

# Symantec System Center Administrator's Guide

**Norton AntiVirus™ Enterprise Solution**

INTELLIGENT SOLUTIONS TO PROTECT YOUR ORGANIZATION

# Symantec System Center 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 4.0

## Copyright Notice

Copyright © 1999 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, Peter Norton Group, 10201 Torre Avenue, Cupertino, CA 95014.

## Trademarks

Symantec, the Symantec logo, Norton AntiVirus, LiveUpdate, Striker, Bloodhound, and Symantec AntiVirus Research Center (SARC) are trademarks of Symantec Corporation.

Microsoft, Windows, and Windows logo are registered trademarks of Microsoft Corporation. NetWare is a registered trademark of Novell, Inc. Mac and Mac OS are trademarks of Apple Computer, Inc. OS/2 is a registered trademark of IBM Corporation in the United States and other countries. 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

# SYMANTEC LICENSE AND WARRANTY

NOTICE: SYMANTEC LICENSES THE ENCLOSED SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THE LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE OPENING THIS PACKAGE, AS OPENING THE PACKAGE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN SYMANTEC IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE FULL PRODUCT WITH PROOF OF PURCHASE TO THE DEALER FROM WHOM IT WAS ACQUIRED WITHIN SIXTY DAYS OF PURCHASE, AND YOUR MONEY WILL BE REFUNDED.

## LICENSE AND WARRANTY

The software which accompanies this license (collectively the "Software") is the property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, you will have certain rights to use the Software after your acceptance of this license. Except as may be modified by a license addendum which accompanies this license, your rights and obligations with respect to the use of this Software are as follows:

- You may:

use that number of copies of the appropriate titles of the software as have otherwise been licensed to you by Symantec under a Symantec Volume Incentive or Value License, provided that the number of copies of all such titles in the aggregate will not exceed the total number of copies so indicated on such Volume Incentive or Value license;

make one copy of the Software for archival purposes, or copy the software onto the hard disk of your computer and retain the original for archival purposes;

use the Software on a network, provided that you have a licensed copy of the Software for each computer that can access the Software over that network;

after written notice to Symantec, transfer the Software on a permanent basis to another person or entity, provided that you retain no copies of the Software and the transferee agrees to the terms of this agreement; and

if a single person uses the computer on which the Software is installed at least 80% of the time, then after returning the completed product registration card which accompanies the Software, that person may also use the Software on a single home computer.

- You may not:

copy the printed documentation which accompanies the Software;

sublicense, rent or lease any portion of the Software

reverse engineer, decompile, disassemble, modify, translate,

make any attempt to discover the source code of the Software, or create derivative works from the Software;

use a previous version or copy of the Software after you have received a disk replacement set or an upgraded version as a replacement of the prior version, unless you donate a previous version of an upgraded version to a charity of your choice, and such charity agrees in writing that it will be the sole end user of the product, and that it will abide by the terms of this agreement. Unless you so donate a previous version of an upgraded version, upon upgrading the Software, all copies of the prior version must be destroyed;

use the server based software products included with the Software if you have not licensed the Norton AntiVirus Solution for server-based products;

use the client based software products included with the Software if you have not licensed the Norton AntiVirus Enterprise Solution for client-based products;

use the suite based software products included with the Software if you have not licensed the Norton AntiVirus Solution Suite;

use other than the Macintosh versions of the software if you have only licensed the Macintosh versions of the software; or use a later version of the Software than is provided herewith unless you have purchased upgrade insurance or have otherwise separately acquired the right to use such later version.

- Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to you. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money you paid for the Software. Symantec does not warrant that the Software will meet your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE.

- Disclaimer of Damages:

REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether you accept the Software.

- U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items", as that term is defined in 48 C.F.R. §2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are defined in 48 C.F.R. §252.227-7014(a)(5) and 48 C.F.R. §252.227-7014(a)(1), and used in 48 C.F.R. §12.212 and 48 C.F.R. 227.7202, as applicable.

Consistent with 48 C.F.R. §12.212, 48 C.F.R. §252.227-7015, 48 C.F.R. §227.7202 through 227.7202-4, 48 C.F.R. §52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 10201 Torre Avenue, Cupertino, CA 95014.

- General:

This Agreement will be governed by the laws of the State of California. This Agreement may only be modified by a license addendum which accompanies this license or by a written document which has been signed by both you and Symantec. Should you have any questions concerning this Agreement, or if you desire to contact Symantec for any reason, please write:

Symantec Customer Service, 175 W. Broadway, Eugene, OR 97401. Symantec, the Symantec logo, Norton AntiVirus, SAM, and SAM Administrator are U.S. registered trademarks of Symantec Corporation. Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation. NetWare is a registered trademark of Novell, Inc. Other brands and products are trademarks of their respective holder/s. © 1998 Symantec Corporation. All rights reserved. Printed in the U.S.A. Manufactured under an NSAI registered ISO 9002 quality system. 21088 8/98 07-70-00896

## SYMANTEC SOFTWARE LICENSE ADDENDUM

Notwithstanding any of the terms and conditions contained in the Symantec Software License, you may make and use up to that number of copies of the Software that is indicated on the License Authorization Coupon contained in your box. The coupon will constitute proof of your right to make and use such additional copies.

# C O N T E N T S

## Chapter 1 Understanding Symantec System Center

Symantec System Center basics .....	9
Managing Symantec products .....	12
How Symantec System Center works .....	12
What products can I manage with Symantec System Center? .....	14
What is a server group? .....	14
How do I see server groups? .....	15
Primary servers and secondary servers .....	16
Supported operating systems and protocols .....	17

## Chapter 2 Installing Symantec System Center

Planning your installation .....	20
What components do I want to install? .....	20
Do I have to uninstall Norton AntiVirus Corporate Edition 6.0 or LANDesk Virus Protect 5.x? .....	21
Do I have to uninstall Norton System Center? .....	21
Planning for network traffic .....	22
Server-to-server network traffic .....	23
Client network traffic .....	23
Other sources of traffic .....	23
Management policy planning .....	24
Symantec System Center system requirements .....	25
Understanding installation options .....	25
Locating servers during installation .....	26
Windows NT server reboot may be required after installation or update .....	26
Verifying network access and privileges .....	26
Installing Symantec System Center .....	27
Uninstalling Symantec System Center .....	28

## Chapter 3 Managing with Symantec System Center

Starting the Symantec System Center console .....	29
Using console views .....	30
Understanding Symantec System Center icons .....	31
Finding machines and refreshing the console .....	32
Managing server groups .....	36
How do I see server groups? .....	37
Filtering the server group view .....	37

---

Grouping servers into server groups .....	37
Selecting a primary server for a server group .....	38
Locking and unlocking server groups .....	39
Managing Symantec products .....	41

## Chapter 4 Using the Alert Management System2

What is Alert Management System2? .....	43
Should I use Alert Management System2? .....	44
Configuring alert actions .....	44
Configuring alert action messages .....	46
Speeding up alert configuration with Advanced Discovery .....	46
Configuring the Message Box alert action .....	47
Configuring the Broadcast alert action .....	48
Configuring the Run Program alert action .....	49
Configuring the Load An NLM alert action .....	49
Configuring the Send Internet Mail alert action .....	50
Configuring the Send Page alert action .....	51
Configuring the Send SNMP Trap alert action .....	54
Configuring the Write To Event Log alert action .....	56
Working with configured alerts .....	56
Testing configured alert actions .....	56
Exporting alert actions to other computers .....	57
Using the Alert Management System2 Alert Log .....	58
Viewing detailed alert information .....	60
Filtering the Alert Log display list .....	61
Alert Management System2 Services .....	62

## Chapter 5 Symantec System Center Troubleshooting

Seeing servers and clients from the Symantec System Center console .....	63
Alert Management System2 .....	63
I have installed the Alert Management System2 console but cannot configure alerts .....	64
My modem doesn't work with Alert Management System2 .....	64
Computer doesn't appear in the Select Action Computer list ...	64
AMS alert configuration is lost when you change primary servers .....	65
Alerts not received in Symantec System Center console .....	65

## Symantec Service and Support Solutions

---

# CD Replacement Form

## Index



# Understanding Symantec System Center

This chapter introduces:

- Symantec System Center basics
- Products you can manage with Symantec System Center
- Server groups

## Symantec System Center basics

Symantec System Center provides a management framework that you use to control Symantec products, solve problems, and perform routine maintenance from a central location over the network. You install additional management tools with Symantec System Center to manage your Symantec product. For example, to manage Norton AntiVirus Corporate Edition, you use Symantec System Center with the Norton AntiVirus Corporate Edition management snap-in.

Symantec System Center also includes sophisticated alert management capabilities.

Symantec System Center includes the following components:

- Symantec System Center console
- Alert Management System<sup>2</sup>

These tools are described in the following sections.

## Symantec System Center console

The Symantec System Center console provides you with an easy way to roll out and manage Norton AntiVirus Corporate Edition in your organization across a variety of desktops and server platforms. From the console, you can perform the following tasks:

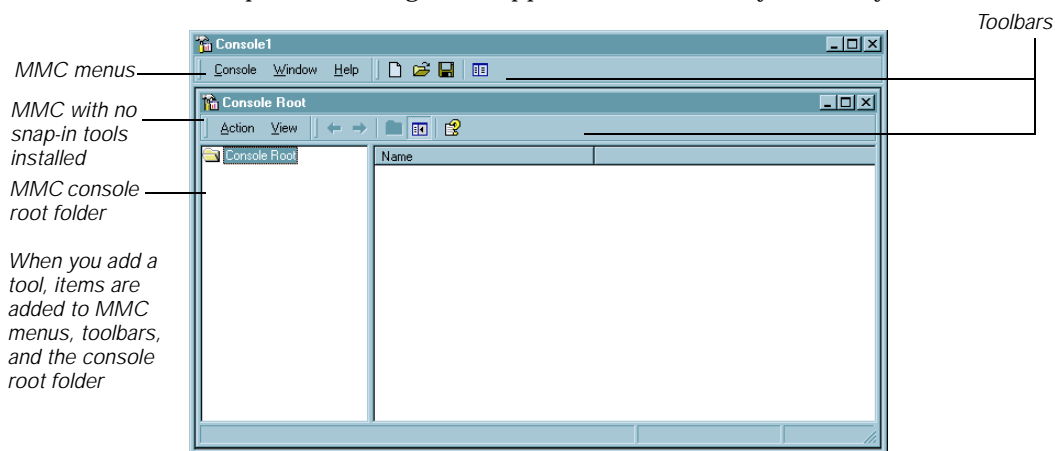
- Set up and administer server groups.
- Discover new servers and clients.
- Install and configure Norton AntiVirus Corporate Edition for server group members.
- Manage events with alerts.
- Perform remote operations.

