto-Protect status of submissions to Symantec Security Response from the Central Quarantine Console.

For information on using the Central Quarantine Console, see the *Symantec Central Quarantine Administrator's Guide*.

Chapter 6

Managing roaming clients

This chapter includes the following topics:

- About roaming clients
- Roaming client components
- How roaming works
- Implementing roaming
- Command-line options
- Registry values

About roaming clients

A roaming client can do the following:

- Automatically identify its best parent server, based on speed and proximity, and become a managed client of that parent server. For example, when a mobile user who is based in New York travels to California, the roaming client detects the new network address and reassigns the user's laptop to the best parent server.
- Connect to the nearest appropriate parent server whenever its network address changes.
- Connect to a different parent server if the current parent server becomes unavailable.
- Periodically recheck for the nearest parent server to adjust for changes in servers and server load.

- Attempt to balance the load among a pool of equivalent servers when selecting a parent server.
- Automatically identify the best parent server when the client connects to the network (for unmanaged clients that are converted to managed clients). For example, a corporation may have a distribution center for new computers. Administrators enable roaming on the computers before they are sent to branch offices. This entails specifying all of the possible roam servers for the new computers. When end users connect the new computers to the network, Symantec AntiVirus automatically assigns the best parent server.

Roaming client components

Table 6-1 lists roaming client components.

Table 6-1 Roaming client components

Component	Description
List of 0 level servers	Lists the 0 level of servers that are available as possible roam servers for a specific roaming client. Roaming clients store this data in their registries. See "Analyzing and mapping your Symantec AntiVirus network" on page 182. See "Creating a list of 0 level Symantec AntiVirus servers" on page 183.
Hierarchical list of servers	Lists all roam servers, grouped by hierarchical level. Roaming servers store this data in their registries. See "Analyzing and mapping your Symantec AntiVirus network" on page 182. See "Creating a hierarchical list of Symantec AntiVirus servers" on page 184.
Roamadmn.exe	Sets up Symantec AntiVirus servers for roaming access. See "Configuring additional roaming client support for roam servers" on page 187.
SavRoam.exe	Provides roam server data to roaming clients. See "Configuring roaming client support options from the Symantec System Center console" on page 184.

How roaming works

Roaming client support employs the following types of lists:

- One or more lists of 0 level servers
- A hierarchical list of the servers that you want to support roaming clients

Roaming clients store the 0 level list in their registries, and use it to identify the servers to which they should attempt to connect. To implement roaming on your network, start by preparing one or more lists of 0 level servers, and the hierarchical list of servers.

After you roll out this data, roaming clients work in the following manner:

- SavRoam.exe launches on the Symantec AntiVirus client during startup, and selects the best Symantec AntiVirus server, based on registry values and server feedback.
- The selected server provides the client with a list of servers at the next level in the network hierarchy. SavRoam loops through the network hierarchy until no lower level exists. The final server becomes the client's new parent server, and immediately pushes a full configuration to the roaming client.
- SavRoam runs the following checks at regular intervals:
  - Checks for the availability and response time of its parent server. If its parent server is unavailable or another parent server can provide better performance, SavRoam connects the client with a new best parent server on the network.
  - Checks for the computer's network address. If the address has changed, it connects to the new best parent server.
  - If the client was previously assigned to a different parent server, SavRoam attempts to delete itself from the old parent after it checks in with the new parent.

Implementing roaming

To implement roaming, you must complete the following tasks:

- Analyze and map your Symantec AntiVirus network.
- Identify servers in each region that point roaming clients to the next level of roam servers.
- Create a list of 0 level servers for roaming clients.
- Create a hierarchical list of all roam servers, layered hierarchically and identified by type (such as Quarantine Server or Alert server), if necessary.

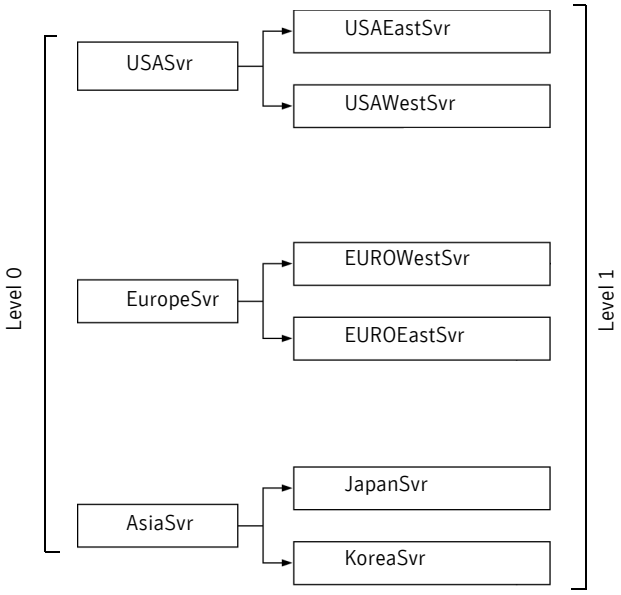
- Configure roaming client support for roaming clients and servers from the Symantec System Center console.
- Configure additional roaming client options for roaming clients in the registry. This task is optional.
- Configure additional roaming client options for roam servers in the registry. This task is optional.
- Configure additional server types for roaming clients in the registry. This task is optional.

Analyzing and mapping your Symantec AntiVirus network

While you may have many servers in your network, you may want to identify only some of them as roam servers. Creating a hierarchical map of your network lets you quickly identify roam servers for your network.

Figure 6-1 illustrates a map of an enterprise network that spans three continents. While this organization has more Symantec AntiVirus servers than appear in the map, only the mapped servers are identified as regional pointer servers.

Figure 6-1 Sample enterprise map



Identifying servers for each hierarchical level

To identify servers for each hierarchical level, you must analyze the needs of your roaming users. For example, you may need to identify mobile users based on whether they travel internationally, throughout the country, or within a smaller geographic area. If users travel internationally, their server lists will contain the names of the country servers from level 0. If they travel within one country only, their server lists will contain servers from level 1.

