

# Symantec AntiVirus™ Corporate Edition Reference Guide



# Symantec AntiVirus™ Corporate Edition Reference 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 8.1

## Copyright Notice

Copyright © 2003 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, and Norton AntiVirus are U.S. registered trademarks of Symantec Corporation. LiveUpdate, LiveUpdate Administration Utility, Symantec AntiVirus, Symantec AntiVirus Corporate Edition, 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
- 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](http://www.symantec.com/certificate). Alternatively, you may go to [www.symantec.com/techsupp/ent/enterprise.html](http://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](http://www.symantec.com/techsupp).

When contacting the Technical Support group, please be sure to have the following information available:

- 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](http://www.symantec.com), select the appropriate Global Site for your country, 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 (such as features, language availability, dealers in your area)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advise on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

# Contents

## Technical support

### Chapter 1 Introducing the reference guide

Reference guide topics ..... 7

### Chapter 2 User scenarios

Scenario 1: Medium-sized organization ..... 10

How medium-sized organizations roll out Symantec AntiVirus

Corporate Edition ..... 10

How medium-sized organizations manage alerting ..... 10

How medium-sized organizations protect their environments from  
viruses ..... 11

How medium-sized organizations update their virus definitions ..... 12

Scenario 2: Large organization ..... 12

How large organizations roll out client installations ..... 13

How large organizations manage alerting ..... 13

How large organizations protect their environments from viruses ..... 14

How large organizations update their virus definitions ..... 16

Scenario 3: Enterprise-sized organization ..... 16

How enterprise-sized organizations roll out Symantec AntiVirus

Corporate Edition ..... 17

How enterprise-sized organizations manage alerting, logging, and  
reporting ..... 18

How enterprise-sized organizations protect their environments from  
viruses ..... 18

How enterprise-sized organizations update their virus definitions ..... 21

### Chapter 3 Reset ACL tool

About the Reset ACL tool ..... 24

Restricting registry access with the Reset ACL tool ..... 24

Chapter 4	Importer tool	
	About the Importer tool .....	26
	How the Importer tool works .....	26
	Where the Importer tool is located .....	27
	Importing addresses using the Importer tool .....	27
	Deleting entries from the address cache .....	28
	Advanced usage .....	29
	Getting Help while using the Importer tool .....	30
	Known problems .....	31
Chapter 5	Windows XP/2000/NT services	
	Symantec AntiVirus Corporate Edition services .....	34
	Symantec System Center services .....	35
Chapter 6	Windows XP/2000/NT Event Log entries	
	Symantec AntiVirus Corporate Edition events .....	37
	Index	

# Introducing the reference guide

## Reference guide topics

This reference guide contains technical product information for Symantec AntiVirus Corporate Edition, including information on tools that are on the Symantec AntiVirus Corporate Edition CD. It is intended for system administrators and others who install and maintain this product in a networked, corporate environment.

[Table 1-1](#) lists and describes the topics in this reference guide.

**Table 1-1** Reference guide topics

Topic	Description
Scenarios	This chapter provides examples of how Symantec AntiVirus Corporate Edition is implemented in three different-sized organizations: medium, large, and enterprise. Although your particular situation may not precisely match any of the examples, you can get an idea of how others have implemented security solutions, and what types of issues influenced their choices.
Reset ACL tool	Many of the configuration settings for Symantec AntiVirus Corporate Edition are stored in the Windows registry. Reset ACL lets you restrict access to these registry settings on Windows XP/2000/NT operating systems to prevent unauthorized users from making changes.

**Table 1-1** Reference guide topics

Topic	Description
Importer tool	The Importer tool is a command-line utility specifically for use with the Symantec System Center. The Importer tool lets you import as many sets of computer names and IP addresses into a special address cache as you need. Symantec AntiVirus Corporate Edition can then locate computers during the Discovery process in situations where the computer names cannot be resolved using WINS/DNS.
Windows XP/2000/ NT services	This chapter lists the names of services run automatically by Symantec AntiVirus Corporate Edition and the Symantec System Center. Those names appear in the Windows XP/2000/NT Services control panel.
Windows XP/2000/ NT Event Log entries	This chapter lists and describes the events associated with Symantec AntiVirus Corporate Edition as they are listed in the Windows Event Log.

# User scenarios

This chapter includes the following topics:

- [Scenario 1: Medium-sized organization](#)
- [Scenario 2: Large organization](#)
- [Scenario 3: Enterprise-sized organization](#)

## Scenario 1: Medium-sized organization

This organization has one office and several remote users. The organization's environment includes the following:

- The organization has a total of 1,000 workstations, 96% of which are Windows 98/Me. MIS uses Windows 2000/XP for personal desktop workstations.
- Several users work remotely from their home computers, which run Windows 98/Me.
- Currently, 98% of the organization's servers are NetWare. There are several Windows 2000 servers in the organization.
- Microsoft Word and Microsoft Excel are in wide use.

### How medium-sized organizations roll out Symantec AntiVirus Corporate Edition

Medium-sized organizations roll out Symantec AntiVirus Corporate Edition in the following way:

- Deployment packages are created using Symantec Packager. Administrators use several different deployment tools. For example, one administrator rolls out silent installs through logon scripts while another uses the Web-based client install method.
- Remote users are given a CD to install an unmanaged Symantec AntiVirus Corporate Edition client.