If your site has a decentralized administration structure with multiple administrators, you can run as many copies of the Symantec System Center console as you need. Because each server group has its own password, you can divide or share administrative duties in any way that works best for you.

## Symantec System Center console and Microsoft Management Console

The Symantec System Center console snaps in to the Microsoft Management Console (MMC). MMC is a common framework for many management tools, including Microsoft SMS and SQL Server, as well as Norton System Center. With no management functionality of its own, MMC

simply serves as a central host from which you can run multiple network and product management applications, such as Symantec System Center.



MMC is installed on a local drive of a Windows NT 4.0 (Workstation or Server) machine. When Symantec System Center is installed to this same machine, it snaps in to MMC.

For more information about Microsoft Management Console, see the Microsoft website:

<http://www.microsoft.com/management/mmc/overview.htm>

Just as the Symantec System Center console snaps in to the MMC, other Symantec product management components snap in to Symantec System Center. For example, the Alert Management System<sup>2</sup>, which is described in the next section, snaps in to the Symantec System Center console. You may install additional snap-ins, such as the Norton AntiVirus Corporate Edition management snap-in, to manage specific Symantec products.

## Alert Management System<sup>2</sup>

Alert Management System<sup>2</sup> (AMS<sup>2</sup>) provides sophisticated emergency management capabilities. AMS<sup>2</sup> supports alerts from NetWare 3.12, 3.2, 4.1x, and 5.x servers, Windows NT servers and workstations, and Windows 95/98 workstations.

AMS<sup>2</sup> can process the notifications that are generated by Norton AntiVirus Corporate Edition to perform the following types of actions:

- Message Box

- Broadcast
- Send Internet Mail
- Send Page
- Run Program
- Write to Windows NT Event Log
- Send SNMP Trap
- Load an NLM

## Managing Symantec products

To manage Symantec products using Symantec System Center, you install both the Symantec System Center snap-in and the Symantec product management snap-in to MMC. For example, when you install both Symantec System Center and the Norton AntiVirus Corporate Edition management snap-in, you can do the following:

- Configure Norton AntiVirus Corporate Edition on servers and clients.
- Manage updates.
- Configure and respond to alerts.
- View information about servers and connected clients running Norton AntiVirus Corporate Edition.
- Create and manage server groups, which are containers of servers and clients that share communications channels.

Server groups can also share Symantec product configuration options. You can also invoke a Symantec product operation, such as a Norton AntiVirus scan, to run on all members of the group.

## How Symantec System Center works

From the Symantec System Center console, you can do the following:

- Administer server groups
- Configure Norton AntiVirus Corporate Edition
- Run Norton AntiVirus Corporate Edition tasks, such as scans
- View information about protected servers and connected clients

You can use Symantec System Center to solve problems and perform routine maintenance without the need to visit each server or workstation.

Symantec System Center provides these services:

Service	Description
Alerting	Symantec System Center uses events, alerts, and actions to provide proactive solutions to problems.
Logging and data export	Logs can be consolidated for easier viewing and improved report generation.
Remote configuration	Set options for Norton AntiVirus Corporate Edition on remote machines in the same primary server group.
Activating tasks	Remotely run tasks for Norton AntiVirus Corporate Edition. For example, when the Norton AntiVirus Corporate Edition snap-in is installed, you can run virus scans.

The Symantec System Center console can communicate with Symantec to receive product updates (via LiveUpdate) for Symantec System Center and Norton AntiVirus Corporate Edition components.

The following sections summarize some of the ways you can use Symantec System Center to simplify your job.

## Administering Windows NT and NetWare servers

You can combine both NetWare and Windows NT servers into the same server groups, which allows simultaneous remote configuration of either or both types of systems.

## Remotely configuring clients

If you need to modify the Symantec product settings for any of your Windows clients on which you have Norton AntiVirus Corporate Edition installed, you can use Symantec System Center to:

- Select clients by server
- Multi-select servers from a list
- Choose a single client

Changes you make to the client's parameters are automatically implemented.

## What products can I manage with Symantec System Center?

Current Symantec System Center products protect your network from known and unknown viruses. This includes the following protection:

- Norton AntiVirus Corporate Edition version 7.0 Server.
- Norton AntiVirus Corporate Edition version 7.0 Client.
- Norton AntiVirus for NetWare version 7.0.
- Norton AntiVirus for DOS/Windows 3.x.
- Quarantine, which safely isolates infected files on the system.
- Scan and Deliver, which quickly and easily separates the virus strain from the data and emails the strain to Symantec.
- Symantec AntiVirus Research Automation (SARA) provides automatic virus sample analysis and virus definition creation.
- Definition Updater, a tool to keep mobile users' virus protection up to date via your corporate email system.

For more information about managing these products, see the *Norton AntiVirus Corporate Edition Implementation Guide*.

## What is a server group?

A server group is a container of servers and clients that share communications channels. Server groups are independent of Windows NT domains and are not dependent on any other products.

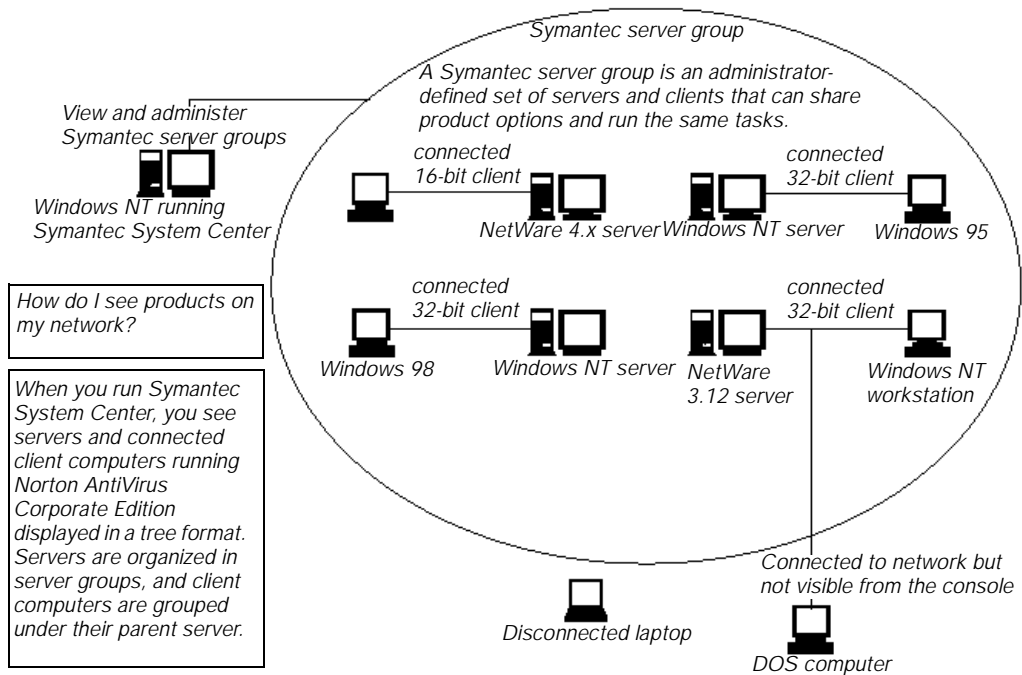
You can set server group-wide options and run Norton AntiVirus operations (such as a scan) for the computers in a server group.

You create and manage server groups. When you first roll out a Symantec server product, you create your first server group. For example, the first time that you run the AntiVirus Server Rollout option from Disk 2, the Setup wizard prompts you to create a server group.

From the Symantec System Center console, you can create new server groups and manage their membership. You can create as many server groups as you need to manage your servers and clients efficiently. Servers can be a member of only one server group at a time, but you can easily move servers from one server group to another.

You can easily move servers from one group to another using drag and drop. All clients of the server that you move are also moved to the new server group.

For administrators who have been using Norton AntiVirus Corporate Edition 6.0 or LANDesk Virus Protect 5.x until now: Server groups are identical in functionality to your old Virus Protect or Norton AntiVirus domains. You must migrate your old domains to server groups before you can manage them. The migration can be performed automatically during installation.



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

## How do I see server groups?

When you run the Symantec System Center console, you see protected servers and connected clients displayed in a tree format. Servers are grouped under the server group, and client computers are grouped under

the server they are connected to. Clients are managed through their associated server. You can define as many server groups as you need.

## Primary servers and secondary servers

When you manage with Symantec System Center, all servers are classified as primary or secondary.

### Primary server

Each server group has an administrator-designated primary server. 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.

The primary server is also the server that keeps a copy of the default server group configuration.

If you are using Alert Management System<sup>2</sup>, the primary server also processes all notifications.

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

- Windows 2000 or Windows 2000 Professional
- Windows NT 4.0 Server or Workstation
- NetWare

### Secondary server

All servers in a server group but the primary server are secondary servers. Secondary servers are clients of the primary server and retrieve information from them.

---

**Note:** 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 tasks on the server group level.

---

## Master primary server

A master primary server is a primary server from which other primary servers retrieve information. For example, when you manage Norton AntiVirus Corporate Edition using Symantec System Center, you can download virus definitions file updates to a master primary server. You can then set up all of your other primary servers to retrieve virus definitions file updates from the master primary server.

## Clients

Clients interact with their parent server when they poll for updates and configuration settings changes. If you are using the Alert Management System<sup>2</sup>, they also send event notifications to parent servers. Parent servers may be either primary or secondary servers.

## Supported operating systems and protocols

Symantec System Center is a cross-platform management tool. The Symantec System Center console can manage Norton AntiVirus Corporate Edition on these server and client operating systems:

Servers:

- Windows 2000 Professional
- Windows 2000 Server
- Windows NT Server 4.0
- Windows NT Workstation 4.0
- Novell NetWare 3.12, 4.1x, and 5.0

Clients:

- Windows 2000 Professional
- Windows 2000 Server
- Windows NT Server 4.0
- Windows NT Workstation 4.0
- Windows 95/98

## Supported protocols

- IP
- IPX

---

**Note:** 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 servers and clients that appear in the console.

---

# Installing Symantec System Center

In this chapter you'll learn about:

- Components that you can install
- Products to uninstall, migrate, or keep
- Planning for network traffic
- Management policies to consider before installation
- System requirements for Symantec System Center
- Symantec System Center installation options
- Answers to frequently asked questions about Symantec System Center installation
- Symantec System Center installation procedures
- Uninstalling Symantec System Center

---

**Tip:** We suggest that you read the Quick Start card included with your copy of the Norton AntiVirus Enterprise Solution.