Depending on network speeds, the server list could contain only the top level servers (level 0 in Figure 6-1). This simplifies building the clients' server list. The only limit to the number of levels that you can define is the text file size limit of 512 characters.

Creating a list of 0 level Symantec AntiVirus servers

You can create the clients' server list text file using a text editor such as Notepad. The server list text file must contain lines in the following format:

<local><type of server><level><server list>

where:

- <local> indicates to the client that this is the 0 level of servers that the client should attempt to contact when searching for a roam server.
- <type of server> is the server type, such as parent server, Quarantine Server, Grc.dat server, or Alert server.
- <level> is 0.
- <server list> is the list of servers, which are separated by commas. (Spaces between the commas are optional.)

For example, the clients' server list text file that corresponds to Figure 6-1 is as follows:

<local> Parent 0 USASvr,EuropeSvr,AsiaSvr

This is the only line in the server list for the roaming clients in this example. The list tells the clients to contact and compare response time from these three servers only. Depending on which server is best, the client continues its search down the list into one of the three continents.

Creating a hierarchical list of Symantec AntiVirus servers

You can create the hierarchical list using a text editor such as Notepad. It must contain lines in the following format:

<computer> <type of server> <level> <server list>

where:

- <computer> is the host name of the server.
- <type of server> is the server type such as parent server, Quarantine Server, Grc.dat server, or Alert server.
- <level> is the level that is specified in the server list text file.
- <server list> is the list of servers, which are separated by commas. (Spaces between the commas are optional.)

For example, in the enterprise map in Figure 6-1, the USA branch would have the following server list:

USASvr Parent 1 USAWestSvr,USAEastSvr

Configuring roaming client support options from the Symantec System Center console

You can configure roaming client support options from the Symantec System Center console. You can configure options at the following levels:

- Server group
- Client group
- Server
- Client

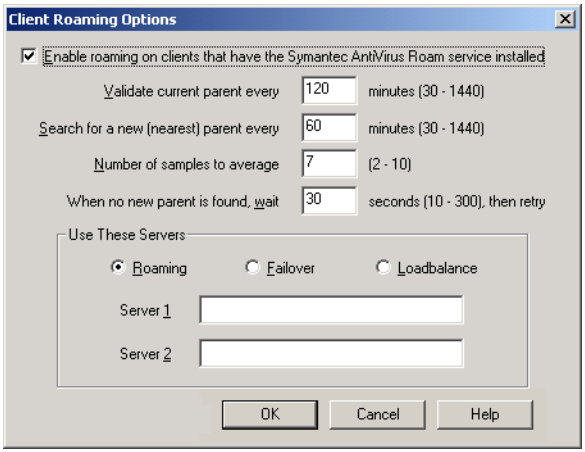
Once you set the options, Symantec AntiVirus pushes them to the Symantec AntiVirus servers and Symantec AntiVirus clients based on the selected level.

To configure roaming client support options from the Symantec System Center console

1. In the Symantec System Center console, right-click the server group, Symantec AntiVirus servers, client group, or Symantec AntiVirus clients that you want to configure, and then click **All Tasks** > **Symantec AntiVirus** > **Client Roaming Options**.

   If you select a server group, the Symantec System Center will configure all of the servers that are in the server group. If you select a client group, the

Symantec System Center will configure all of the clients that are in the client group.



2 In the Client Roaming Options dialog box, do the following:

- Enable roaming on clients on which the Symantec AntiVirus roam service is installed.
- Set the number of minutes that a client waits before it validates that its parent server is available. The default setting is 120 minutes.
- Set the number of minutes that a client waits before it checks for a closer parent server. The default setting is 60 minutes.
- Set the number of times that a client checks each server to determine the average number of seconds required to contact it. The client then uses this sampling to determine how close a server is to the client. The default setting is 7 times.
- Set the number of seconds that a client that cannot find a new parent server waits before retrying to connect to a new parent server. The default setting is 30 seconds.

3 Under Use These Servers, select one of the following:

Roaming	You can set up 0 level parent servers.
Failover	You can set up a fault tolerance system by specifying backup servers to handle clients when roam servers are unavailable. A roaming client checks the response time for the first server in the list that answers. If the first backup server fails, the roaming clients that it manages migrate to the next available backup server in the list when they check their parent server availability. Backup servers do not load balance.

Loadbalance	If you have multiple servers and want to distribute roaming clients among them, you can load balance by treating roam servers as equals regardless of how long it takes clients to contact them. A roaming client will contact each server in the list. Roaming servers keep a count of the Symantec AntiVirus clients that they manage, and return this value to the roaming client. The roaming client selects the server with the fewest clients. This server becomes the roaming client's new parent server. Load balancing has a higher priority than finding the closest parent.

4. To specify load balancing among servers, use an equal sign (=) between the servers.
   For example:
   MiamiSvr=AtlantaSvr=RichmondSvr
5. To specify failover servers, Use a greater than symbol (>) in the hierarchical list of servers.
   For example:
   MiamiSvr>AtlantaSvr>RichmondSvr
6. Click **OK**.

Configuring additional roaming client support for roaming clients

Configuring additional roaming client support for roaming clients consists of the following tasks:

- Configuring roaming on each roaming client
- Adding 0 level server data to the registry of each roaming client

Configuring additional roaming on each roaming client

You can configure additional roaming on Symantec AntiVirus clients by setting the required values in a configurations file (Grc.dat), or by directly editing each roaming client's registry using Regedit. Type the registry values under the following key:

HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\ProductControl

Table 6-2 lists and describes each registry value.

Table 6-2 Roaming client registry values

Value	Description
ProductControl\RoamQuarantine	1: Enable Central Quarantine roaming. 0: Disable Central Quarantine roaming (default).
ProductControl\RoamAlerts	1: Enable Alert server roaming. 0: Disable Alert server roaming (default).
ProductControl\RoamManagingParent Level0	List of parent servers to check for proximity.
ProductControl\RoamManagingGRC Level0	List of GRC servers to check for proximity.
ProductControl\RoamManaging QuarantineLevel0	List of Quarantine Servers to check for proximity.
ProductControl\RoamManagingAlert Level0	List of Alert servers to check for proximity.