### How medium-sized organizations manage alerting

Medium-sized organizations manage alerting in the following way:

- AMS<sup>2</sup> is installed on the primary server. An email is sent to an administrator's account when a virus is found.
- AMS<sup>2</sup> logs are monitored from the Symantec System Center for events or viruses that might require extra attention.

## How medium-sized organizations protect their environments from viruses

Medium-sized organizations protect their environments from viruses in the following way:

- The Symantec AntiVirus Corporate Edition server program is installed on NetWare servers.
- All workstations are protected by Symantec AntiVirus Corporate Edition client. The workstations use the Symantec AntiVirus Corporate Edition options defined by MIS. MIS locks Symantec AntiVirus Corporate Edition options to prevent users from changing how Symantec AntiVirus Corporate Edition protects their computers from viruses.
- MIS has installed the Symantec System Center on a Windows 2000 Professional computer for antivirus administration.
- One nonproduction Windows 2000 server was selected to be the single primary server. Using a nonproduction server saves resources on the production servers. The primary server updates automatically using LiveUpdate. The primary server then uses the Virus Definition Transport Method to push virus definitions files to all NetWare servers and all managed clients.
- Workstations that MIS considers less secure are members of the same client group. MIS configures the Symantec AntiVirus Corporate Edition settings for this client group to provide the workstations with a higher level of protection than other workstations.
- Virus alerts and definitions updates are monitored regularly from the Symantec System Center console. The administrator regularly checks the Event Log and Virus History for any events or viruses that might require extra attention.
- Most of the NetWare servers are file and application servers. Users access files on these servers often. By default, Symantec AntiVirus Corporate Edition server realtime protection scans files when they are created, renamed, moved, opened, copied, executed, or saved. MIS configures server realtime protection to scan files only when they are created, renamed, or moved. This improves performance because the number of file operations monitored is reduced.

- The administrator has scheduled a Server Group Scan to scan all Symantec AntiVirus Corporate Edition servers during nonproduction hours. The antivirus scan is scheduled to run at a different time than the scheduled nightly backup so that they do not interfere with each other.
- The administrator has scheduled a weekly Client Scan.

## How medium-sized organizations update their virus definitions

Medium-sized organizations update their virus definitions in the following way:

- The NetWare servers cannot use the automatic virus definitions update method because they are not configured for FTP connections. The administrator uses a scheduled batch file to run twice a week. The batch file downloads the definitions file from the Symantec FTP site and copies it to the SAV directory on the primary server.
- Secondary servers automatically retrieve updates from the primary server.
- Most Symantec AntiVirus Corporate Edition clients automatically receive virus definitions from their parent server using the Virus Definition Transport Method. When the parent server receives new virus definitions, it immediately begins sending the clients definitions updates. The parent server is able to update multiple clients at a time, and simultaneously updates one client on each subnet to reduce network traffic.
- Remote clients retrieve definitions updates from Symantec by running LiveUpdate.

## Scenario 2: Large organization

This organization has one corporate office and 50 branch offices scattered across the New England states. The organization's environment includes the following:

- The corporate office has 5,000 workstations that are located in five buildings. Each of the branch offices averages about 100 workstations.
- There are 420 servers in the organization, 95% of which are Windows NT/2000 and 5% of which are NetWare. Most of the servers are located at the corporate office, so many branch offices do not have a local server. There are two Terminal Servers.
- The organization has a total of 10,000 workstations, 50% of which are Windows 2000 and 50% of which are Windows 98/Me/XP.
- There are 60 thin clients connected to the Terminal Servers.

- The branch offices are connected to the corporate office through a 56-KB WAN link, and the corporate office has a 128-KB link to the Internet. Because of limited bandwidth, it is important to keep network traffic on these links to a minimum.
- Microsoft Exchange, Microsoft Word, and Microsoft Excel are in wide use. Most of the organization's workstations are highly susceptible to macro viruses, viruses spread through email, and blended threats.

## How large organizations roll out client installations

Large organizations roll out client installations in the following way:

- At their corporate headquarters, MIS rolls out installation and migration packages for local computers using Novell ZENworks. Custom deployment packages are created using Symantec Packager. The footprint of Symantec AntiVirus Corporate Edition products on users' hard disks is reduced by installing only components that MIS want users to have. When setting up the packages, MIS chose to install silently. They also specified the Symantec AntiVirus Corporate Edition product settings that users can modify.
- The branch offices do not use Symantec Packager to deploy because the bandwidth to the corporate office is limited. Users at the branch offices use a Web-based install method to install Symantec AntiVirus Corporate Edition for desktops. MIS sent these users an email with instructions and a URL link to the Web-based installer.

## How large organizations manage alerting

Large organizations manage alerting in the following way:

- Each primary server is also an AMS<sup>2</sup> server. All other server (including Terminal Server Console) and workstation alerts are forwarded to these servers.
- When a virus is found, AMS<sup>2</sup> emails the administrator in charge of antivirus protection.
- AMS<sup>2</sup> logs are monitored from the Symantec System Center for events, viruses, or blended threats that might require extra attention.