---

## Planning your installation

### What components do I want to install?

You can install the components shown in the following table.

Symantec System Center console	Install the Symantec System Center console to the computer(s) from which you plan to manage your Symantec product. You must have at least one installation of Symantec System Center to see and administer your system. If your organization is large, or if you work out of several different offices, you can install Symantec System Center to as many computers as you need by rerunning the installation program and selecting the appropriate option.
Alert Management System <sup>2</sup> Console	Install the Alert Management System <sup>2</sup> (AMS <sup>2</sup> ) Console to the same computer where Norton AntiVirus Corporate Edition for Servers is installed. This allows you to configure alert actions. When a problem occurs, AMS <sup>2</sup> can send notifications through a pager, an email, and other means. If you choose not to install AMS <sup>2</sup> , you can use the notification and logging mechanisms available in Norton AntiVirus Corporate Edition.  Note: This option installs the Alert Management System <sup>2</sup> Console only. You must also install AMS <sup>2</sup> services from the Install AntiVirus To Servers option on Disk 2.
LiveUpdate Administration Utility	Install the LiveUpdate Administration Utility if you plan to update virus definitions and Symantec managed products on your servers and clients from your intranet FTP server or other internal server.

## Do I have to uninstall Norton AntiVirus Corporate Edition 6.0 or LANDesk Virus Protect 5.x?

You do have to uninstall Norton AntiVirus Corporate Edition 6.0 or LANDesk Virus Protect before you install Symantec System Center. However, the Symantec System Center installation program can uninstall for you.

If the Symantec System Center installation program detects Norton AntiVirus Corporate Edition 6.0 or LANDesk Virus Protect, it prompts you to allow it to automatically uninstall before installing Symantec System Center.

## Do I have to uninstall Norton System Center?

If you run Norton System Center product management snap-ins, such as Norton Speed Disk and Norton Helpdesk Assistant, you will still need to run Norton System Center.

You can safely run Norton System Center on the same system with Symantec System Center. You can plug them both into the same MMC console.

Symantec System Center and Norton System Center are completely independent of each other and will be unaware of the other's presence. Both tools have their uses. Norton System Center offers a job distribution model while Symantec System Center offers scalability. (Future versions of Symantec System Center will offer a job distribution model.)

If you are installing the Norton AntiVirus Corporate Edition snap-in to Symantec System Center, you will no longer need the Norton AntiVirus snap-in for Norton System Center. You may want to remove it.

## Understanding how Symantec System Center uses IP and IPX

Symantec System Center uses an adaptive communication method that handles both IP and IPX communication at any time. Two benefits of this new method are that Symantec System Center does not require or create NetWare SAPs, and Symantec System Center is fully compatible with IP-only networks. Even though this new communication method is very flexible, certain combinations of mixed protocols can prevent proper client or server communication.

### *A general rule of thumb*

Avoid using the Symantec System Center console across a link that does not support the protocols used on the other side of the link. This also applies to setting up server groups that cross a link. For example, servers and clients will not be visible in Symantec System Center if Symantec System Center is running on one side of an IP-only WAN link being used to connect NetWare servers that are only running IPX (no IP loaded) on the other side.

## Planning for network traffic

This section helps you understand how much network traffic (and what type of traffic) can be generated by alerts, configuration file transfers, clients checking for updates, the Discovery service, and refreshing.

Symantec System Center can communicate with all NetWare servers, Windows NT servers, and Windows clients. The communication protocol can be IP or IPX and may switch automatically from one to the other depending on throughput. The initial view of servers and clients that displays on the Symantec System Center console originates from the local cache and is then updated by retrieving information from each server. The client lists are gathered from each server rather than from each individual client.

Whenever server configuration parameters change, Symantec System Center sends the updates to each server in the server group directly, rather than through the primary server. Global client changes are sent through the parent server; individual client changes go directly to each client. In each case, an IP-to-IP or IPX-to-IPX path must exist for each leg of the communication.

For example, if the computer running Symantec System Center only has IP loaded, the servers have IP and IPX, but clients have only IPX, you could send updates to servers and clients through the server. Because there's no common protocol between individual clients and Symantec System Center, no updates can be sent directly to the individual clients.

Because the servers have both IP and IPX loaded, Symantec System Center communicates to the servers through IP and then the servers send the updates to the clients through IPX. To configure clients in this scenario, you must highlight the server and not individual clients. Highlighting

individual clients causes Symantec System Center to attempt direct communication with the client, which is not possible in this case.

Symantec System Center generates network traffic with activities such as when you make configuration changes, when you run discovery, and when you refresh the console. The amount of traffic generated depends on the number and type of configuration parameters you change, as well as your discovery settings.

## Server-to-server network traffic

Using either IP or IPX, protected servers can communicate with each other to send updates and to forward alerts. Other servers in the server group can pull updates from the primary server. Placing a newer update on a server other than the primary server allows that server to use the update. However, no other servers will automatically receive that update (unless a server-to-server download is scheduled). No network traffic is generated between servers until there's a new update to send.

Whenever a secondary server detects an event that triggers an alert notification to the primary server, the Alert Management System<sup>2</sup> on the primary server then processes the alert. No AMS<sup>2</sup>-related network traffic is generated when there are no notifications to forward.

## Client network traffic

Clients running managed products such as Norton AntiVirus Corporate Edition may need to communicate with servers to send event notifications and receive updates and configuration data. Clients send notifications to their parent server only when an event is generated. Windows clients periodically poll their parent server for updates and configuration changes.

## Other sources of traffic

The Discovery Service, Find feature, and Refresh feature can also generate network traffic.

- Local Discovery broadcasts to the Symantec System Center console's local subnet. Servers then respond immediately with information about themselves and their clients. Intense Discovery serially pings every server in the Network Neighborhood. The amount of traffic generated depends upon the number of minutes set for the discovery cycle interval and the number of discover threads set to run at once.

For more information, see [“Discovery service”](#) on page 32.

- A Network Discovery using the Find feature generates a small amount of traffic.

For more information, see [“Find feature”](#) on page 34.

- The Refresh feature generates a small amount of traffic when run at the server group or server level. When a server group is refreshed, Symantec System Center pings all members of the group. When a server is refreshed, Symantec System Center pings the server and its clients.

For more information about using Refresh, see [“Refresh feature”](#) on page 36.

## Management policy planning

You may want to establish some policies related to managing with Symantec System Center. Consider the following issues:

### *Locking server groups*

- You can lock a server group with a password to prevent unauthorized administrators from making configuration changes. What server groups do you want to lock? Who will have the password?

For details, see [“Locking and unlocking server groups”](#) on page 39.

### *Event management*

- What types of alert actions do you want to configure for events?
- Do you want to set up a single centralized alert server per site, or do you want alerts to go to more than one administrator?

For details, see [Chapter 4, “Using the Alert Management System2”](#) on page 43.

### **What else do I need to plan for?**

If you are installing Symantec products to be managed by Symantec System Center, you may have additional planning considerations. For example, how will you and other administrators roll out, administer, and maintain the products? What settings do you want to lock for the products?

See the documentation and Getting Started card included with your Symantec product for more information.

## Symantec System Center system requirements

- Windows NT 4.0 with Service Pack 3 or higher
- Microsoft Management Console version 1.1
- Internet Explorer 4.01
- 32 MB RAM (64 MB RAM recommended)
- Pentium 166 processor (or faster)
- 12 MB disk space

---

**Note:** If Microsoft Management Console version 1.1 is not present on the computer to which you are installing, the installation program will install it for you.

---

## Understanding installation options

When you install Symantec System Center the installation program does this:

- Lets you install Symantec System Center console to the Windows NT computer where you're running the installation program.
- Lets you install the Alert Management System<sup>2</sup> (AMS<sup>2</sup>) console to the computer where you're running the installation program (if you're also installing Symantec System Center console). When a problem occurs, AMS<sup>2</sup> can send notifications through a pager, email, and other means.

---

**Note:** To view and configure alerts, you will also need to install AMS<sup>2</sup> services to servers from the Install AntiVirus To Servers option on Disk 2.

---

### *Which computer should I use to run the server installation program?*

You can run the installation program on computers running Windows NT Workstation or Server 4.0.

## Locating servers during installation

When you run the server installation program, you can browse for the servers that you want to install to. However, servers that are across routers may be difficult to locate. To verify that you will be able to see a server when you run the server installation program, try mapping a drive to the server using Windows Explorer. If you can see a server in Windows Explorer, you should be able to see the server when you run the server installation program.

## Windows NT server reboot may be required after installation or update

As you install or update Norton AntiVirus, the installation program displays a status for each server to report the progress of the installation or update, to alert you to any errors, and to prompt you for any required action. After an installation or update, the status will be "Restart necessary" for Windows NT servers if the installation program needs to replace any files that are in use.

### Specific cases where reboot is required

- When installing AMS<sup>2</sup> to a Windows NT server, you must reboot the computer after the installation program has completed in order for AMS<sup>2</sup> to start working. (You should install AMS<sup>2</sup> to all servers that may be assigned primary status.)
- When updating Norton AntiVirus files on a Windows NT server (for example, when applying a service release), some files may be in use. In this case, you must reboot the server to replace the older files. This is a rare case.

## Verifying network access and privileges

The computer you use to run the server installation program should have the appropriate network clients and protocols running so that you can see all the NetWare and Windows NT servers where you want to install Norton AntiVirus.

The rights you need to install to server and client computers depend on the server platform and version.

## Rights to install to Windows NT servers

During the installation, if you select a server that you're not currently logged on to, the installation program will prompt you to log on. You must log on as an administrator or as a user with administrator privileges. This is necessary because the server installation program launches a second installation program at the server to create and start services and to modify the registry. For this to work properly, you must have administrator rights for the server or for the domain that the server belongs to.

# Installing Symantec System Center

To install Symantec System Center and the LiveUpdate Administration Utility:

- 1 Insert Disk 1 into the CD-ROM drive on your computer. Cdstart.exe on the CD automatically displays the installation screen.
- 2 Click Install Symantec System Center.
- 3 Select Symantec System console and Alert Management System Console.
- 4 Follow the instructions on the screen.
- 5 If you want to set up an internal LiveUpdate server, click Install LiveUpdate Administration Utility when the install screen returns, then follow the instructions on the screen.
- 6 Click Exit.

