



Product Bulletin No. 3502

Using Symantec Norton AntiVirus with Cisco Unified CallManager

INTRODUCTION

Windows 2000 servers should have virus protection, and the Cisco[®] Unified CallManager is no exception. Although the installation and configuration of Symantec Norton AntiVirus is very easy, a few important steps need to be taken. This document provides information about the installation and configuration of Symantec and Norton AntiVirus on the Cisco Unified CallManager platform (including the newest Norton AntiVirus Corporate Edition Version 7.61 and Symantec AntiVirus Corporate Edition 10.1.4.4000).

This paper provides a detailed description of the Symantec AntiVirus for use on Cisco CallManager Version 3.3(0) and Cisco Unified CallManager Versions 4.1(0), and 4.2(0). It describes the need for the product, a description of the product, and product features and functions.

SYMANTEC PRODUCT OVERVIEW

Symantec AntiVirus provides comprehensive virus prevention, detection, and elimination for your computer. It automatically finds and repairs infected files to keep your data secure.

CISCO SYSTEMS SUPPORT POLICY

Cisco Systems[®] makes no warranty or claims as to the accuracy or completeness of this document. Furthermore, the Cisco Technical Assistance Center (TAC) is not responsible for supporting this integrated solution.

Note: This statement is included in documentation until the product passes interoperability verification testing [IVT] and coordinated support is in place.

PERFORMANCE

Testing indicated the following:

1. Symantec active virus scans do not add any CPU memory overhead.
2. Drive scanning takes up a lot of CPU and is not recommended during call processing.
3. Virus updates use little CPU, so they can be scheduled to run during low traffic.

REQUIRED HARDWARE AND SOFTWARE LEVELS

Cisco hardware levels are not a concern of Symantec AntiVirus; please refer to the hardware requirements section of the Symantec documentation. Following are the tested Cisco CallManager and Cisco Unified CallManager software levels; please refer to this list for all supported Cisco CallManager and Cisco Unified CallManager versions:

- Norton AntiVirus Corporate Edition Version 7.61 with Cisco CallManager Version 3.2(2c) to 3.3(3)
- Symantec AntiVirus Corporate Edition Version 8.0 with Cisco CallManager Version 3.2(2c) to 3.3(3)
- Symantec AntiVirus Corporate Edition Version 8.1 with Cisco CallManager Version 3.2(2c) to Cisco Unified CallManager Version 4.0(0)

- Symantec AntiVirus Corporate Edition Version 9.0 with Cisco CallManager Version 3.3(4) to Cisco Unified CallManager Version 4.1(0)
- Symantec AntiVirus Corporate Edition Version 10.0 with Cisco CallManager Version 3.3(5)
- Symantec AntiVirus Corporate Edition Version 10.1 with Cisco Unified CallManager Version 4.2(0)

INSTALLATION

Installing the Symantec AntiVirus Corporate Edition Client

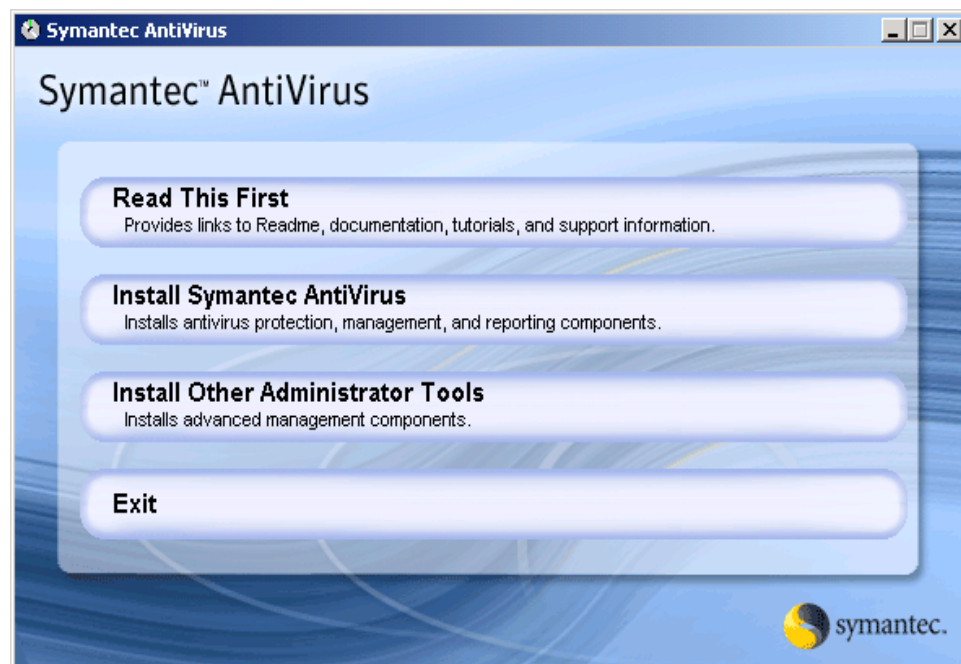
To install the Symantec AntiVirus Corporate Edition client, complete the following:

- Start the installation.
- Run the client setup program.