## How large organizations protect their environments from viruses

Large organizations protect their environments from viruses in the following way:

- To guard their site from infections originating on the Internet, MIS runs Symantec Enterprise Firewall.
- The Microsoft Exchange server is protected by Symantec AntiVirus/Filtering for Microsoft Exchange.
- All NetWare servers are protected by Symantec AntiVirus Corporate Edition server.
- All Windows NT/2000 servers that manage Symantec AntiVirus Corporate Edition clients are protected by the Symantec AntiVirus Corporate Edition server. All other Windows NT/2000 servers are protected by the Symantec AntiVirus Corporate Edition client.
- Symantec AntiVirus Corporate Edition server runs on the Terminal Servers.
- All workstations are protected by the Symantec AntiVirus Corporate Edition client. The workstations use the Symantec AntiVirus Corporate Edition options defined by the MIS group. Email is scanned by the Symantec AntiVirus Corporate Edition email plug-in. MIS locks Symantec AntiVirus Corporate Edition options to prevent users from changing the way that their computers are protected from viruses.
- MIS set up multiple Symantec AntiVirus Corporate Edition server groups and client groups. Before setting up server groups and client groups, MIS created a comprehensive plan. The plan addressed numerous issues, such as physical server requirements, link speeds, and the security levels required for departments and groups with varying needs and levels of vulnerability.
- The Symantec System Center is installed at the corporate office so the administrators can configure antivirus settings from a central location.
- Servers running the Symantec AntiVirus Corporate Edition server are divided into several different server groups. For example, all Terminal and NetWare servers running Symantec AntiVirus Corporate Edition server are members of the same server group because they share common functions, load, and overhead requirements.
- The number of clients attached to each parent server varies between 3,500 and 15,000. Approximately ten clients check in with their parent server every minute.

- Client groups have been set up for different departments. For example, computers in the Development group are assigned to a client group with lower-level security settings. Computers in the Customer Service department are highly susceptible to email viruses. These computers are organized into a client group with all Symantec AntiVirus Corporate Edition client settings locked.
- Some local and remote clients are separated into different client groups because they use different virus definitions updating methods.
- Windows NT/2000 servers that do not act as parent servers run the Symantec AntiVirus Corporate Edition client. Users access files on these servers often. By default, Symantec AntiVirus Corporate Edition client realtime protection scans files when they are created, renamed, moved, opened, copied, executed, or saved. MIS configures client realtime protection to scan files only when they are created, renamed, or moved. This improves performance because the number of file operations monitored is reduced.
- Clients are configured so that when File System Realtime Protection is disabled by a user, it is automatically reenabled after thirty minutes.
- Symantec AntiVirus Corporate Edition is configured to forward infected files that cannot be repaired to a Central Quarantine Server. The administrator submits suspicious files to Symantec Security Response for analysis. Symantec Security Response analyzes the file submissions and reports back to the administrator with new virus definitions or other solutions.
- The administrator has scheduled a Server Group Scan to scan all computers running the Symantec AntiVirus Corporate Edition server during nonproduction hours. The antivirus scan is scheduled to run at a different time than the scheduled nightly backup so that they do not interfere with each other.
- Administrators have scheduled client scans to run every five days. In the Client Administrator Only Options dialog box, Symantec AntiVirus Corporate Edition has been configured to snooze scheduled scans when the client is running on a battery; this way, if a laptop is running on batteries, a scheduled scan will wait until the laptop is back on AC power.
- For scheduled and manual scans, CPU utilization is configured on Windows computers based on when they are idle and not idle. The idle setting allows for higher CPU utilization when the computer is idle. The not idle setting is set for lower CPU utilization, which minimizes the impact on user productivity.

## How large organizations update their virus definitions

Large organizations update their virus definitions in the following way:

- MIS has implemented an approach that reduces traffic to the Internet. The administrator has selected an established FTP server that makes up part of the company intranet to act as a LiveUpdate server. This is not a dedicated LiveUpdate or Symantec AntiVirus Corporate Edition server. The LiveUpdate Administration Utility pulls Symantec AntiVirus Corporate Edition product updates and virus definitions files from the Symantec FTP site to the FTP server in the corporate office.
- The LiveUpdate Administration Utility is scheduled to download new packages daily, after hours.
- The primary servers retrieve virus definitions updates from the internal LiveUpdate server. They then push the virus definitions updates to the secondary servers.
- Parent servers push the clients' virus definitions updates using the Virus Definition Transport Method. The virus definitions file size is small. MIS configured Symantec AntiVirus Corporate Edition to deliver the virus definitions files efficiently. The push is multi-threaded, from fastest to slowest. Each thread deploys to one subnet at a time until all clients on that subnet have been served.

## Scenario 3: Enterprise-sized organization

This organization has offices around the world. The organization has 150 offices in the United States, ranging from 20 to 3,000 employees. The organization's environment includes the following:

- 2,500 servers, of which 10% run NetWare, 20% Windows NT, 65% Windows 2000, and 5% UNIX.
- The organization has a total of 35,000 workstations in the United States, of which 50% run Windows 98/Me/XP and 50% run Windows NT/2000.
- Many Windows NT/2000 users do not have administrative rights to their workstations.
- Many of the Windows computers are laptops.
- A small number of workstations are 64-bit computers that use Windows XP 64-Bit Edition 2003.

- MIS uses a software distribution utility to install software on all workstations.
- Lotus Notes, Microsoft Exchange, Microsoft Word, and Microsoft Excel are in wide use.