---

**Note:** To use the Alert Management System<sup>2</sup> you will also need to install Alert Management System<sup>2</sup> services. You can install Alert Management System<sup>2</sup> services at the same time that you install Norton AntiVirus Corporate Edition to computers running Windows NT Server or Workstation, or NetWare. For more information, see "Rolling out Norton AntiVirus Corporate Edition for servers" in Chapter 2 of the *Norton AntiVirus Corporate Edition Implementation Guide*.

---

# Uninstalling Symantec System Center

To uninstall Symantec System Center:

- 1 From Start Menu, choose Settings > Control Panel.
- 2 Double-click Add/Remove Programs.
- 3 Choose Symantec System Center, then click OK.

All Symantec System Center components are uninstalled. Norton AntiVirus Corporate Edition is also uninstalled.

# Managing with Symantec System Center

In this chapter you'll learn about:

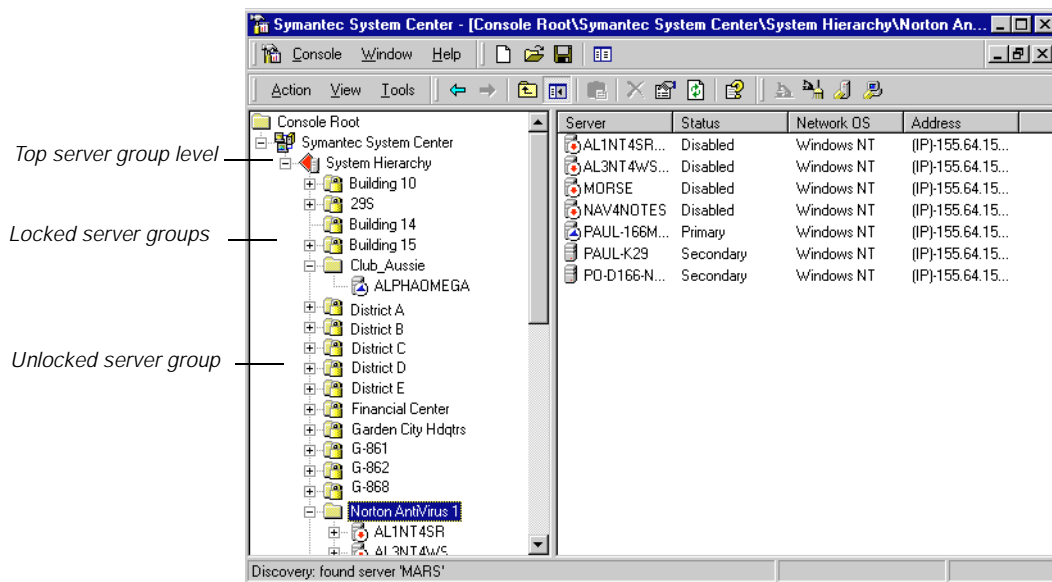
- Starting Symantec System Center
- Refreshing the console view
- Using Find and Discovery options to locate computers on your network
- Managing server groups
- Symantec System Center services
- Managing Symantec products

## Starting the Symantec System Center console

The installation program adds items to your Start menu and also creates a program group. When Symantec System Center runs, you will see server groups, servers, and connected client computers displayed in an expandable/collapsible tree format on the left pane of the console. Servers are grouped under server groups. Though not visible from the console, connected client computers are grouped under the servers to which they connect.

To start Symantec System Center:

- Click Start > Programs > Symantec System Center > Symantec System Center console.



## Using console views

When you add a product management snap-in, a new product view becomes available from the Symantec System Center console. For example, when you install the Norton AntiVirus Corporate Edition management snap-in, a new view is added that includes fields related to Norton AntiVirus, such as Last Scan and Definitions.

Unless, you change the view, the Symantec System Center console displays the Console default view.

To change views:

- 1 From the Symantec System Center console, select View.
- 2 Select from the list of views that appears at the bottom of the menu.

**Note:** When you close the MMC, you are prompted to save console settings for Symantec System Center. Click Yes if you want to see the same console view the next time that you launch MMC. Click No if you want to see the default console view the next time you launch MMC.

---

## Understanding Symantec System Center icons

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 displays with a padlock icon, the server group is locked, and you must enter the server group password before you can configure or run scans for the computers in the server group.

### Icon



### Icon descriptions

Highest level object representing all server groups.



Unlocked server group. Compare this icon to the next one, which is a locked server group. For security reasons, all server groups default to locked when you start 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.







There is either no primary server assigned to the server group or there are too many primary servers assigned to the server group. Each server group should have a single primary server.



File server. This could be a Windows NT or NetWare server. Compare this icon to the next one, which is the primary server for the server group.



Primary server. This could be a Windows NT or NetWare server.

Icon	Icon descriptions
	Unavailable file server. The file server is probably not running or the managed Symantec product is no longer running on the server, making it impossible for Symantec System Center to communicate with it.
	File server with partial information. Symantec System Center is still reading the server's information.
	Windows 95/98 or Windows NT client computer. When you select this computer, you set options only on that computer.
	Windows 3.1 client computer. From Symantec System Center, you cannot individually configure a Windows 3.1 client computer or run scans on it. To configure Windows 3.1 clients or run scans, select the server or server group above the Windows 3.1 client.

## Finding machines and refreshing the console

At startup, Symantec System Center pings every server running a manageable Symantec product. As soon as the servers respond, they and any connected client computers that are running a manageable Symantec product are added to the console.

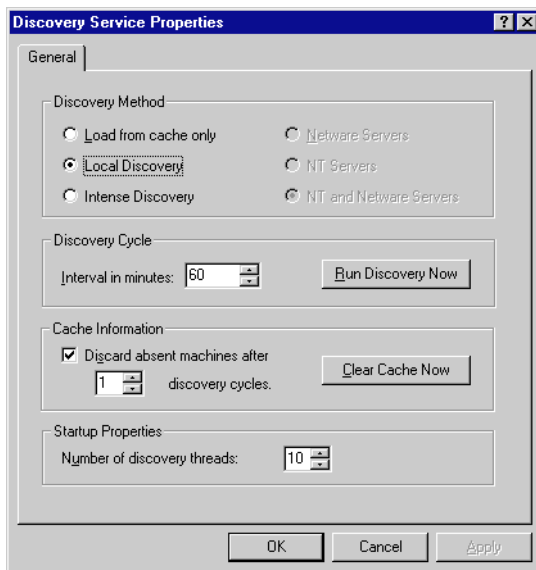
If you start servers or add connected clients that are running a manageable Symantec product while Symantec System Center is already running, you may need to locate the computer using the Find feature or Discovery Service so that it will display in the server group view.

### Discovery service

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

To discover servers and clients:

- 1 From the Tools menu, select Discovery Service.



- 2 Select one of these options:
  - Load From Cache Only—This is the quickest but least thorough method. Symantec System Center reads the list of servers and clients stored in the local cache.
  - 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.
  - Intense Discovery—This is the most thorough method. If you have a large network, the discovery process may take a long time. 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.

You can limit the search to NetWare or Windows NT servers only, or search for both.

- 3 In the Discovery Cycle group box, specify the number of minutes between discovery intervals. If you want to immediately run discovery, click Run Discovery Now, then click Close.

- 4 In the Startup Properties group box, specify the number of discovery threads. Each discovery thread is an independent search for servers and clients.

---

**Tip:** To maintain the most up-to-date discovery information, choose a lower discovery interval and a higher number of discovery threads.

---

- 5 In the Cache Information group box, select Discard Absent Machines After, then specify the number of discovery cycles after which you want to discard machines that Symantec System Center cannot contact. For example, if Interval In Minutes is set to 60 and Discard Machines After is set to 10, any machine that cannot be contacted within five hours will no longer appear in the console.
- 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, click Clear Cache Now.

---

**Note:** When you clear the cache, unlocked server groups are locked.

---

## Find feature

If you want to quickly find a computer without having to expand and browse the tree, you can use the Find feature. To find Windows 95/98 and NT/2000 computers, you search using addresses or machine names. To find NetWare servers, you search using the IPX address.

The Find feature is also useful if you install a client or server and then don't see it in the tree view when you expand a server group or server. This may be because Symantec System Center can't automatically discover servers on LAN segments separated by routers. 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 option in Symantec System Center. Once you use the Find option to locate a server, you can manage it from Symantec System Center.

**To find computers:**

- 1 From the Symantec System Center console Tools menu, select Find Computer.
- 2 For a search of the local cache, click the Local Search tab, then do one of the following:
  - Select Machine name, enter the network name of the computer you want to find in the Machine Name field, then select Exact if you are looking for a specific name or Partial if you are unsure of the machine name.
  - Select User Name, enter the name of the user associated with the machine, then select Exact if looking for a specific user name or Partial if unsure of the user name.
- 3 For a search of the Network Neighborhood, click the Network Discovery tab.
  - To find Windows 95/98 and NT/2000 computers, you search using addresses or machine names.
  - To find NetWare servers, you search using the IPX address.
- 4 Enter the server address or machine name, then choose the address type entered.
- 5 Click Find Now.

***Locating found items in the Symantec System Center console***

You can locate a found item displayed in the Find Computer list to the Symantec System Center console display. To do so, the server group to which the item belongs must be unlocked.

**To locate the item:**

- 1 In the Find Computer list, highlight the item.
- 2 Click Sync Item.

The item appears highlighted in the left pane of the Symantec System Center console.

---

**Tip:** You can perform this same operation by double-clicking the item in the Find Computer list.

---

## 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 Symantec System Center started. If the refresh determines that a server or client that previously displayed in the server group view is no longer communicating, it will dim the object in the server group view.

To refresh:

- From the Symantec System Center console, right-click the system hierarchy, server group, or server, then select Refresh.

Norton AntiVirus will refresh the list of current servers and clients without spending any time to find servers or clients that may have been added since this session.

## Managing server groups

A server group is a container of servers and clients that share communications channels. Server groups are independent of Windows NT domains and are not dependent on any other products.

Server group members can share the same Symantec product configuration settings. You can also run a Symantec product operation on all members of a server group.

The first time that you roll out a manageable Symantec product to servers, you create a server group. (For example, the first time that you run the AntiVirus Server Rollout option from Disk 2, you create a server group.)