To start the installation:

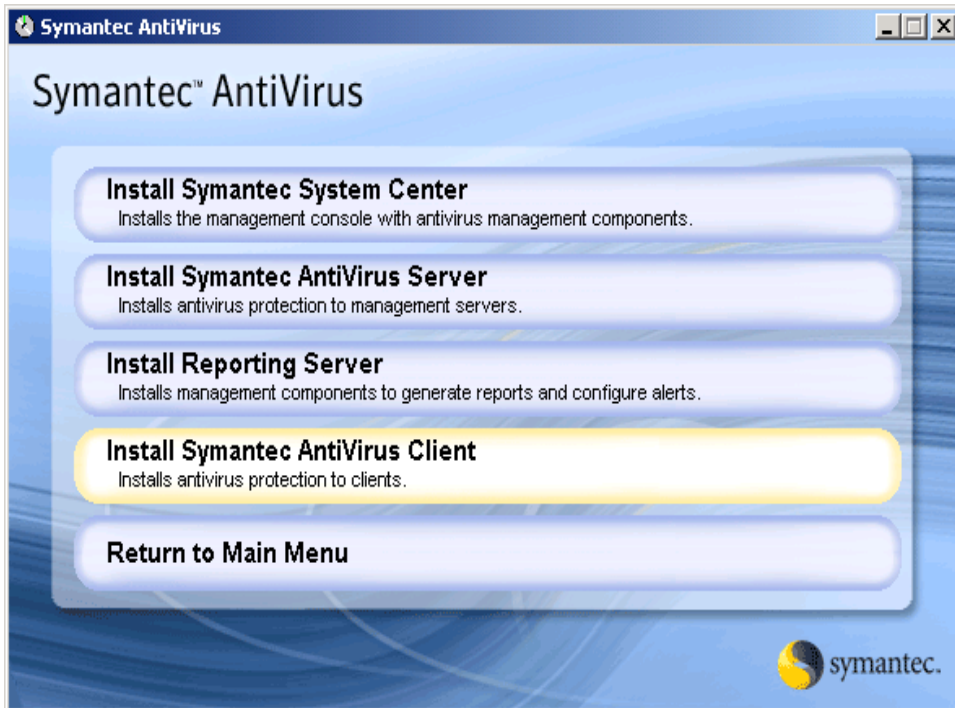
1. Insert the CD into your CD-ROM drive.
2. Double-click My Computer.
3. Double-click your Compact Disc drive.
4. Double-click the Setup.exe folder.
5. Click Install Symantec AntiVirus (Figure 1).

Figure 1. Symantec AntiVirus Window



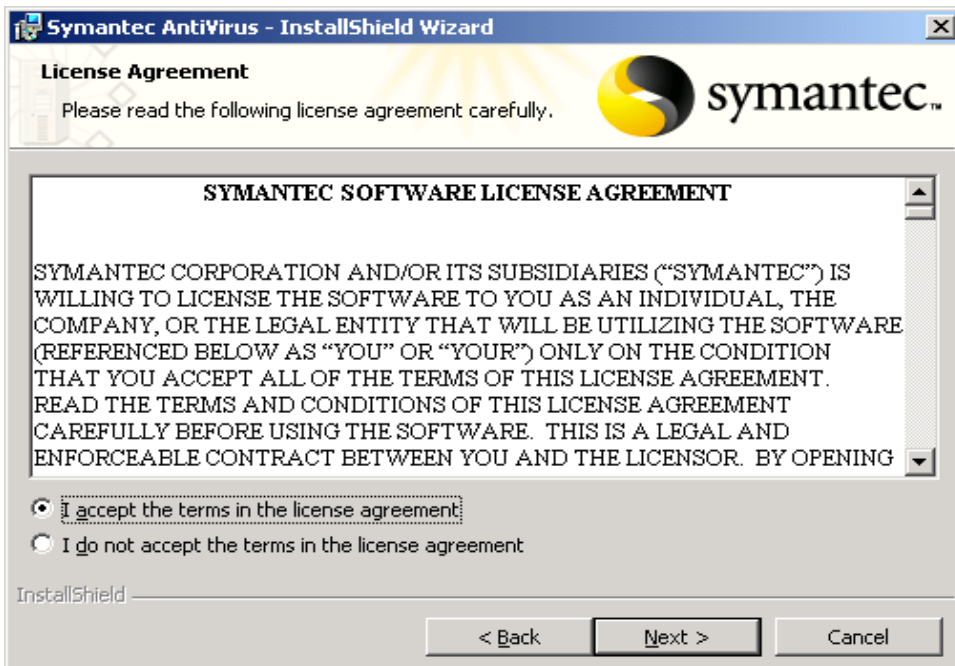
6. Click Install Symantec AntiVirus Client (Figure 2).