This organization uses Tivoli SecureWay Risk Manager 3.7, which ships with an adapter for Symantec AntiVirus Corporate Edition. This adapter allows Tivoli SecureWay Risk Manager to read the Symantec AntiVirus Corporate Edition Event Log. Information gathered and displayed by Tivoli SecureWay Risk Manager includes the following:

- Status of virus definitions updates
- Historical information on scans
- Statistics regarding the number of infections within the organization

## How enterprise-sized organizations roll out Symantec AntiVirus Corporate Edition

Enterprise-sized organizations roll out Symantec AntiVirus Corporate Edition in the following way:

- MIS rolls out installation and migration packages for local computers using Microsoft SMS. Deployment packages are created using Symantec Packager. Different packages from different parent servers are distributed to each client group, depending on the location and special needs of those clients. The footprint of Symantec AntiVirus Corporate Edition products on users' hard disks is reduced by installing only components that MIS wants users to have. When setting up the packages, MIS chose to install interactively. They also specified the Symantec AntiVirus Corporate Edition product settings that users can modify.
- MIS has created a special Symantec AntiVirus Corporate Edition installation CD for laptop users containing a similar installation package.
- Small branch offices that do not utilize SMS use a Web-based install method to distribute the installation packages. MIS sent these users an email with instructions and a URL link to the Web-based installer.

## How enterprise-sized organizations manage alerting, logging, and reporting

Enterprise-sized organizations manage alerting, logging, and reporting in the following way:

- Symantec AntiVirus Corporate Edition events are forwarded to Symantec Enterprise Security via the Symantec AntiVirus Corporate Edition Collector. MIS uses Symantec Enterprise Security to log events, create alert notifications as responses to events, and generate predefined and custom reports that contain event status.
- Thresholds have been set to manage the alerts and notifications. MIS uses pagers, email, and SNMP traps for alert notifications.
- MIS queries, filters, and sorts events to determine which systems are not protected, out-of-date, or have high-severity events occurring on them.
- MIS generates tabular and graphical reports of event status, based on filtered views that the MIS department has created. Some reports are for their own use, others for MIS directors and corporate upper management.

## How enterprise-sized organizations protect their environments from viruses

Enterprise-sized organizations protect their environments from viruses in the following way:

- To guard their site from infections originating in Internet email, MIS runs Symantec AntiVirus for SMTP Gateways.
- Lotus Notes servers are protected by Symantec AntiVirus/Filtering for Domino.
- Microsoft Exchange servers are protected by Symantec AntiVirus/Filtering for Microsoft Exchange.
- All NetWare servers are protected by the Symantec AntiVirus Corporate Edition server program.
- All 64-bit computers are protected by Symantec AntiVirus Corporate Edition client.
- Most Windows NT/2000 servers are protected by the Symantec AntiVirus Corporate Edition client. The few dedicated servers that are part of the enterprise antivirus deployment are protected by the Symantec AntiVirus Corporate Edition server. NetWare servers and Terminal Servers are also protected by the Symantec AntiVirus Corporate Edition server.

- All workstations are protected by the Symantec AntiVirus Corporate Edition client. The workstations use the Symantec AntiVirus Corporate Edition options defined by MIS, including email client protection. MIS locks Symantec AntiVirus Corporate Edition options to prevent users from changing the way that Symantec AntiVirus Corporate Edition protects their computers from viruses. Special antivirus configurations are assigned to client groups with special needs, such as those where security risks are high.
- Branch offices with fast links are under one server group with multiple client groups for different departments.
- Some branch offices with slow links have their own server groups. The administrator at each of these sites is responsible for the antivirus protection at that site. Some branch offices with slow links have their own parent servers rather than server groups. They use the Virus Definition Transport Method. The primary server, which is located at the corporate data center, delivers the virus definitions files over a 56-KB link. The parent servers push the virus definitions files to clients over the branch's LAN. In small branches that do not have a server, clients are assigned to a remote parent server. The clients are configured to run LiveUpdate on a randomized basis. The clients are configured to check if a LiveUpdate session was scheduled to run when the client was unavailable; if so, the client runs LiveUpdate once the computer starts up.
- Nearly all of Symantec AntiVirus Corporate Edition is managed at the corporate MIS office. MIS maintains standard and consistent client security policies.
- There are administrators at the largest branch offices with slow links. The Symantec System Center console runs at corporate MIS and at these offices only. The branch administrators have the passwords for the server groups for which they are responsible.
- Client groups are set up to provide the appropriate level of protection. The Sales department is located in four different offices. All of their client computers are members of the Sales client group. The Development department is located in one office but also has its own client group. Their antivirus options are less restrictive so they can disable antivirus protection when compiling a program.