From the Symantec System Center console, you can create new server groups and manage their membership. You can create as many server groups as you need to manage your servers and clients efficiently. Servers can be a member of only one server group at a time, but you can easily move servers from one server group to another.

For administrators who have used Norton AntiVirus Corporate Edition 6.0 or LANDesk Virus Protect 5.x until recently: Server groups are identical in functionality to your old Virus Protect or Norton AntiVirus domains. You must migrate your old domains to server groups before you can manage them. The migration can be performed automatically during installation.

## How do I see server groups?

When you run Symantec System Center, you see servers and connected clients that are running managed Symantec product displayed in a tree format. Servers are grouped under server groups, and client computers are grouped under the server they connect to. You can define as many server groups as you need.

## 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. If you want to remove server groups from your console, you must 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 From the left pane of the Symantec System Center console, right-click System Hierarchy, then select View > Filter Server Group View.
- 2 Uncheck the server groups you want to filter from the server group list. All server groups display by default.
- 3 Click OK.

---

**Tip:** To filter to a single server group, from the left pane of the Symantec System Center console, right-click the server group, then choose New Window From Here.

---

## Grouping servers into server groups

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

For example, you may have some servers that require higher levels of protection. In this case, you can place all of them in the same server group and set special options to protect that server group.

**To create a new server group:**

- 1 From the left pane of the Symantec System Center console, right-click System Hierarchy, then select New > Server Group.
- 2 Enter the name for the new server group. The name cannot be more than 47 characters.

---

**Tip:** A server can only belong to one server group. You can move servers between groups using drag and drop.

---

**To rename a server group:**

- 1 Unlock the server group you want to unlock, if necessary.
- 2 Right-click the server group.
- 3 Click Rename, then enter the new server group name.

**To delete a server group:**

- 1 Unlock the server group you want to delete, if necessary.
- 2 Cut any existing servers from the server group you will delete and paste them into another server group.
- 3 Right-click the empty server group, then click Delete.
- 4 Right-click System Hierarchy, then click Refresh.

## Selecting a primary server for a server group

When you select a server group object in Symantec System Center and set options, the settings are saved to the primary server in the server group. Other servers in the same server group will then 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 will not be allowed to perform some manageable Symantec product management options.

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

- Windows 2000 Server or Windows 2000 Professional
- Windows NT 4.0 Server or Workstation
- NetWare

Because the primary server plays an important role, select a stable server that's always running.

To assign the primary server for an existing server group:

- Right-click the server that you want to be the primary server, then select Make Server A Primary Server.

---

**Note: AMS<sup>2</sup> configuration is lost**

When changing primary servers, you will lose the AMS<sup>2</sup> alerts you've set up. You can reconfigure the alerts on the new primary server, or you can export the alerts to the new server

---

## 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 whenever you want. The default password is:

`symantec`

### Locking all server groups when exiting the console

By default, all server groups are locked when you exit the console.

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

- 1 From the Symantec System Center console, right-click System Hierarchy, then select Properties.
- 2 Clear Lock All Server Groups When Exiting Console.

## Using cached server group passwords

When entering a password, you can click the Save This Password option if you don't want to have to reenter that particular password in future sessions or for other server groups that may have the same password.

Cached passwords are DES encrypted and are stored in the registry of the local computer. On Windows NT, the password is cached for your logon only, so any other users logging on to the same computer would have to reenter the password.

## If you do not use cached server group passwords

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

### To change a server group password:

- 1 Right-click the server group, then select Configure Server Group Password.
- 2 Enter the old password, if the server group is still locked.
- 3 Enter the new password, then enter it again for confirmation.
- 4 Click OK.

### To lock a server group:

- 1 Right-click the server group that you want to lock, then select Lock Server Group.
- 2 Click Yes to confirm that you want to lock the server group.

### To unlock a server group:

- 1 Right-click the server group, then click Unlock Server Group.
- 2 Enter the password to unlock the server group.
- 3 Check the Save This Password box if you don't want to have to reenter that particular password in future sessions or for other server groups that may have the same password.
- 4 Click OK to unlock the server group.

# Managing Symantec products

From the Symantec System Center console, you can:

- Configure options settings for managed Symantec products in the same server group.
- Update managed Symantec products.
- Schedule tasks.
- Perform other activities specific to the manageable Symantec product. For example, with the Norton AntiVirus Corporate Edition snap-in installed, you can perform such tasks as scanning for viruses and viewing virus history.

For information about performing these tasks, see the documentation specific to your managed Symantec product; for example, for information about managing Norton AntiVirus Corporate Edition, see the *Norton AntiVirus Corporate Edition 7.0 Implementation Guide*.



# Using the Alert Management System<sup>2</sup>

In this chapter you'll learn about:

- The power and ease of use of the Alert Management System<sup>2</sup>
- How to configure alert actions
- Working with the Alert Management System<sup>2</sup> alert log

## What is Alert Management System<sup>2</sup>?

Alert Management System<sup>2</sup> (AMS<sup>2</sup>) provides sophisticated emergency management capabilities. AMS<sup>2</sup> supports alerts on NetWare 3.12, 3.2, 4.1x, and 5.x servers, Windows NT servers and workstations, and Windows 95 and 98 workstations.

AMS<sup>2</sup> is a robust and fault-tolerant alert system with no single point of failure. While other alert handling mechanisms require a functioning network in order to send and receive alerts, AMS<sup>2</sup> can send and receive alerts when the network has failed or is only partly functional.

AMS<sup>2</sup> can generate alerts through these means:

- Message Box
- Broadcast
- Send Internet Mail
- Send Page
- Run Program
- Write to Windows NT Event Log

- Send SNMP Trap
- Load an NLM

## Should I use Alert Management System<sup>2</sup>?

AMS<sup>2</sup> lets you configure many different methods of notification for detected viruses, including pager, SNMP, and email. Your Norton AntiVirus Corporate Edition management snap-in also has built-in notification capabilities that you can use instead of, or in addition to, the AMS<sup>2</sup> notification.

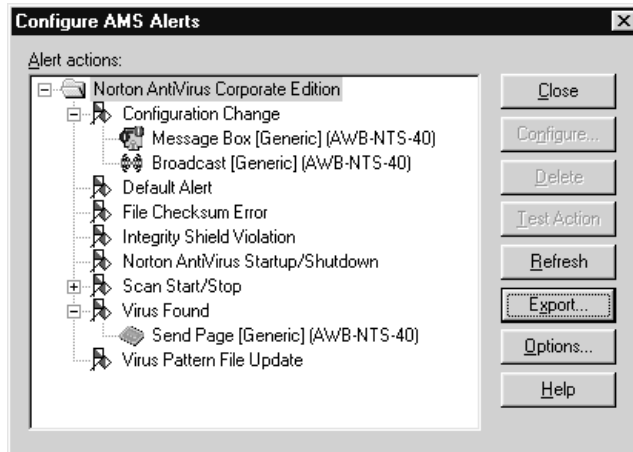
## Configuring alert actions

AMS<sup>2</sup> alert configuration requires three related tasks:

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

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

There are no default alert actions for any of the alerts. This means that until you configure AMS<sup>2</sup>, no alerts are generated, though virus events are logged in the AMS<sup>2</sup> log file.



#### To configure an alert:

- 1 From the Symantec System Center console, right-click the server group, then select All Tasks > Configure AMS.
- 2 Select an alert, then click Configure to define an alert action.

Once you've configured alert actions for an alert, a "+" or "-" sign appears next to each configured alert, depending on whether the entry is collapsed or expanded.

Each AMS<sup>2</sup> alert action has its own configuration wizard. Once you've configured an alert action, the action appears in the Alert Actions dialog box under the alert you configured the action for.

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

AMS<sup>2</sup> supports these alert actions:

- Message Box
- Broadcast
- Send Internet Mail
- Send Page

- Run Program
- Write to Windows NT Event Log
- Send SNMP Trap
- Load an NLM

## 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, such as:

- Host name
- Date
- Time
- Severity
- Alert name
- Alert value

You can enter as many as 256 characters of message text in each alert action's Message dialog. The Message dialog includes two fields. The Message field contains the text of the message you want to send. The Alert Parameters field contains any parameters you want included as message text. Parameters are delimited by "<" and ">" characters. Each parameter placeholder you add to the Message field is substituted with corresponding alert information when an alert occurs. You can click the Use Default Message option to use the default message information for this alert action.

You should test the alert actions you configure to ensure that they work as expected. For more information, see ["Testing configured alert actions"](#) on page 56 later in this chapter.

If the AMS<sup>2</sup> alerting system detects a message larger than 1 KB, the message will not be delivered. Instead, a default alert message is delivered. You can configure this default alert to notify you when a message exceeds 1 KB.

## Speeding up alert configuration with Advanced Discovery

If you have a large network, you may be able to speed up and simplify your configuration of AMS<sup>2</sup> by using the Advanced Discovery option to only search a certain segment of your network for AMS<sup>2</sup> 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 discovery process is faster when you limit your search, and alerts are contained in the defined network segment.

You can get a faster response to AMS<sup>2</sup> discovery 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<sup>2</sup> to discover clients only within a certain octet or subnet mask.

**To configure Advanced Discovery options:**

- 1 From the Symantec System Center console, right-click the server group, then select All Tasks > Configure AMS.
- 2 Click the Options button.
- 3 If you use an IPX network, enter the IPX network address where you want to search for AMS<sup>2</sup> computers in the Add IPX Net Address for Broadcast entry field.
- 4 If you use a TCP/IP network, enter the TCP/IP network address where you want to search for AMS<sup>2</sup> computers in the Add IP Broadcast Address entry field.
- 5 Click Add to add this net address to the Current Broadcast Network list. Only broadcast networks listed here are searched to discover new AMS<sup>2</sup> computers. If you have not specified any broadcast networks, the entire network is searched each time you start a discovery.
- 6 Click Remove to remove net addresses that are no longer needed from the Current Broadcast Network list. 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<sup>2</sup> from searching that section of the network for AMS<sup>2</sup> computers.
- 7 Click OK to save the Broadcast Network 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 you configure the action from. You can select whether the message box sounds a beep when it appears and whether the message box is system modal. A system modal message box prevents you from working in other programs until you acknowledge the dialog.