For information on using the configurations file, see the *Symantec AntiVirus Reference Guide*.

Configuring additional roaming client support for roam servers

To configure a Symantec AntiVirus server for additional roaming options, you must complete the following tasks:

- Enable roaming and roll out the hierarchical list of servers to each roam server using RoamAdmn.exe, which is located on Disk 1 in the AdmTools folder.
- Optionally configure additional load balancing, failover, and alternate Symantec AntiVirus servers.
  See "Configuring roaming client support options from the Symantec System Center console" on page 184.

Enable roaming and roll out the hierarchal list of servers

Enabling roaming requires adding a value to the registry of each roam server, and rolling out server list data. When you run RoamAdmn, it communicates with each server named at the beginning of each line in the hierarchical list of servers. On each server, RoamAdmn adds a registry value containing the servers at the next level down in the hierarchy. If the server cannot be reached, that server is bypassed.

To enable roaming

- Add the DWORDs to the following registry key:
  HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\ProductControl\RoamServer

To roll out the hierarchical list of servers

1. Copy RoamAdmn to the computer from which you want to work while rolling out the hierarchical list of servers to the roaming servers.
2. At the command prompt, type the following:
   ```
   RoamAdmn /import <serverlist.txt>
   ```
   where <serverlist.txt> is the name of the hierarchical server list that you created.

Roaming server example

A corporation has a computer from which all roam servers are visible. The Serverlist.txt file includes the following lines:

USASvr Parent 1 USAWestSvr,USAEastSvr

EuropeSvr Parent 1 EUROEastSvr,EUROWestSvr

AsiaSvr Parent 1 JapanSvr,KoreaSvr

Table 6-3 describes the ServerList.txt data as it appears in each roam server's registry.

Table 6-3 Sample registry values

Server name	Registry value	Data
USASvr	RoamManagingParentLevel1	USAWestSvr,USAEastSvr
EuropeSvr	RoamManagingParentLevel1	EUROEastSvr,EUROWestSvr
AsiaSvr	RoamManagingParentLevel1	JapanSvr,KoreaSvr

Configuring additional server types for roaming clients

In addition to parent, load balancing, and failover servers that you can configure from the Symantec System Center console, you can specify the following server types in the registry:

- Central Quarantine Server (this must also have Symantec AntiVirus server installed).
- Alert (Alert Management System[2]) server.
- Grc.dat server, which provides the roaming client with Grc.dat settings. Using nearest_GRC lets the roaming client get policy settings from the specified server and process them immediately.

Note: A client cannot connect with multiple parents of the same type.

To configure additional server types for roaming clients

1. Set the roaming client's registry values that correspond to the server type to 1.
   See "Registry values" on page 191.
2. At the command prompt, type any of the following:
   - `SavRoam /nearest_parent`
   - `SavRoam /nearest_quarantine`
   - `SavRoam /nearest_GRC`
   - `SavRoam /nearest_alerts`

   The main difference between /nearest_parent and /nearest_GRC occurs when the configurations file (Grc.dat) is processed. Typing /nearest_parent lets the roaming client find the nearest parent. Policy settings are not processed until the client checks in with the parent. Typing /nearest_GRC lets the roaming client get the policy settings from the parent immediately, and the settings are processed immediately.

Command-line options

Table 6-4 describes the command-line options that can be used with SavRoam.exe and RoamAdmn.exe.

You must have local Administrator rights to use command-line options.

Table 6-4 Command-line options

Option	Description
/h	Displays a list of the options with descriptions of their usages.
/import <server list>	Sets up client or server registry keys. When you use RoamAdmn.exe, you can import the server list to remote servers. When you use SavRoam.exe, you can import the server list to the registry of the local computer. <server list> is the text file that contains the list of potential parent servers.
/export > <file>	Reports all of the roam servers that the client can find at all levels and for all parent types (including parent, Quarantine, Alert, and Grc.dat servers). <file> is the name of the file to which the information is written. You can use the file that is created with the export command as the server list for import.
/install <path> <new service name> <new exe name>	Registers and starts the roaming client service. The service runs until the computer is turned off. <path> is the path to the folder in which you want to copy SavRoam.exe. <new service name> is SavRoam.exe. <new exe name> is SavRoam.exe.
/remove <new service name>	Stops and removes SavRoam.exe.
/nearest	Finds and sets the nearest appropriate parent for the parent, Quarantine, Alert, or Grc.dat server. Requires that the parent GRC path be set manually in the registry.
/nearest_parent	Finds and sets the nearest parent server.
/nearest_quarantine	Finds and sets the nearest Quarantine parent server.
/nearest_GRC	Finds and applies the configurations file (Grc.dat) from the nearest Grc.dat server. Requires that the parent GRC path be set manually in the registry.

Table 6-4 Command-line options

Option	Description
/nearest_alerts	Finds and sets the nearest Alert (Alert Management System[2]) server.
/check_parent	Verifies that the parent server is running.
/shutdown	Disconnects the client from the parent server.
/time-network <elapsed-time-in-seconds> <delta-time-in-milliseconds> <servers>	Provides the average amount of time that it takes to contact each specified server. <elapsed-time-in-seconds> is the number of seconds to allow the process to run. <delta-time-in-milliseconds> is how often to contact the server in milliseconds. For example, 10,000 would cause the client to contact the server every ten seconds. <servers> is the list of servers to be contacted. Separate server names with commas. Do not include spaces between server names or commas.

Registry values

You can edit the roaming registry values using a registry editor such as Regedit or Regedt32.

The agent behavior is controlled by the registry keys under the following path:

HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\ProductControl

Table 6-5 describes the registry values for roaming clients.

Table 6-5 Registry values for roaming clients

Registry value	Description
CheckForNewParentIntervalInSeconds	Checks periodically to see if the network is up if a computer cannot find the nearest parent when it first starts. The interval is set by this registry key. The default value is 30 seconds.
CheckParentIntervalInMinutes	Determines how often a computer checks to see if its parent is available. If the parent is not available, it tries to find a new parent. The default value is 120 minutes.