**Scenario 3: Enterprise-sized organization**

- Windows NT/2000 servers that do not act as parent servers run the Symantec AntiVirus Corporate Edition client. Users access files on these servers often. By default, Symantec AntiVirus Corporate Edition client realtime protection scans files when they are created, renamed, moved, opened, copied, executed, or saved. MIS configures client realtime protection to scan files only when they are created, renamed, or moved. This improves performance because the number of file operations monitored is reduced.
- Laptop users are set up as roaming clients. When they do connect to the internal network via modem, they are assigned the best parent server based on proximity and speed. Symantec AntiVirus Corporate Edition checks for updates and may receive a small settings file to update options.
- Workstations that do not fall into a special-needs category share a parent server. There are no more than 5,000 clients attached to each parent server. These clients check in with their parent server every 200 minutes.
- Symantec AntiVirus Corporate Edition forwards unrepairable infected files to a Central Quarantine Server. Suspicious files are forwarded to Symantec Security Response through the Digital Immune System for analysis. The Digital Immune System (DIS) analyzes the file submissions, then either returns new virus definitions available at the DIS gateway or submits the file to Symantec Security Response for further analysis.
- Clients are configured so that when File System Realtime Protection is disabled by a user, it is automatically reenabled after thirty minutes.
- The administrator has scheduled a Server Group Scan to scan all computers running the Symantec AntiVirus Corporate Edition server program during nonproduction hours. The antivirus scan is scheduled to run at a different time than the scheduled nightly backup so they do not interfere with each other.
- The administrator has scheduled a weekly client scan. In the Client Administrator Only Options dialog box, Symantec AntiVirus Corporate Edition has been configured to snooze scheduled scans when the client is running on a battery; this way, if a laptop is running on batteries, a scheduled scan will wait until the laptop is back on AC power.

- For the Sales client group, the administrator configures the scheduled scan to allow the salesperson to delay the scan. If the scheduled scan starts during a task like a presentation, the salesperson can click the Snooze button to delay the scan for three hours. The salesperson may use the snooze button two times before the scheduled scan runs.
- For scheduled and manual scans, CPU utilization is configured on Windows computers based on when they are idle and not idle. The idle setting allows for higher CPU utilization when the computer is idle. The not idle setting is set for lower CPU utilization, which minimizes the impact on user productivity.

## How enterprise-sized organizations update their virus definitions

Enterprise-sized organizations update their virus definitions in the following way:

- One Windows 2000 server in the central office is designated as a master primary server. This server receives definitions updates from Symantec using a scheduled LiveUpdate.
- The primary servers pull from the master primary server at their scheduled time and frequency. The primary servers push the virus definitions files to the parent servers. The parent server updates multiple clients at a time, and simultaneously updates one client on each subnet to reduce network traffic.
- 64-bit computers are configured to use Continuous LiveUpdate, which automatically forces a computer to look for new updates when the virus definitions file exceeds a specified age.
- Most mobile users receive virus definitions from their assigned roaming parent server. The virus definitions files are small and do not take a long time to transfer across a dial-up connection. Mobile users also use Continuous LiveUpdate as a backup option for receiving updates directly from Symantec whenever the computer connects to the Internet. MIS has specified a maximum number of days that the virus definitions files on a Symantec AntiVirus Corporate Edition computer can be out-of-date before forcing an update. When the Symantec AntiVirus Corporate Edition client determines that its virus definitions files exceed their maximum age, it initiates a silent LiveUpdate session when it detects that an Internet connection is available.
- Dial-up mobile users have a logon script or a RAS/VPN script that triggers LiveUpdate to update virus definitions files once the user is authenticated to the RAS/VPN server.

**Scenario 3: Enterprise-sized organization**

# Reset ACL tool

This chapter includes the following topics:

- [About the Reset ACL tool](#)
- [Restricting registry access with the Reset ACL tool](#)

## About the Reset ACL tool

Reset ACL (Resetacl.exe) lets you limit access to the Symantec AntiVirus Corporate Edition registry key on Windows XP/2000/NT 4.0 computers.

By default, these computers allow all users to modify the data stored in the registry for any application, including Symantec AntiVirus Corporate Edition. Reset ACL removes the permissions that allow full access by all users to the following Symantec AntiVirus Corporate Edition registry key and its subkeys:

HKLM\SOFTWARE\Intel\LANDesk\VirusProtect6\CurrentVersion

## Restricting registry access with the Reset ACL tool

You can use the Reset ACL tool to restrict registry access.

### To restrict registry access with the Reset ACL tool

- 1 Roll out Resetacl.exe, located on the Symantec AntiVirus Corporate Edition CD in the Tools folder, to unsecured computers.
- 2 Run Resetacl.exe on each of these computers.

After you have run Resetacl.exe, only users with Administrator rights can change the registry key values.

While the Reset ACL tool boosts security for Symantec AntiVirus Corporate Edition on these computers, administrators should be aware that there are several trade-off considerations.

In addition to losing access to the registry, users without Administrator rights will not be able to do the following:

- Start or stop the Symantec AntiVirus Corporate Edition service.
- Run LiveUpdate.
- Schedule LiveUpdate.
- Configure Symantec AntiVirus Corporate Edition.  
For example, users cannot set realtime protection or email scanning options.

The options associated with these operations appear dimmed in the Symantec AntiVirus Corporate Edition interface.

In addition, the user can modify scan options, but the changes are not saved in the registry or processed. The user can also save manual scan options as the default set, but the options are not written to the registry.

# Importer tool

This chapter includes the following topics:

- [About the Importer tool](#)
- [Importing addresses using the Importer tool](#)
- [Deleting entries from the address cache](#)
- [Advanced usage](#)
- [Getting Help while using the Importer tool](#)

## About the Importer tool

The Importer tool (Importer.exe) identifies computers in a non-WINS environment to the Symantec System Center console. This lets Symantec AntiVirus Corporate Edition locate computers during the network discovery process, when the names cannot be browsed using WINS/DNS. It is a command-line utility.