**To configure a Message Box alert action:**

- 1 From the Symantec System Center console, right-click the server group, then select All Tasks > Configure AMS.
- 2 Select the alert you want to configure alert actions for.
- 3 Click Configure.
- 4 Click the Message Box alert action, then click Next.
- 5 Select a computer to execute the action, then click Next.
- 6 Select whether you want an error beep and whether you want the dialog to always appear on top until it is cleared.
- 7 Click Next.
- 8 Type any message text you want to display in the Message box and move available parameters you want from the Alert Parameters list to the Message box. You can click the Use Default Message option to use the default message information for this alert action.
- 9 Enter 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 Broadcast alert action

The Broadcast alert action sends a message to everyone connected to the server that generates the alert.

**To configure the Broadcast alert action:**

- 1 From the Symantec System Center console, right-click the server group, then select All Tasks > Configure AMS.
- 2 Select the alert you want to configure alert actions for.
- 3 Click Configure.
- 4 Select the Broadcast alert action, then click Next.
- 5 Select a computer to execute the action, then click Next.
- 6 Type any message text you want to display in the Message box and move available parameters you want from the Alert Parameters list to the Message box. You can click the Use Default Message option to use the default message information for this alert action.
- 7 Enter an action name. The action name appears 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 you configure the alert action from. You must complete two fields in the Run Program dialog.

The Command Line box should contain the full path to the program you want to run and any command line options for that program. If you are running the program on a remote computer, the path you enter needs to be the path to the program from that computer. You can click the “...” button to browse for the program.

The program you select should be on the computer’s local drive to ensure that AMS<sup>2</sup> can find it.

If you’re 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 From the Symantec System Center console, right-click the server group, then select All Tasks > Configure AMS.
- 2 Select the alert you want to configure alert actions for.
- 3 Click Configure.
- 4 Click the Run Program alert action, then click Next.
- 5 Select a computer to execute the action, then click Next.
- 6 Enter a full path and command line. Click the Browse button to locate a computer. You can enter any command line options you want the program to use in the Command Line field
- 7 Select an execution state, either normal, minimized, or maximized.
- 8 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<sup>2</sup> alert occurs. You must configure this alert to determine which NLM is loaded, and the server it loads onto. This alert action is similar to the Run Program alert action for a Windows NT computer.

For example, if you were running the Norton AntiVirus Corporate Edition snap-in, you could configure the Load An NLM alert action to load an NLM on a selected NetWare server when Norton AntiVirus detects a virus. This NLM could monitor who accesses the server, and who's using the infected file, and back up files should the server crash because of the infection.

### To configure the Load An NLM alert action:

- 1 From the Symantec System Center console, right-click the server group, then select All Tasks > Configure AMS.
- 2 Select the alert you want to configure alert actions for.
- 3 Click Configure.
- 4 Click the Load An NLM alert action, then click Next.  
The first time you configure this action, AMS<sup>2</sup> needs to search the network for NetWare computers that can perform this action. When completed, the NetWare computers appear in tree format.
- 5 Click Discover.
- 6 Select the computer where the NLM will load, then click Next.
- 7 Enter the NLM to load or select it from the drop-down list. NLMs are usually stored in the SYS:SYSTEM directory on NetWare servers.
- 8 Click Finish.

## Configuring the Send Internet Mail alert action

The Send Internet Mail alert action sends an Internet mail message to the user you specify. When using the Send Internet Mail alert action, you need to also specify the SMTP Internet mail server that the alert action will send the message through. 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 don't have a DNS server, you can enter the mail server's IP address directly.

If you don't 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 From the Symantec System Center console, right-click the server group, then select All Tasks > Configure AMS.
- 2 Select the alert you want to configure alert actions for.
- 3 Click Configure.

- 4 Click the Send Internet Mail alert action, then click the Next button.
- 5 Select the computer to perform the action, then click the Next button.
- 6 Enter information in the Internet Address, Sender Name, Subject, and Mail Server fields as appropriate, or select from the drop-down lists.
- 7 Click Next.
- 8 Type any message text you need in the Message box and move available parameters you want from the Alert Parameters list to the Message box. You can click the Use Default Message option to use the default message information for this alert action.
- 9 Enter an action name. The action name appears 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 you specify. Any computer you configure a Send Page action on needs to have a modem.

You should test Send Page alert actions to ensure that they work as expected. For more information, see the [“Testing configured alert actions”](#) on page 56 section later in this chapter.

Send Page alert action configuration is divided into three parts:

- Configuring a modem for AMS<sup>2</sup> to use
- Configuring for a paging service
- Entering a pager message

The following sections describe each part of the configuration in more detail.

To configure a Send Page alert action:

- 1 From the Symantec System Center console, right-click the server group, then select All Tasks > Configure AMS.
- 2 Select the alert that you want to configure alert actions for.
- 3 Click Configure.
- 4 Click the Send Page alert action, then click Next.
- 5 Select a computer to execute the action, then click Next.

- 6 Enter the Access Telephone Number you are calling to reach the paging service. Be sure to include any numbers necessary to access an outside line from your site.
- 7 Enter the Pager ID number. Enter the password you use to access the paging service network in the Password field. If your paging service doesn't use a password, leave the Password field blank.
- 8 In the Service drop-down list, select your service type. If your paging service isn't listed, you can try one of the generic types. For more information, see ["Configuring for a paging service"](#) on page 53.
- 9 Click Next.
- 10 If you're creating a message for an alphanumeric pager, type any message text you want to display in the Message box and move available parameters you want from the Alert Parameters list to the Message box. You can click the Use Default Message option to use the default message information for this alert action.  
  
If you're creating a message for a numeric pager, you can only type numbers in the Message box.
- 11 Enter an action name. The action name appears in the Alert Actions dialog box beside this action.
- 12 Click Finish.

### Configuring a modem for AMS<sup>2</sup>

You must configure a modem for AMS<sup>2</sup> to use to contact your paging service. You need to run the modem configuration utility and select the correct COM port and modem type settings for the Send Page alert action to function correctly.

#### To configure a modem for AMS<sup>2</sup>:

- 1 Double-click the MODEMCFG.EXE modem configuration utility in the Windows Explorer to run the utility. This utility is installed on the action computer in the WINNT\SYSTEM32\AMS\_ii folder on Windows NT computers, and in the WINDOWS\SYSTEM\AMS\_ii folder on Windows 95 and 98 computers.
- 2 Select the COM port the modem uses in the Com Port drop-down list.
- 3 Select the correct modem type in the Modem Type drop-down list.
- 4 Click OK to save these settings, and your modem is configured to work with the AMS<sup>2</sup> alerting system.

## 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 their computer network directly to enter the pager identification number. The paging service network then sends the message to the pager.

AMS<sup>2</sup> 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, then sends the message to the pager. The indirect paging method 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 you're using.

Always put the paging service's phone number in the Send Page dialog's Service Provider field. If your paging service isn't in the Send Page dialog's Service drop-down list, you can try using the Generic Beeper or the Generic Alphanumeric service (pick the one that matches the type of pager you're using). Put the password you use to access the paging service network in the Password field.

If the generic service you select doesn't work with your pager, you must configure the communication parameters 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.

If you do need to configure your paging service manually, refer to the following section.

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

- 1 From the Symantec System Center console, right-click the server group, then select All Tasks > Configure AMS.
- 2 Select the alert that you want to configure alert actions for.
- 3 Click Configure.
- 4 Click the Send Page alert action, then click Next.

- 5 Select a computer to execute the action, then click Next.
- 6 Click the Settings button.
- 7 Enter the protocol, maximum message length, baud, data bits, stop bits, and parity that your paging service requires. You can get this information from your paging service.
- 8 Click OK, then continue configuring the pager action starting with step 7 in [“To configure a Send Page alert action:”](#) on page 51.

### 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 you type in and information from the alert that generated the message. This message should not exceed the maximum number of characters your paging service supports; otherwise, you could get a truncated message.

If you're paging a numeric-only pager, you can only send numbers. In this case, you may want to create a system of server numbers and numeric error codes that correspond to alerts 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<sup>2</sup> can generate an SNMP trap when an alert occurs. You can configure systems generating alerts to send these traps to an SNMP management console if you have one.

#### To configure the Send SNMP Trap alert action:

- 1 From the Symantec System Center console, right-click the server group, then select All Tasks > Configure AMS.
- 2 Select the alert you want to configure alert actions for.
- 3 Click Configure.

- 4 Click the Send SNMP Trap alert action, then click Next.
- 5 Select a computer to execute the action, then click Next.
- 6 Type any message text you want to display in the SNMP trap and move available the parameters you want from the Alert Parameters list to the Message box. You can click the Use Default Message option to use the default message information for this alert action.
- 7 Enter an action name. The action name appears in the Alert Actions dialog box beside this action.
- 8 Click Finish.

## Configuring SNMP trap destinations

You must specify the address (either IP or IPX) of the computers that you want SNMP traps sent to. The following sections describe configuring trap destinations for the operating systems that Symantec System Center supports.

### To configure trap destinations for Windows NT 4.0:

- 1 From the Windows NT Control Panel, double-click the Network icon.
- 2 Click Services.
- 3 Select the SNMP Service item, then click Properties.
- 4 Click Traps.
- 5 In the Community Name drop-down list box, select Public. If there's no public entry in the list, type it in, then click Add.
- 6 Once you've selected the Public community name, click Add below the Trap Destinations list.
- 7 Enter the addresses of the computers you want traps sent to, then click Add.
- 8 Click OK > Close.

### To configure trap destinations for NetWare 4.1x and 5.x servers:

- 1 From the NetWare server console, type:  

```
load inetcfg
```
- 2 Click Protocols.
- 3 Click TCP/IP.
- 4 Click SNMP Manager Table.
- 5 Press the INS key to add the address.

- 6 Enter the addresses of the computers you want traps sent to, then click Add.

## Configuring the Write To Event Log alert action

The Write to Event Log alert action creates an entry in the Windows NT Event Log's Application Log. This entry is logged on the server where the alert came from. This alert action is available only on Windows NT computers.

To configure the Write To Event Log alert action:

- 1 From the Symantec System Center console, right-click the server group, then select All Tasks > Configure AMS.
- 2 Select the alert you want to configure alert actions for.
- 3 Click Configure.
- 4 Click the Write To Event Log alert action, then click Next.
- 5 Select a computer to execute the action, then click Next.
- 6 Type any message text you want to display in the Message box and move available parameters you want from the Alert Parameters list to the Message box. You can click the Use Default Message option to use the default message information for this alert action.
- 7 Enter an action name. The action name appears in the Alert Actions dialog box beside this action.
- 8 Click Finish.

## Working with configured alerts

Once you've configured alert actions, you can:

- 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, all alert actions configured for that alert execute. When you select a specific alert action and click Test, only that alert action executes.