Table 6-5 Registry values for roaming clients

Registry value	Description
RoamClient	Instructs the agent to make this computer a child of the nearest parent. The default value is 1. Set this value to 0 if you do not want the computer to become a child of the nearest parent.
RoamQuarantine	If the value is set to 1, sets Quarantine forwarding to the nearest server that is found from the Quarantine search keys. The default value is 0.
RoamAlerts	If the value is set to 1, sets Alert Management System[2] alert forwarding to the nearest server that is found from the Alerts search keys. The default value is 0.
RoamGRC	If the value is set to 1, lets the client roam to the server from which it should receive configurations file (Grc.dat) updates. The default value is 0.
RoamServer	If the value is set to 1, lets the client roam to the best parent server. The default value is 0.
ParentGRCPath	Sets the ParentGRCPath value to the configurations file (Grc.dat). The agent copies the configurations file to the local computer and applies it. For more information, see the RoamGRC description. If the RoamClient and RoamGRC keys are set to 1, SavRoam.exe copies the configurations file from the parent, and then copies the configurations file from the GRC parent and overwrites the parent copy.
ParentLiveUpdateHstPath	Defines the directory beneath the SAV home directory. For example: \MyLiveUpdateHost\Liveupdt.hst The .hst file must be placed under OSDRIVE/ProgramFiles/Symantec/LiveUpdate. The agent copies the LiveUpdate host file to this location.

Chapter 7

Working with Histories and Event Logs

This chapter includes the following topics:

- About Histories and Event Logs
- Sorting and filtering History and Event Log data
- Viewing Histories
- Forwarding client logs to parent servers
- Deleting Histories and Event Logs

About Histories and Event Logs

Histories and Event Logs offer a central view of virus and other threat activity and scanning on your network. Using the Symantec System Center, you can do the following:

- View data at the server group, server, or individual managed workstation level. In addition, each Symantec AntiVirus client stores its own Event Log data locally. The data is viewable from the Symantec AntiVirus client user interface.
- Sort and filter History and Event Log data.
- Perform actions based on History and Event Log data. For example, if a Threat History displays a virus found, you can perform actions such as repairing the virus or moving the infected file to the Central Quarantine.
- Export data to Microsoft Access (as an .mdb file) or in comma-separated value (CSV) format.
- Remove History and Event Log data.

Symantec AntiVirus provides several types of Histories and Event Logs as described in Table 7-1.

Table 7-1 History and Event Log types

Name	Description	Available for
Event Log	Provides information about Symantec AntiVirus startups and shutdowns, scans that were started, stopped, or aborted, configuration changes, virus definitions files updates, virus infections, items that were forwarded to the Central Quarantine, and items that were forwarded to Symantec Security Response.	■ Server groups ■ Individual servers ■ Individual clients
Scan History	Provides information about scans that have run or are running on Symantec AntiVirus clients at the server group, server, or individual workstation level. Specify a time range to filter the view. For example, you might want to view only those scans that ran within the last seven days.	■ Server groups ■ Individual servers ■ Individual clients
Threat History	Lists all viruses and threats that were detected for selected computers or server groups. You can select a virus item in the list and perform additional actions, such as Delete or Move To Quarantine. (Expanded threats cannot be placed in Quarantine.) Threat History shows many details about each virus infection, such as the name and location of the infected file, the name of the infected computer, the primary and secondary actions that were configured for the detected virus, and the action that was taken on the virus. You can click on the link to the right of the expanded threat item to access detailed information about it at the Symantec Security Response Web site.	■ Server groups ■ Individual servers ■ Individual clients
Virus Sweep History	Includes information about previous virus sweeps for servers or server groups.	■ Server groups ■ Individual servers

Sorting and filtering History and Event Log data

When you view the Threat History, Virus Sweep History, Scan History, or Event Log, you can filter items in the following ways:

- Today

- Past 7 days
- This month
- All items
- A selected range of days

You can also filter event types by selecting just the events that you want to view.

Sort and filter History and Event Log data

When you view Histories and Event logs, you can sort the data in any column.

You can filter History and Event Log data by date. You can also filter by event type for the Event Log.

To sort the data

◆ Click the column header.
The ascending sort icon appears within a column header the first time that you click it. The descending sort icon appears the next time that you click the column header.

To filter History and Event Log data by date

1 In the Symantec System Center console, right-click a server or server group, and then click **All Tasks** > **Symantec AntiVirus** > **Logs**, and then select one of the following:
   - Event Log
   - Scan History
   - Threat History
   - Virus Sweep History

2 In the list, select one of the following:
   - Today
   - Past 7 Days
   - This Month
   - All Items
   - Selected Range
     If you select Selected Range, select start and end dates, and then click **OK**.

To filter Event Log data by event type

1 In the Symantec System Center console, right-click a server or server group, and then click **All Tasks** > **Symantec AntiVirus** > **Logs** > **Event Log**.

2 In the Event Log dialog box, click the filter icon.

3 In the Filter Event Log dialog box, select the events you want to display:

- Configuration change
- Symantec AntiVirus startup and shutdown
- Virus definition file
- Scan omissions
- Forwarded to the Quarantine Server
- Delivered to Symantec Security Response
- Realtime protection load/unload
- Client management and roaming
- Unauthorized communication (access denied) warnings

4 Click **OK**.

Viewing Histories

Table 7-2 describes the Histories that you can view in the Symantec System Center console.

Table 7-2 Histories

History	Description
Threat Histories	■ At the server group level, displays all of the viruses and other threats that were found in that server group ■ At the server level, displays all of the viruses and other threats that were found for clients that are managed by that server ■ At the client level, displays all of the viruses and other threats that were found for the client
Virus Sweep Histories	■ At the server group and server level, displays all of the virus sweeps for all servers in a server group or a server
Scan Histories (current and scheduled)	■ At the server group level, displays all of the virus scans for that server group ■ At the server level, displays all of the virus sweeps for clients that are managed by that server ■ At the client level, displays all of the virus sweeps for that client

View Histories

You can view Threat Histories, Virus Sweep Histories, and Virus Scan Histories.

See "Working with Threat Histories" on page 198.