In addition to importing the paired names and IP addresses of computers located in non-WINS environments, you can add any other computer name and IP address pairing to the text file so that the computer is discovered in the future. For example, you may want to add the name and address of a computer that has not been discovered successfully for an unknown reason.

---

**Note:** In most cases, you should not need the Importer tool. The Find Computer feature of the Symantec System Center can usually find and identify Symantec AntiVirus Corporate Edition servers on the network by means of address caching and the normal Discovery process.

---

## How the Importer tool works

The Importer tool runs on any computer on which the Symantec System Center is installed. You can use it to import pairs of computer names and IP addresses from a text file into the address cache registry entries used by the Symantec System Center.

Once the computer name and address pairs are imported, entries are created in the registry under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\  
CurrentVersion\AddressCache
```

You must run a Local Discovery or Intense Discovery after importing the data file. The Discovery queries the addresses of the computers. The computers running the Symantec AntiVirus Corporate Edition server are added to the Discovery Service in memory and have complete entries created in the registry. The Discovery Service can then find the computers each time that the Discovery Service is run.

## Where the Importer tool is located

The Importer tool consists of a single file, Importer.exe. Importer.exe is located on the Symantec AntiVirus Corporate Edition CD in the Tools folder.

You can copy Importer.exe to any folder on a computer on which the Symantec System Center is installed, then run it.

## Importing addresses using the Importer tool

To import addresses to the address cache, you must be logged on with Administrator rights. This is necessary so that you have write access to HKEY\_LOCAL\_MACHINE.

### Import addresses using the Importer tool

To import addresses using the Importer tool, you must complete the following tasks:

- Create a data file containing paired computer names and IP addresses.
- Run the Importer tool.

---

**Note:** You must run the Importer tool from a command prompt.

---

- Run the Discovery Service.

### To create a data file

- 1 Create a new file with a text editor such as Notepad.

- 2 Type the data in the following format:

<server name><comma><IP address><linefeed>

Avoid typing incorrect IP addresses for servers. No validation is performed to determine if two servers have the same IP address in the Importer text file.

- 3 Save the file.

For example, a data file named Computers.txt might look as follows:

Computer 1, 155.64.3.121

Computer 2, 155.64.3.122

Computer 3, 155.64.3.123

Computer 4, 155.64.3.124

Computer 5, 155.64.3.125

Computer 6, 155.64.3.126

---

**Note:** You can type a semicolon or colon to the left of an address to comment it out. For example, if you know that a network segment is down, you can comment out associated subnet addresses.

---

#### To run the Importer tool

- 1 At the command-line prompt, type the following command:  
`<fullpath> importer <filename>`  
where <fullpath> represents the full path to the Importer and <filename> represents the full path of the import file, such as  
C:\Computers\Computers.txt
- 2 Press Enter.

## Deleting entries from the address cache

Data imported from the data file does not overwrite information that is already stored in the address cache. If you have data that should be overwritten, such as an incorrect computer address, clear the cache before running the Importer.

---

**Note:** After importing the contents of the data file, do not click Clear Cache Now. Doing so deletes the contents of the address cache, including the imported data.

---

#### To delete entries from the address cache

- 1 In the Symantec System Center console, on the Tools menu, click **Discovery Service**.
- 2 Under Cache Information, click **Clear Cache Now**.

Once you run Discovery after the data import, the correct data is available for future discovery sessions.

## Advanced usage

The command line takes four parameters:

- Import file path
- First delimiter
- Second delimiter
- Order (1 = computer name/IP address, 2 = IP address/computer name; the default is 1)

---

**Note:** The second delimiter needs to be a single character only. For example, the ampersand cannot be used because the user would have to enter the following: "&"

---

For example, an import file named Machines.txt, in C:\MACHINES, could read as follows:

```
155.64.3.121/Server 1
```

```
155.64.3.122/Server 2
```

```
155.64.3.123/Server 3
```

The above example is in IP address/computer name order (2). The first parameter is a slash (/) and the second is a linefeed. The corresponding syntax for the command line would be:

```
importer C:\MACHINES\Machines.txt / LF 2
```

After the computer name and IP address pairs are imported, entries are created in the registry under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\  
CurrentVersion\AddressCache
```

You must run a local or intense discovery after importing the data file. The discovery queries the computer IP addresses. The computers running Symantec AntiVirus Corporate Edition are added to the Discovery Service in memory and have complete entries created in the registry. The Discovery Service can then find the computers each time that the Discovery Service is run.

# Getting Help while using the Importer tool

You can access Help on Importer switch and syntax information.