To test an alert:

- Click an alert, then click Test.

To delete an alert action from an alert:

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

## Exporting alert actions to other computers

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

There may be times when you want to duplicate configurations of AMS<sup>2</sup> alert actions on a computer across multiple computers so you don't have to repeat your work. The AMS<sup>2</sup> export option lets you export alert actions to other computers that generate AMS<sup>2</sup> alerts.

Alert actions, such as a Send Page alert action configuration or a Message Box alert action configuration, only export if the alert you configured the action for 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<sup>2</sup> 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. By selecting an alert in the Alert Actions dialog box and clicking the Export button, AMS<sup>2</sup> attempts to export all alert actions in its database. By selecting a single alert action in the Manage AMS Alerts dialog and clicking the Export button, AMS<sup>2</sup> only exports the selected alert action. Once AMS<sup>2</sup> exports alert actions to a computer, AMS<sup>2</sup> displays the Export Status dialog to let you know the results of the export.

If the export option can't export an alert action because the alert the action was configured for doesn't exist on the target computer (or for any other reason), the Export Status dialog indicates that the alert action couldn't be exported. Alert actions also may fail to export if the target computer's AMS<sup>2</sup> installation isn't working correctly.

### To export alert actions to other computers:

- 1 From the Symantec System Center console, right-click the server group, then select All Tasks > Configure AMS.
- 2 Select either an alert (if you want to export all of that computer's AMS<sup>2</sup> alert actions) or a specific alert action (if you want to export only the selected alert action).
- 3 Click Export.
- 4 In the Select Computers dialog, select the computers that you want to receive the alert actions you selected. If the computer you want has AMS<sup>2</sup> active on it and it isn't in the Available Computers list, click Refresh to rediscover computers with AMS<sup>2</sup>.
- 5 Select whether you want to export all actions for all alerts or the action you selected in the Alert Actions dialog box.
- 6 Click Export.
- 7 In Export Status dialog, verify that the alert actions exported successfully.

### Viewing export status

After AMS<sup>2</sup> exports alert actions to the computers you selected in the Select Computers dialog, AMS<sup>2</sup> displays the export results in the Export Status dialog. This dialog displays alert actions that don't export successfully. If alerts don't export successfully, it can be for a couple of reasons:

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

## Using the Alert Management System<sup>2</sup> Alert Log

You can use the Alert Log to view a list of all alerts generated by network computers running the Norton AntiVirus Corporate Edition snap-ins. You can configure the Alert Log to:

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

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

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

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

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 isn't powered on or available, you won't be able to retrieve its Alert Log for viewing.

If you configure a threshold for certain events without configuring AMS<sup>2</sup> alert actions, the AMS<sup>2</sup> Alert Log still records the alert.

**To view the Alert Log:**

- Right-click the server group, then select All Tasks > View AMS Log.

**To change the number of entries displayed in the Alert Log:**

- 1 Right-click in the Alert Log window, then click Options.
- 2 In the Maximum Entries text box, specify the number of log entries you want the log to hold.

---

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

---

**To delete Alert Log entries**

**To delete a single log entry:**

- Right-click the log entry you want to delete, then click Selected Entries.

**To delete multiple log entries:**

- 1 Press the Ctrl key and select the multiple log entries.
- 2 Right-click in the Alert Log window, then click Selected Entries.

To delete all visible log entries:

- Right-click in the Alert Log window, then click Delete > Filtered Entries.

To copy Alert Log contents to the clipboard:

- 1 Adjust the log filters so that only the entries you want to copy are visible in the log.
- 2 Right-click in the Alert Log window, then click Copy.

---

**Note:** Only the alerts visible in the log are copied. If you want to limit the number of entries 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 the Alert Log displays. The Alert Information dialog displays the detailed information and includes alerts, their values, and the action status of each alert.

The Alert Information dialog displays this information:

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 field can include Pending, Processing Action, Error, Completed Successfully, and Failed To Complete.

To view the alert information and Action Status:

- 1 From the Alert Log window, double-click the alert that you want to display detailed information for.
- 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 you want more information about. The Alert Information window 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 these parameters:

Filter	Description
Computer	Display alerts from a specific computer.
Source	Display alerts from the same type of alert source (such as Windows NT Performance Monitor) on one or more computers.
Alert	Displays all alerts with a specific alert name.
Severity	Displays only alerts matching the severity levels you select. You can specify the following severity levels: Monitor, Information, OK, Non Critical, Critical, and Non Recover.

### To specify which alerts display in the Alert Log:

- 1 From the Symantec System Center console, right-click the server group, then select All Tasks > Norton AntiVirus > View AMS Log.
- 2 Right-click in the Alert Log window, then click the Options button.
- 3 Select the filters you want to apply to the Alert Log list.
- 4 Click OK.

# Alert Management System<sup>2</sup> Services

The following Windows NT services are associated with the Alert Management System<sup>2</sup>:

HNDLRSVC.EXE	Alert Handler Service
PDS.EXE	Server Group Service
XFR.EXE	File Transfer Service

# Symantec System Center Troubleshooting

This chapter provides you with information related to troubleshooting the two main Symantec System Center components, the console and Alert Management System<sup>2</sup>.

## Seeing servers and clients from the Symantec System Center console

If you cannot see all of the servers and clients that you would expect to see in the Symantec System Center console, you can run Intense Discovery. [“Finding machines and refreshing the console”](#) on page 32 for a complete description of the options available for discovering servers and clients and adding them to your console view.

## Alert Management System<sup>2</sup>

AMS<sup>2</sup> lets you configure many different methods of notification for detected viruses, including pager, SNMP, and email. Norton AntiVirus also has built-in notification capabilities that you can use instead of or in addition to the AMS<sup>2</sup> notification. For more information, see [“Should I use Alert Management System<sup>2</sup>?”](#) on page 44.

## I have installed the Alert Management System<sup>2</sup> console but cannot configure alerts

You must install both AMS<sup>2</sup> console and AMS<sup>2</sup> services. For information about installing AMS<sup>2</sup> services, see “Rolling out Norton AntiVirus Corporate Edition for servers” in Chapter 2 of the *Norton AntiVirus Corporate Edition Implementation Guide*.

## My modem doesn't work with Alert Management System<sup>2</sup>

If you use the Send Page alert action, the action computer that sends the pager message must have these items:

- An installed version of AMS<sup>2</sup>
- Access to a phone line to contact your paging service
- A modem configured for AMS<sup>2</sup>

Even if the modem works for other applications, you must configure your modem for AMS<sup>2</sup>. Run the modem configuration utility (MODEMCFG.EXE). This utility configures your modem to work with AMS<sup>2</sup> and transmit AMS<sup>2</sup> messages.

## Computer doesn't appear in the Select Action Computer list

Action computers are computers running AMS<sup>2</sup> alert handlers. If you have a computer running AMS<sup>2</sup>, you should be able to send alert actions to that computer. Keep in mind, however, that some alert actions may not be available on all computers. For example, you can't send a pager message from a computer that doesn't have a configured modem. If AMS<sup>2</sup> doesn't detect a modem on the computer, it won't display that computer as available for Send Page alert actions.

If a computer running AMS<sup>2</sup> doesn't appear in the Select Action Computer list, try one of the following:

- Click Refresh to force AMS<sup>2</sup> to search the network again for AMS<sup>2</sup> computers.
- If you can't locate a specific action computer because it's hidden behind a router, you can add the computer's TCP/IP or IPX address to the Current Broadcast Addresses list in this dialog. The discovery process can then locate that computer, and it will display in the Action Computers list.

You can also use the Advanced Discovery option to search only segments of the network for AMS<sup>2</sup> computers. You can select octets or subnets to search for AMS<sup>2</sup> computers. Broadcast alert action messages are confined to the limits you set.

## **AMS alert configuration is lost when you change primary servers**

When changing primary servers, you will lose all of the AMS alerts you've set up. You can reconfigure the alerts on the new primary server.

## **Alerts not received in Symantec System Center console**

If you stop receiving notifications in the Symantec System Center, expand and refresh the server group where you would expect to receive an alert.





# Symantec Service and Support Solutions

Symantec is committed to excellent service worldwide. Our goal is to provide you with professional assistance in the use of our software and services, wherever you are located.

Technical Support and Customer Service solutions vary by country. If you have questions about the services described below, please refer to the section “Worldwide Service and Support” at the end of this chapter.

## Registering your Symantec product

Visit the Symantec web site at:

<http://www.symantec.com>

and choose Register Your Software under Service and Support.

## Technical support

Symantec offers an array of technical support options designed for your individual needs to help you get the most out of your software investment.

## World Wide Web

The Symantec World Wide Web site (<http://service.symantec.com>) is the portal to an array of customer-centered solutions. These solutions include the services listed below.

## Product knowledge bases

Product knowledge bases enable you to search thousands of documents used by Symantec Support Technicians to answer customer questions.

## Ask Symantec

Ask Symantec discussion groups provide a forum where you can ask questions and receive answers from Symantec online Customer and Technical Support Specialists.

## File downloads

Point your web browser to <http://service.symantec.com> to search for and download technical notes and software updates. You can also click the LiveUpdate button in programs enabled with this feature to automatically download and install software updates and virus definitions.

## Other technical support options

Other Symantec support options include the following:

**Automated fax retrieval system** To receive general product information, fact sheets and product upgrade order forms directly to your fax machine, please call our Customer Service fax retrieval system at (800) 554-4403 or (541) 984-2490.

For technical application notes, please call our Technical Support fax retrieval system at (541) 984-2490 and select option 2.

**GoldCare Support** Site license version of your Norton AntiVirus Enterprise Solution software include Symantec Helpdesk Gold Support for one year. With this support your organization's designated support contact will call Symantec for corporate technical support on a priority, toll-free telephone number.

**PlatinumCare Support** PlatinumCare Support provides Symantec corporate customers with our highest level of technical support. Your organization's designated support contact will receive features such as unlimited toll-free calls, extended hours of operation, access to our most senior technical analysts, access to a secure PlatinumCare web site, plus much more. For complete information, please visit the Symantec web site at:

<http://www.symantec.com/platinum/>

or call your Symantec Sales representative.

## Other Telephone Support

Other telephone support services are available to registered customers. Please see the back of this manual for telephone support numbers.

## Support for old and discontinued versions

When a new version of this software is released, registered users will automatically receive the new version during the first year as part of their site license. After the first year, registered user will receive upgrade information in the mail. Telephone support will be provided for the previous version for up to six months after the release of the new version. Technical information may still be available through online support.