To view a Threat History

◆ In the Symantec System Center console, right-click a server, server group, or client, and then click **All Tasks** > **Symantec AntiVirus** > **Logs** > **Threat History**.

See "Understanding Event Log icons" on page 202.

To view a Virus Sweep History

1 In the Symantec System Center console, right-click a server or server group, and then click **All Tasks** > **Symantec AntiVirus** > **Logs** > **Virus Sweep History**.

2 In the Virus Sweep History dialog box, click **View Results** to examine the results of previous sweeps.

To view the Scan History

- In the Symantec System Center console, right-click a server group, server, or client, and then click **All Tasks** > **Symantec AntiVirus** > **Logs** > **Scan History**.

Working with Threat Histories

In the Threat History window, icons display information about the viruses that were found. You can also perform actions such as saving the data as a CSV file.

Note: You cannot perform additional actions on email data. You can perform only limited actions on compressed files.

Table 7-3 lists and describes Threat History icons.

Table 7-3 Threat History icons

Icon	Description
	The file is infected with a virus or the file is another threat type, such as adware or spyware.
	The file is not infected. The file was never infected, or it has been cleaned. See the action that was taken on the file for more information.
	An error occurred in association with this file.
	Close the Threat History window.

Table 7-4 lists and describes the actions available for viruses and blended threats in the Threat History window.

Table 7-4 Threat History actions for viruses and blended threats

Action	Description
Undo Action Taken	Symantec AntiVirus can undo the last action that was taken on an infected file, including removing a file from the Quarantine and removing the .vbn extension from a renamed file. Symantec AntiVirus cannot restore a file that has been permanently deleted. You cannot undo actions on compressed files.

Table 7-4 Threat History actions for viruses and blended threats

Action	Description
Clean	Symantec AntiVirus virus definitions files are frequently updated. A file that you could not clean yesterday or a few weeks ago might be able to be cleaned when the virus definitions file is updated. You cannot perform this action on compressed files.
Delete Permanently	You can permanently delete any infected file (including a compressed file) that is stored in the Quarantine or Threat History. Permanently deleted files cannot be recovered.
Move To Quarantine	If you determine that Symantec AntiVirus has left an infected file alone, you should move the file to the Quarantine, where the virus will be unable to spread. You can move compressed files to the Quarantine.
Export	You can export information about a specific Threat History or Event Log item as a CSV or Microsoft Access database file.

In the Threat History window, detected non-viral threats appear. You handle these threats differently than viruses and blended threats.

In a Threat History, you can perform a different set of actions for viruses than you can for other threats, such as adware and spyware.

Work with Threat Histories

For viruses, you can undo the last action that was taken on a file, clean a file, delete it permanently, or move the file to the Central Quarantine.

For other threats, you can access a Symantec Security Response web page to learn how to handle the threat.

You can also export the Threat History data.

To undo the last action that was taken

1 Right-click a file, and then click **Undo Action Taken**.

2 In the Take Action dialog box, click **Start Undo**.

To clean an infected file

1 Right-click a file, and then click **Clean**.

2 In the Take Action dialog box, click **Start Clean**.

To delete an infected file permanently

1. Right-click the file, and then click **Delete Permanently**.
2. In the Take Action dialog box, click **Start Delete**.
   Permanently deleted files cannot be recovered.

To move a file to the Central Quarantine

1. Right-click the file, and then click **Move To Quarantine**.
2. In the Take Action dialog box, click **Quarantine**.

To handle a threat in an expanded threat category

1. Double-click the file.
   A Symantec Security Response web page appears that describes the threat in detail and provides information about removal methods.
2. Take the recommended actions to remove the threat.

To export the Threat History data

1. Right-click the file, and then click **Export**.
2. In the Save as type list, select one of the following:
   - CSV
   - Access Database
3. In the File name box, type a file name.
4. Click **OK**.

Working with Scan Histories

In the Scan History window, icons display information about any viruses that were found. You can also perform actions, such as saving the data as a CSV file.

Note: You cannot perform additional actions on email data and only limited actions on compressed files.

Table 7-5 lists and describes the icons.

Table 7-5 Scan History icons

Icon	Description
	The file is infected.
	The file is not infected. The file was never infected, or it has been cleaned. See the action taken on the file for more information.
	Close the Scan History window.
	Display item properties.
	Save the data that is shown in the Scan History as a comma separated value (.csv) file.
	Display Help for the Scan History.

Table 7-6 lists and describes the actions available in the Scan History window.

Table 7-6 Scan History actions

Action	Description
Undo Action Taken	Symantec AntiVirus can undo the last action that was taken on an infected file, including removing a file from the Quarantine, and removing the .vbn extension from a renamed file. Symantec AntiVirus cannot restore a file that has been permanently deleted. You cannot undo actions on compressed files.
Clean	Symantec AntiVirus virus definitions files are frequently updated. A file that you could not clean previously might be able to be cleaned when the virus definitions file is updated. You cannot perform this action on compressed files.
Delete Permanently	You can permanently delete any infected file (including a compressed file) that is stored in the Quarantine or Scan History. Permanently deleted files cannot be recovered.
Move To Quarantine	If you determine that Symantec AntiVirus has left an infected file alone, you should move the file to the Quarantine where the virus will be unable to spread. You can move compressed files to the Quarantine.
Export	You can export information about a specific Scan History or Event Log item as a CSV or Microsoft Access database file.

Work with Scan Histories

In a Scan History, you can undo the last action that was taken on a file, clean a file, delete it permanently, or move the file to the Central Quarantine. You can also export Scan History data.

To undo the last action that was taken

1. Right-click a file, and then click **Undo Action Taken**.
2. In the Take Action dialog box, click **Start Undo**.

To clean an infected file

1. Right-click a file, and then click **Clean**.
2. In the Take Action dialog box, click **Start Clean**.

To delete an infected file permanently

1. Right-click a file, and then click **Delete Permanently**.
2. In the Take Action dialog box, click **Start Delete**.
   Permanently deleted files cannot be recovered.