## To get Help while using the Importer tool

**1** At the command line, type the following:

**Importer**

**2** Press Enter.

The Importer tool displays the following Help information:

```
Simple Usage : IMPORTER <filename>
```

```
<filename> : full path of import file
```

```
File format : <server name><comma><ip address><linefeed>
```

```
Example File : Server 1,155.64.3.121
```

```
Server 2,155.64.3.122
```

```
Server 3,155.64.3.123
```

```
press "a" for advanced usage
```

```
When "a" is pressed for advanced usage, the following help will be displayed:
```

```
Advanced Usage: IMPORTER <filename> <delimiter 1> <delimiter 2> <order>
```

```
<filename> : full path of import file
```

```
<delimiter 1> : separator between first and second item in pair
```

```
<delimiter 2> : separator between pairs
```

```
NOTE: for carriage return/linefeed delimiters, use LF
```

```
for space delimiters, use SP
```

```
for comma, use ,
```

```
<order> : order of computer name/ip address pairs
```

```
1 = computer name/ip address order
```

```
2 = ip address/computer name order
```

```
EXAMPLE -
```

```
File contents : 155.64.3.121/Server 1
```

```
155.64.3.122/Server 2
```

```
155.64.3.123/Server 3
```

```
Command line : IMPORTER C:\MyFolder\MyFile.txt / LF 2
```

## Known problems

Importer depends on the HKLM\SOFTWARE\Intel\LANDesk\VirusProtect6\CurrentVersion\AddressCache key used by the Symantec System Center. If this key is not present, an error message appears.

The Importer modifies the AddressCache key under HKLM, so the user needs local administrator rights.

The Importer tool aids in the discovery process of the Symantec System Center. The Importer determines whether the Symantec System Center is present on the local computer. If not, an error message appears.

After an import, the computer names paired with their IP addresses in the registry are not complete. They show only the computer under the Address\_0 and Protocol dword values. A discovery must be run to complete the process (using the Run Discovery Now button in the Discovery Service Properties dialog box).

Do not click the Clear Cache Now option in the Discovery Service Properties dialog box. This deletes the contents of the address cache, including the imported data.

The Importer cannot assist in locating computers during the installation process.

---

**Note:** When you are pushing the Symantec AntiVirus Corporate Edition client and server to remote computers, an Import option appears in the Select Computer dialog box. Do not confuse this Import option with the Import option on the NT Client Install and AV Server Rollout installation screens.

---

The Importer does not overwrite existing IP addresses in the address cache; this is an intended design feature. However, there is a possibility that an incorrect IP address may exist in the cache. In such a case, the Importer cannot correct it.



# Windows XP/2000/NT services

This chapter includes the following topics:

- [Symantec AntiVirus Corporate Edition services](#)
- [Symantec System Center services](#)

## Symantec AntiVirus Corporate Edition services

[Table 5-1](#) lists the names and descriptions for Symantec AntiVirus Corporate Edition server services. These appear in the Windows XP/2000/NT Services control panel.

**Table 5-1** Symantec AntiVirus Corporate Edition server services

Service name	Binary name	Description
Symantec AntiVirus Server	Rtvscan.exe	Main Symantec AntiVirus Corporate Edition service. Most Symantec AntiVirus Corporate Edition server-related tasks are performed in this service.
Defwatch	Defwatch.exe	Service that watches for newly arriving virus definitions. Launches a scan of the files in Quarantine when the new virus definitions arrive.
Intel PDS	Pds.exe	Ping Discovery Service. Allows Discovery of Symantec AntiVirus Corporate Edition on this computer to occur. Applications register with this service, along with an APP ID, and a pong packet to return in response to ping requests.

[Table 5-2](#) lists the names and descriptions for Symantec AntiVirus Corporate Edition client services. These appear in the Windows XP/2000/NT Services control panel.

**Table 5-2** Symantec AntiVirus Corporate Edition client services

Service name	Binary name	Description
Symantec AntiVirus Client	Rtvscan.exe	Main Symantec AntiVirus Corporate Edition service. Most Symantec AntiVirus Corporate Edition client-related tasks are performed in this service.

**Table 5-2** Symantec AntiVirus Corporate Edition client services

Service name	Binary name	Description
Defwatch	Defwatch.exe	Service that watches for newly arriving virus definitions. Launches a scan of the files in Quarantine when the new virus definitions arrive.

## Symantec System Center services

[Table 5-3](#) lists the names and descriptions for Symantec System Center services. These appear in the Windows XP/2000/NT Services control panel.

**Table 5-3** Symantec System Center services

Service name	Binary name	Description
Symantec System Center Discovery Service	Nsctop.exe	Discovery Service used to find Symantec AntiVirus Corporate Edition servers on the network. The Discovery Service also populates the console with objects.

[Table 5-4](#) lists the names and descriptions for Alert Management System<sup>2</sup> services. These appear in the Windows XP/2000/NT Services control panel.

**Table 5-4** Alert Management System<sup>2</sup> services

Service name	Binary name	Description
Intel Alert Handler	Hndlrsvc.exe	AMS <sup>2</sup> Alert Handler service. Provides alerting actions such as message boxes, pages, emails, and so on.
Intel Alert Originator	Iao.exe	AMS <sup>2</sup> Alert Originator service. Lets alerts be received on this computer. Alerts can be received from either the local computer (in the case of a primary server), or from a remote computer (in the case of unmanaged clients using a centralized AMS <sup>2</sup> server).

**Table 5-4** Alert Management System<sup>2</sup> services

Service name	Binary name	Description
Intel File Transfer	Xfr.exe	File transfer service. Provides file transfer capabilities to AMS <sup>2</sup> .
Intel PDS	Pds.exe	Ping Discovery Service. Allows Discovery of Symantec AntiVirus Corporate Edition on this computer to occur. Applications register with this service, along with an APP ID, and a pong packet to return in response to ping requests.

# Windows XP/2000/NT Event Log entries

## Symantec AntiVirus Corporate Edition events

[Table 6-1](#) lists events written by Symantec AntiVirus Corporate Edition to the Windows XP/2000/NT Event Log.