When Symantec announces that a product will no longer be marketed or sold, telephone support will be discontinued up to one year later. Support will only be available for discontinued products through online services. See the section "Technical support" for online service options.

## Customer Service

You can contact Customer Service online at:

<http://service.symantec.com/>

Customer Service can assist you with non-technical questions, such as:

- Subscribing to the Symantec Support Solution of your choice.
- Obtaining product literature or trialware.
- Locating resellers and consultants in your area.

- Replacing missing or defective CD-ROMs, disks, manuals, and so on.
- Updating your product registration with address or name changes.
- Getting order, return, or rebate status information.
- Accessing Frequently Asked Questions, or FAQs.
- Posting questions to the Customer Service newsgroup.

You can also call Customer Service at (800) 441-7234.

## Upgrade Orders

For upgrade orders after the first year, please call the Customer Service Order Desk at (800) 568-9501.

Or, you can visit the upgrade center online at:

<http://www.symantec.com/upgrades/>

## Worldwide Service and Support

Symantec provides Technical Support and Customer Service worldwide. Services vary by country and include International Partners who represent Symantec in regions without a Symantec office. For general information, please contact the Symantec Service and Support Office for your region. Or, you can get more information at <http://www.symantec.com/>.

## Service and Support offices

### **NORTH AMERICA**

Symantec Corporation  
175 W. Broadway  
Eugene, OR 97401

<http://www.symantec.com/>

(800) 441-7234 (USA & Canada)  
(541) 334-6054 (all other locations)  
Fax: (541) 984-8020

Automated Fax Retrieval

(800) 554-4403  
(541) 984-2490

**EUROPE, MIDDLE EAST, AFRICA**

Symantec Customer Service Center  
P.O. Box 5689  
Dublin 15  
Ireland

[http://www.symantec.com/region/reg\\_eu/](http://www.symantec.com/region/reg_eu/)  
+353 (1) 811 8032  
Fax: +353 (1) 811 8033

Automated Fax Retrieval +31 (71) 408 3782

**ASIA/PACIFIC RIM**

Symantec Australia Pty. Ltd.  
408 Victoria Road  
Gladesville, NSW 2111  
Australia

[http://www.symantec.com/region/reg\\_ap/](http://www.symantec.com/region/reg_ap/)  
+61 (2) 9850 1000  
Fax: +61 (2) 9850 1001

Automated Fax Retrieval +61 (2) 9817 4550

**LATIN AMERICA**

Symantec América Latina  
Oficina principal  
2500 Broadway, Suite 200  
Santa Monica, CA 90404

<http://www.symantec.com/region/mx/>  
(310) 449-7086  
Fax: (310) 449-7576

**BRAZIL**

Symantec Brazil  
Av. Juruca, 302 - cj 11  
São Paulo - SP  
04080 011  
Brazil

<http://www.symantec.com/region/br/>  
+55 (11) 5561 0284  
Fax: +55 (11) 5530 8869

Most International Partners provide Customer Service and Technical Support for Symantec products in your local language. For more information on other Symantec and International Partner locations, please call our Technical Support automated fax retrieval service, in the United States at +1 (541) 984-2490, choose Option 2, and request document 1400.

Every effort has been made to ensure the accuracy of this information. However, the information contained herein is subject to change without notice. Symantec Corporation reserves the right for such change without prior notice.



# Norton AntiVirus Enterprise Solution

## CD Replacement Form

**CD REPLACEMENT:** If your CD becomes unusable, fill out and return 1) this form, 2) your damaged CD, and 3) your payment (see pricing below, add sales tax if applicable), to the address below to receive replacement CD. You must be a registered customer in order to receive CD replacements.

### FOR CD REPLACEMENT

Please send me:  CD Replacement

Name \_\_\_\_\_

Company Name \_\_\_\_\_

Street Address (No P.O. Boxes, Please) \_\_\_\_\_

City \_\_\_\_\_ State \_\_\_\_\_ Zip/Postal Code \_\_\_\_\_

Country\* \_\_\_\_\_ Daytime Phone \_\_\_\_\_

Software Purchase Date \_\_\_\_\_

\*This offer limited to U.S., Canada, and Mexico. Outside North America, contact your local Symantec office or distributor.

Briefly describe the problem: \_\_\_\_\_

CD Replacement Price \$ 10.00  
Sales Tax (See Table) \_\_\_\_\_  
Shipping & Handling \$ 9.95  
TOTAL DUE \_\_\_\_\_

SALES TAX TABLE: AZ (5%), CA (7.25%), CO (3%), CT (6%), DC (5.75%), FL (6%), GA (4%), IA (5%), IL (6.25%), IN (5%), KS (4.9%), LA (4%), MA (5%), MD (5%), ME (6%), MI (6%), MN (6.5%), MO (4.225%), NC (6%), NJ (6%), NY (4%), OH (5%), OK (4.5%), PA (6%), SC (5%), TN (6%), TX (6.25%), VA (4.5%), WA (6.5%), WI (5%). Please add local sales tax (as well as state sales tax) in AZ, CA, FL, GA, MO, NY, OH, OK, SC, TN, TX, WA, WI.

### FORM OF PAYMENT \*\* (CHECK ONE):

Check (Payable to Symantec) Amount Enclosed \$ \_\_\_\_\_  Visa  Mastercard  American Express

Credit Card Number \_\_\_\_\_ Expires \_\_\_\_\_

Name on Card (please print) \_\_\_\_\_ Signature \_\_\_\_\_

**\*\*U.S. Dollars. Payment must be made in U.S. dollars drawn on a U.S. bank.**

### MAIL YOUR CD REPLACEMENT ORDER TO:

Symantec Corporation  
Attention: Order Processing  
175 West Broadway  
Eugene, OR 97401-3003 (800) 441-7234

**Please allow 2-3 weeks for delivery within the U.S.**

Symantec and Norton SystemWorks are trademarks of Symantec Corporation.  
Other brands and products are trademarks of their respective holder/s.  
© 1998 Symantec Corporation. All rights reserved. Printed in the U.S.A.

**SYMANTEC**™



# I N D E X

## A

- administering Windows NT and NetWare servers 13
- advanced discovery 46
- alert actions 44
  - configuring
    - Broadcast 48
    - Load NLM 49
    - Message Box 47
    - messages 46
    - modem for 52
    - paging services for 54
    - Run Program 49
    - Send Internet Mail 50
    - Send Page 51
    - Write to Event Log 55
  - exporting to other computers 57
  - limiting to certain network segments 46
  - supported types 45
  - testing 56
  - viewing the Alert Log 58
- alert configuration, speeding up with Advanced Discovery 46
- Alert Log
  - copying contents to clipboard 60
  - deleting entries 59
  - displaying alerts in 58
  - filtering display list 61
  - viewing detailed information 60
- Alert Management System
  - alerting methods 11
  - overview 11
  - What is Alert Management System? 43

## B

- Broadcast alert, configuring 48

## C

- cache, discovering machines from 33

- cached server group passwords 40
- configuring
  - alert actions 44
  - alerts 13
  - clients remotely 13
  - for a paging service 53
  - modems for Alert Management System 52
- configuring SNMP traps 55
- console views 30
- copying Alert Log contents to clipboard 60

## D

- deleting Alert Log entries 59
- discovering machines 32
- Discovery Service, running 32
- discovery, advanced 46

## E

- exporting alert actions to other computers 57

## F

- filtering
  - Alert Log display list 61
  - server group view in the console 37
- finding machines 32
  - locating found items in the console 35

## G

- grouping servers into server groups 37

## H

- hardware requirements 25

---

## I

- icons, Symantec System Center console 30
- installation
  - locating servers 26
  - options 25
  - planning 20
  - products you don't need to uninstall 21
  - rights to installation to Windows NT servers 27
  - uninstalling Symantec System Center 28
  - verifying network access and privileges 26
  - what the installation program does 25
  - Windows NT reboot may be required 26
  - worksheet 25
- intense discovery 33
- IP and IPX protocol usage 21

## L

- Load NLM alert
  - configuring 49
- local discovery 33
- locking server group 39

## M

- master primary server 17
- Message Box alert
  - configuring 47
- Microsoft Management Console 10
- modems, configuring for Alert Management System 52
- moving servers from one server group to another 15

## N

- network traffic
  - client 23, 24
  - planning for 22
  - server-to-server 23
- networks, what you can see and do on networks other than indows NT and NetWare 25

## O

- operating systems supported 17

## P

- pager message, entering 54
- paging services
  - configuring for AMS 54
- planning
  - alert management 24
  - management policy 24
  - Symantec System Center installation 20
- primary server 17
  - choosing for a server group 38
- protocols
  - how Symantec System Center uses IP and IPX 21
  - supported by Symantec System Center 17

## R

- refreshing the console 36
- remotely configuring clients 13
- requirements, hardware and software 25
- Run Program alert
  - configuring 49

## S

- secondary server 17
- Send Internet Mail alert
  - configuring 50
- Send Page alert
  - configuring 51
  - configuring paging service 53
- server group 14
  - choosing primary server 38
  - compared to Virus Protect and Norton AntiVirus domains 15
  - creating 38
  - deleting 38
  - discovering servers and clients 30
  - filtering views 37
  - grouping servers 37
  - how to see server groups 15
  - locking 24, 40
  - locking and unlocking 39
  - managing 36
  - refreshing the console 36
  - renaming 38
  - seeing in the console 37

---

server group (*continued*)  
    unlocking 40  
server types 17  
SNMP traps, configuring 55  
starting the Symantec System Center console 30  
Symantec System Center  
    administering Windows NT and NetWare  
        servers with 13  
    components 17  
    finding and discovering machines with 32  
    how it works 12  
    installing 19  
    Microsoft Management Console  
        requirement 10  
    operating systems supported 17  
    planning your installation 20  
    protocols supported 17  
    remotely configuring clients 13  
    requirements 25  
    server groups 37  
    understanding installation options 25  
    using to manage Symantec products 12  
Symantec System Center console  
    starting 30  
    tasks you can perform with 10  
system requirements 25

## **W**

Write to Event Log alert  
    configuring 55

## **T**

testing alert actions 56  
traps, configuring 55  
troubleshooting 63

## **U**

uninstalling 28  
unlocking server group 39

## **V**

viewing  
    export status 58  
    servers in the console 36  
views  
    changing 30  
    displayable in console 30