To move a file to the Central Quarantine

1. Right-click a file, and then click **Move To Quarantine**.
2. In the Take Action dialog box, click **Quarantine**.

To export the Scan History data

1. Right-click the file, and then click **Export**.
2. In the Save as type list, select one of the following:
   - CSV
   - Access Database
3. In the File name box, type a file name.
4. Click **OK**.

Understanding Event Log icons

In the Event Log window, icons display information about any viruses that were found, and allow you to perform actions, such as saving the data as a CSV file.

Table 7-7 lists and describes Event Log icons.

Table 7-7 Event Log icons

Icon	Description
	Get information about an event.
	An error occurred in association with this event.
	Close the Event Log window.
	View item properties.
	Save the data shown in the Event Log window as a CSV or Microsoft Access database file.
	Filter the Event Log by the following categories: ■ Configuration change ■ Symantec AntiVirus startup/shutdown ■ Virus definitions file ■ Scan Omissions ■ Forward to Quarantine ■ Deliver to Symantec Security Response
	Display Help for the Event Log.

Forwarding client logs to parent servers

Symantec AntiVirus managed and sometimes managed clients forward log data to their parent servers. Log forwarding runs continually on managed clients. Log data accumulates between connections to parent servers for sometimes managed clients, such as roaming clients.

Symantec AntiVirus monitors and provides fault tolerant forwarding of the client logs. The client logs are located in the following directory:

C:\Documents and Settings\All Users\Application Data\Symantec\Symantec AntiVirus\7.5\Logs

Symantec AntiVirus tracks a client log throughout the forwarding process and handles delivery failures by resending the log when necessary.

Configuring log forwarding options

You can edit the client log forwarding registry values using a registry editor such as Regedit or Regedt32. You can reset values to achieve a balance between

the log delivery speed and network performance. You can also set the amount of data that Symantec AntiVirus forwards from clients.

Log forwarding behavior is controlled by the registry keys under the following path:

HKLM\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\Common\ForwardEvents

Table 7-8 describes the registry values for client log forwarding.

Table 7-8 Client log forwarding registry key values

Registry value	Description
Interval	Number of seconds between log record processing intervals. There is no minimum or maximum number.
Count	The number of records to process in each polling interval. The default is 10 records. There is no minimum or maximum number.

Configuring log events to forward

You can configure the events that you want Symantec AntiVirus to forward. Table 7-9 lists the client and server events in the order in which they appear in the Log Event Forwarding dialog box.

Table 7-9 Client and server events

Event name	Forwarding Required	Forwarded by Default
Scan stopped	✓	✓
Scan started	✓	✓
Virus definition update information		
Virus infections		
File not scanned		
New virus defs applied		✓
Configuration change		
Service shutdown		
Service startup		

Table 7-9 Client and server events

Event name	Forwarding Required	Forwarded by Default
Virus definitions downloaded from parent		
File forwarded to Quarantine Server		
File forwarded to Symantec		
File backed-up/restored to/from Quarantine		
Scan aborted	✓	✓
Error loading services		✓
Services loaded		
Services unloaded		
Client removed from parent server		✓
Scan delayed	✓	✓
Scan restarted	✓	✓
Client roamed to new parent server		
Client roamed from parent server		
Unauthorized communication	✓	✓
Log forwarding error		

Configure log events to forward

You can configure the events to forward from a client to its parent server or from a secondary server to its primary server.

Note: If you change primary servers, the log from the former primary server is not forwarded to the new primary server.

To configure events to forward from clients to their parent servers

1. In the Symantec System Center console, right-click a server, server group, or client, and then click **All Tasks** > **Symantec AntiVirus** > **Logs** > **Client Log Forwarding**.
2. Check the events that you want the clients to forward to their parent servers.
3. Click **OK**.

To configure events to forward from secondary servers to their primary servers

1. In the Symantec System Center console, right-click a server or server group, and then click **All Tasks** > **Symantec AntiVirus** > **Logs** > **Server Log Forwarding**.
2. Check the events that you want the secondary servers to forward to their primary server.
3. Click **OK**.

Best practice: Configuring events to forward for sometimes managed clients

For sometimes managed clients, as a best practice, you can create a separate client group. See "Creating new client groups" on page 53. You can then set log forwarding Windows registry values to do the following:

- Forward the Virus definition update information event only.
- Poll at a high interval.
- Count at a low value.

See Table 7-8, "Client log forwarding registry key values," on page 204.

Reviewing the forwarding status file

You can verify that a client log was forwarded and received by reviewing Fwdstatus.log, the default status log.

To verify that a client log was forwarded and received

1. Open the following folder:
   C:\Documents and Settings\All Users\Application Data\Symantec\Symantec AntiVirus\7.5\Logs
2. Use a standard text editor, such as Notepad, to open **Fwdstatus.log**.

Deleting Histories and Event Logs

You can configure Symantec AntiVirus to automatically remove data from Histories and Event Logs that is older than a specified date.

To set the delete frequency

1. In the Symantec System Center console, right-click a server, server group, or client, and then click **All Tasks** > **Symantec AntiVirus** > **Configure History**.
2. In the History Options dialog box, select the time period after which the Histories or Event Logs will be deleted.
3. Check **Apply settings to clients not in Groups** to apply the settings to the selected client or clients under the selected server or server group that are not members of client groups.
4. Click **OK**.
   This does not permanently remove data, but hides it in the History and Event Log views. To permanently delete History or Event Log records, delete the .log files that contain the event records. Events are recorded in .log files for each day of the week in a Logs directory. These files are named according to the day on which they were created.