**Table 6-1** Events written to the Windows Event Log

Event	Event number	Description
Event_Scan_Stop	2	Occurs when scanning completes.
Event_Scan_Start	3	Occurs when scanning starts.
Event_Pattern_Update	4	Occurs when a parent server sends a .vdb file to a secondary server.
Event_Infection	5	Occurs when scanning detects a virus.
Event_File_Not_Open	6	Occurs when scanning fails to gain access to a file or directory.
Event_Load_Pattern	7	Occurs when Symantec AntiVirus Corporate Edition loads a new .vdb file.
Event_Trap	11	Occurs when realtime protection email scanning handles email attachments.

**Table 6-1** Events written to the Windows Event Log

Event	Event number	Description
Event_Config_Change	12	Occurs when a server updates its configurations according to the changes made from the console, excluding configuration changes made in the PRODUCTCONTROL or DOMAINDATA registry keys.
Event_Shutdown	13	Occurs when the Symantec AntiVirus Corporate Edition service is unloaded.
Event_Startup	14	Occurs when the Symantec AntiVirus Corporate Edition service is loaded.
Event_Pattern_Download	16	Occurs when new definitions are downloaded by a scheduled definitions update.
Event_Too_Many_Viruses	17	Occurs when Symantec AntiVirus Corporate Edition has deleted or quarantined more than 5 infected files within the last minute. The number of files quarantined or deleted and the time interval are configurable from the registry. The defaults are 5 files in 60 seconds.
Event_Fwd_To_Qserver	18	Occurs when quarantined files are sent to a Quarantine Server.
Event_Backup_Restore_Error	20	Occurs when Symantec AntiVirus Corporate Edition cannot back up a file or restore a file from Quarantine.
Event_Scan_Abort	21	Occurs when a scan is stopped before it completes.
Event_Rts_Load_Error	22	Occurs when AutoProtect fails to load.
Event_Rts_Load	23	Occurs when AutoProtect loads successfully.

**Table 6-1** Events written to the Windows Event Log

Event	Event number	Description
Event_Rts_Unload	24	Occurs when AutoProtect is unloaded.
Event_Remove_Client	25	Occurs when a parent server removes a client computer from its clients list. This will happen by default when a client computer fails to check in with its parent server for over thirty days.
Event_Scan_Delayed	26	Occurs when a scheduled scan is snoozed (delayed).
Event_Scan_Restart	27	Occurs when a snoozed/paused scan is restarted.



# Index

## A

- access, limiting with the Reset ACL tool 24
- address cache
  - and administrator rights 27
  - deleting entries from 28
- Administrator rights, and the Importer tool 27
- alerts
  - and the Intel Alert Handler service 35
  - and the Intel Alert Originator service 35
- AMS services
  - Intel Alert Handler 35
  - Intel Alert Originator 35
  - Intel File Transfer 36
  - Intel PDS 36

## C

- client services
  - See also* server services; services
  - Defwatch 35
  - Symantec AntiVirus Client 34
- command line, and the Importer tool 26
- computer names
  - creating a data file for the Importer tool 27
  - importing 8
- customer profiles
  - enterprise-sized organizations 16
  - large organizations 12
  - medium-sized organizations 10

## D

- data file, creating 27
- Defwatch.exe 34, 35
- Discovery
  - and the Importer tool 8, 26
  - Intense Discovery 26
  - Local Discovery 26

## E

- Event Log entries, Windows XP/2000/NT 8, 37

## F

- file transfer service, and AMS 36
- Find Computer feature, and the Importer tool 26

## H

- Help, for the Importer tool 30
- Hndlrsvc.exe 35

## I

- Iao.exe 35
- implementation scenarios 7
- Importer tool
  - about 8, 26
  - advanced usage 29
  - and the Find Computer feature 26
  - getting help with 30
  - how it works 26
  - importing addresses with 27
  - known problems 31
  - running 28
  - where it is located 27
- Importer.exe 27
- Intel Alert Handler 35
- Intel Alert Originator 35
- Intel File Transfer 36
- Intel PDS 36
- Intense Discovery 26
- IP addresses
  - creating a data file for the Importer tool 27
  - importing 8

## L

- LiveUpdate, and the Reset ACL tool 24
- Local Discovery 26

**N**

Nscstop.exe 35

**P**

Pds.exe 34, 36

Ping Discovery Service, and the Intel PDS service 34  
profiles

- enterprise-sized organizations 16

- large organizations 12

- medium-sized organizations 10

**R**

registry

- key 24

- restricting access 24

- settings 7

Reset ACL tool

- about 7, 24

- restricting registry access with 24

Resetacl.exe 24

Rtvscan.exe 34

**S**

security, and the Reset ACL tool 24

server services

- See also* client services; services

- Defwatch 34

- Intel PDS 34

- Symantec AntiVirus Server 34

services

- See also* client services; server services

- for the Symantec System Center 35

- for Windows XP/2000/NT 8

Symantec AntiVirus Corporate Edition services 34

Symantec System Center services 35

**V**

virus definitions updates

- and the Defwatch client service 35

- and the Defwatch server service 34

**W**

Windows registry

- configuration settings in 7

- restricting access to 24

Windows XP/2000/NT

- Event Log entries 8, 37

- services 8

**X**

Xfr.exe 36