Index

Numerics

32-bit and 16-bit operating systems, running virus sweeps 176
64-bit operating systems
  using Continuous LiveUpdate 147
  virus definitions files 147

A

access list
  reloading 51
  using to enhance server group security 48
  values for IP and IPX addresses 50
Action Status for alerts 83
Active Directory
  requirement for Discovery 21
address cache discovery 22
adware 90
alert actions
  configuring messages 64
  viewing export status 79
Alert Log
  Action Status 83
  copying contents to Clipboard 82
  deleting entries 81
  displaying alerts in 80
  filtering display list 83
  viewing detailed information 82
Alert Management System
  about 61
  alert forwarding for unmanaged clients 84
  Alert Log 80
  alert notification methods 61
  configuring alert action messages 64
  event threads 62
  forwarding alerts to servers 85
  limiting alert configuration network segments 66
  speeding up alert configuration 66
alerts
  actions
    deleting actions from alerts 78
    export status 79
    exporting to other computers 78, 79
    limiting to network segments 66
    testing 78
  configuring
    Broadcast 69
    default messages 65
    paging services 73
    SNMP traps 74
  configuring actions
    about 63
    Broadcast 69
    Load An NLM 70
    Message Box 68
    messages 64
    Run Program 69
    Send Internet Mail 71
    Send Page 72
  forwarding
    for roaming clients 192
    to AMS servers 85
  message
    parameters 64
    size limitation 65
antivirus clients
  configuring with Grc.dat 13
antivirus protection 13, 15, 37
antivirus servers
  configuring using the Virus Definition Transport Method 148
audits
  determining network security 31
  labeling items and rerunning audits 34
  labeling items during 34
Auto-Protect
  advanced options 98, 103
  configuring 96
  email scanning 105
  preserving file times 100
  resetting options at different levels 109
  scanning
    about 92

configuring for mail applications 96
email support issues 108
options 95
SmartScan 98

B

backup files 101
blended threats 90
Bloodhound scanning 101, 104
Broadcast alert, configuring 69

C

cache
adding Windows NT/2000 server addresses to NetWare server address cache 151
caching client information when filtering client groups 56
discovering computers from 26
Discovery Clear Cache Now setting 26
file options 104
finding computers in local cache 27, 28
items
server group passwords 43
server names and IP addresses in Symantec System Center console 21
Load from cache only discovery type 22
Normal Discovery address cache comparisons 21
client groups
adding clients to 53
caching information when filtering 56
changing settings 50
configuration change priority 39
configuring settings 54
creating 53, 57
deciding whether to manage with 39
deleting 57
dragging and dropping clients to add them 53
dragging and dropping clients to move them 54
filtering client group view 56
finding settings 54
icon 15
moving clients between 54
renaming 57
running tasks 54
scenario 40
viewing 54
clients
about antivirus protection for 37
adding to client groups 53
assigned and unassigned 39
Auto-Protect options for 96
changing between unmanaged and managed 58
check-in time 121
configuring check-in intervals 121, 122
configuring expiration 121, 122
disabling scheduled scans 120
dragging and dropping to add into client groups 53
dragging and dropping to move between client groups 54
enumerating in server groups 56
forcing virus definitions files updates 162
log forwarding, registry values 203
moving between client groups 54
overview of centralized scanning control for 96
scheduling scans 116
settings when the client group is deleted 57
viewing virus list 167
with intermittent connectivity 121
compressed files, configuring scanning 141
computers
finding
computers that are running antivirus software from other vendors 36
computers that are running unmanaged antivirus client or server 36
in local cache 27
unprotected 31
using computer names 27
using IP addresses 29
using IPX addresses 27
using network search 28
using TCP/IP 27
with outdated virus definitions 167
configuration
change priority 39
roaming client support
for servers 187
scan options 123
about 123
on multiple selected computers 95
sharing in server and client groups 38
unauthorized change attempts log 51

console
refreshing 30
starting 14
Continuous LiveUpdate
changing registry values to enable 164
configuring for managed clients 164
CPU utilization, setting for scheduled and manual scans 144

D

data columns in console views 15
dates of virus definitions files, verifying 167
delete frequency, setting for Histories and Event Logs 207
deletion, alert actions 78
dialers 90
Discovery Service
address cache discovery 22
changing the Discovery Cycle interval 22
Discovery Cycle configuration 21
how it works 20
how to find NetWare computers 21
Intense Discovery 23
limitations 23
IP Discovery 23
Local Discovery 22
Normal Discovery 21
running 23
why Discovery may not find computers 27
WINS or Active Directory requirement 21
within octets or subnet masks 66
without IP 25
drag-and-drop operation
add a client to a client group 53
move a client from one client group to another 54
move a server between server groups 41, 46

E

email, Lotus Notes, configuring scans for 96
Emergency Disk, recovering from boot virus 177
enhancement, server group security 48
event logs
deleting 207
filtering data 194
icons 203
setting delete frequency 207
sorting data 194
types 194
event threads 62
events, forward from clients and servers 204
expanded threat detection 89
export command for roaming client support 190
export status, viewing for alert actions 79

F

failover servers for roaming clients 185
files
backing up before repairing 101
cache options 104
cleaning infected 199, 202
deleting infected 200, 202
excluding from scanning 132
exclusions 133
moving to Quarantine 200, 202
undoing action taken 199, 202
filter, server group view 47
forward log events 204
forward logs to parent servers 203
found items, locating in the Symantec System Center console 29

G

GRC servers 187
Grc.dat 46
changing parent servers 46, 58
configuring antivirus clients 13
enabling and configuring roaming clients 186
forwarding alerts to AMS servers 85
Grcsrv.dat 46

H

hack tools 90
heuristic scanning 104
Hierarchical Storage Management (HSM) settings, configuring 141
Histories
about 193
deleting 207
filtering data 194
Scan Histories 200
Scan History actions 201
Scan History icons 201
setting delete frequency 207
sorting data 194

Threat History actions 198
Threat History icons 198
types 194
viewing 197
History and Event Log data, filtering 194
History and Log data, exporting to Microsoft Access 199

I

icons
Scan History 200
Symantec System Center 17
Threat History 198
infected email message 130
infected files
cleaning 199
deleting 200
deleting on creation 101
infections, managing 171
Intelligent Updater 166
Intense Discovery
about 23, 26
about Discovery types 20
IP addresses, finding computers using 29
IP Discovery 23
IPX addresses, finding computers using 27

J

joke programs 90

L

LiveUpdate
configuring servers to retrieve from Symantec FTP site 154
setting client policy for 165
using with internal LiveUpdate server 155
LiveUpdate servers, configuring internally for managed clients 163
Load An NLM alert, configuring 70
load balancing for roam servers 186
Load from cache only discovery 20
Local Discovery 20, 22, 26
locking server groups 42
log events, forward 204
log forwarding 203
log type comparisons 197
log unauthorized configuration change attempts 51
Lotus Notes, configuring scans for 96

M

managed clients
changing to unmanaged clients 58
configuring Continuous LiveUpdate for 164
configuring for internal LiveUpdate servers 163
mobile clients 121
manual scans
configuring 110
options 92
Message Box alert, configuring 68
mobile clients, managing 121

N

NetWare
adding Windows NT/2000 server addresses to cache 151
finding NetWare servers 21
network auditing
setting options 34
Nsctop.exe 20

P

pager message, entering 74
paging service alerting, configuring 73
paging services, configuring for AMS 74
parent server 46
See also servers
passwords
cached 43
changing 43
changing for server groups 44
saving or unsaving 43
Ping Discovery Service 20
primary server 37, 46
purge of suspicious files from local Quarantines automatically 174

Q

Quarantine
forwarding for roaming clients 192
moving files to 200, 202
purging suspicious files from 174

R

Refresh feature 30
registry value
for access list 50
registry values
changing to enable Continuous LiveUpdate 164
for client log forwarding 203
for roaming clients 191
remote access programs 90
roam servers 180
RoamAdmn.exe
about 180
command-line options 189
roaming client support
configuring
for clients 186
from Symantec System Center console 184
how it works 181
roaming clients
about 179
analyzing and mapping the antivirus network 182
components 180
configuring load balancing, failover servers, and alternate servers 189
creating hierarchical server list 184
difference between /nearest_parent and /nearest_GRC servers 189
enabling and configuring with Grc.dat 186
export command 190
failover servers for 185
forwarding alerts for 192
forwarding to Quarantine 192
implementing 181
registry values 191
server list 180
specifying server types 184
roaming servers
configuring roaming support 187
example 188
identifying 182
sample registry values 188
Run Program alert, configuring 69
running tasks at the client group level, configuring settings 54

S

SavRoam.exe 180, 181
command-line options 189
Scan History
icons 200
sorting columns 194
Scan History data, exporting 202
scan with Bloodhound heuristics 104
scanning
by program type 137
configuring
Auto-Protect scans 96
manual scans 110
email 105
exclusions 108, 113
for viruses 89
History 194
option precedence 95
recommended file extensions 135
scheduled scans, configuring 113
selected files and folders 137
scans
assigning actions 123
Bloodhound 101, 104
configuring for compressed files 141
configuring manual scans 141
deleting scheduled 119
dimmed or missing options 95
displaying warning message on client 128
manual, scheduled, and Auto-Protect scan options 123
option precedence 95
options
Auto-Protect for files 96
manual 141
scheduled scans 113
to exclude files from scanning 132
scheduled scans
deleting 119
disabling 119
editing 119
running on demand 120
selecting files and folders to scan 137
setting
Auto-Protect for files 96
CPU utilization 144
options on multiple selected computers 95
scheduled scans

configuring 113
deleting 119
secondary server 38
security, enhancing for server groups 48
Send Internet Mail alert, configuring 71
Send Page alert
configuring 72
paging service 74
server groups
about 48
cached passwords 43
changing passwords 43, 44
configuration change priority 39
creating 41
deciding whether to manage with 39
deleting 48
discovering servers and clients 14
dragging and dropping servers to move them 41, 46
enhancing security 48
enumerating clients 56
filtering views 47
grouping servers into 41
how to view 47
locking and unlocking 42
moving servers to a new server group 46
planning 47
refreshing the console 30
renaming 45
saving passwords 43
scenario 40
selecting primary server for 45
unlocking and locking 42
viewing 47
servers
about antivirus protection for 37
Auto-Protect options 96
changing parent servers with Grc.dat 46, 58
changing primary and parent servers 46
configuring antivirus servers using the Virus Definition Transport Method 148
disabling scheduled scans 120
dragging and dropping to move between server groups 41, 46
grouping into server groups 41
identifying best parent for roaming clients 179
moving to a new server group 46
parent 38
primary 37
secondary 38
types
parent server 38
primary server 37
secondary server 38
viewing
in console 30
virus list for 167
SmartScan 98
SNMP trap destinations, configuring 75
spyware 90
subnet, IP discovery for 23
Symantec Security Response, tracking submissions 177
Symantec System Center
changing views 16
console views 15
icons 17
locating found items 29
populating the console 19
product management snap-ins 15
refreshing the console 30
saving console settings 16
starting 14
system hierarchy display 14
syncing to computers 31
System Hierarchy
configuration change priority 39
data columns in Console Default View 15
description 14
icon 17

T

threat 89
Threat History
icons and actions 198
sorting columns of data 194
viewing 197
Threat History data, exporting 200
Threat Tracer 104
trace threats 104
tracking
submissions to Symantec Security Response 177
virus alerts 177
Trackware 91
Trojan horses 90

U

unlocking server groups 42
unmanaged clients
    alert forwarding 84
    changing to managed clients 58
    finding with network audits 31
    using creating a custom .hst file for LiveUpdate 163
unprotected computers, finding 31
updating virus definitions files 145

V

viewing
    Alert Log 80
    client groups 54
    Histories 197
    server groups 47
    virus list 167
views
    changing 16
    Symantec System Center console 15
Virus Definition Transport Method
    configuring antivirus servers with 148
    implementation examples 168
    updating NetWare servers 150
virus definitions files
    finding computers with outdated definitions 167
    forcing updates
        on all unlocked servers 148
        on clients 163
        on servers 148
    Intelligent Updater 157
    LiveUpdate 154
    rolling back 167
    rollouts 166
    update methods 146
    verifying dates 167
    verifying version numbers 167
virus list 167
virus protection, how it works 89
virus sweep
    History 194, 197
    running in response to outbreaks 171
viruses 89

W

warning message
    adding to infected email message 130
    displaying on infected computer 128
    example 128
    for email scanning 105, 107
    variables 128
WINS requirement for Discovery 21
worms 90