Figure 2. Symantec AntiVirus Client Installation



7. Click Next (Figure 3).

Figure 3. Symantec AntiVirus InstallShield Wizard



8. Accept the License Agreement and Click Next
9. Now select the Setup Type as “Complete” and Click Next (Figure 4).

Figure 4. Symantec AntiVirus Setup Type



10. Select the Network Setup Type as “Managed” and Click Next (Figure 5).

Figure 5. Network Setup Type



11. Enter the Symantec AntiVirus Server Name and Click Next (Figure 6).

Figure 6. Selecting Symantec AntiVirus Server Name



12. Click Install (Figure 7).

Figure 7. Installing Symantec AntiVirus

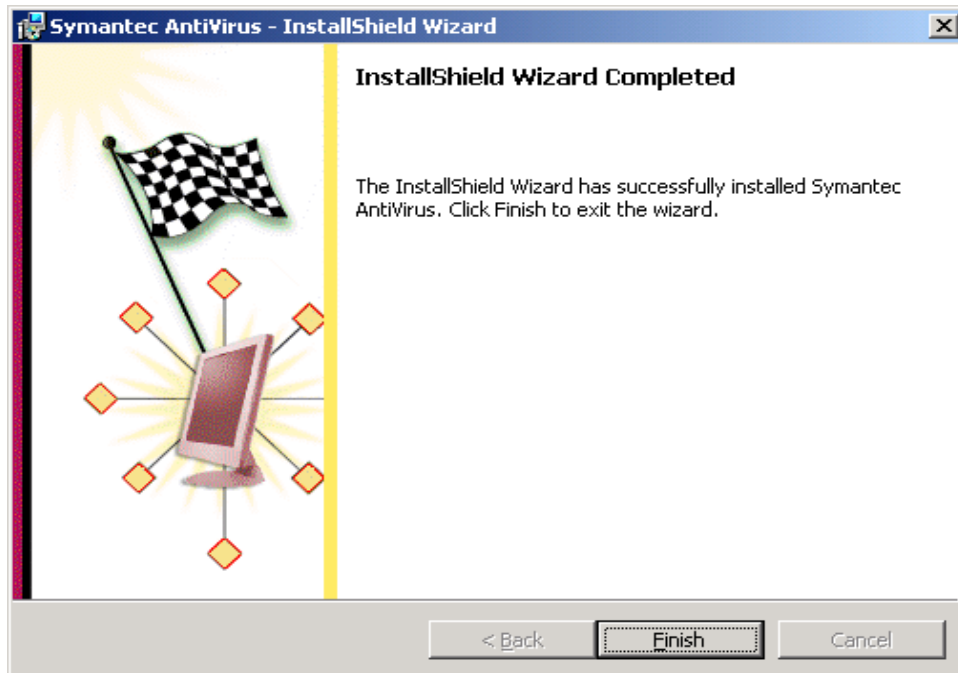


13. When the installation (Figure 8) is completed, click Finish (Figure 9).

Figure 8. Symantec AntiVirus Installation

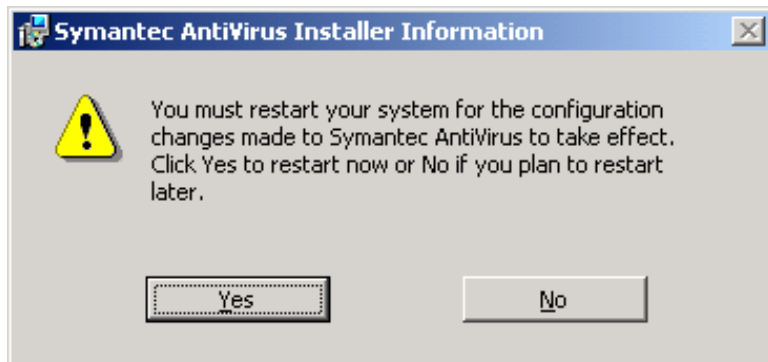


Figure 9. Installation Complete



14. When installation is finished, it will prompt you to restart (Figure 10).

Figure 10. Installer Information Screen Shot



CONFIGURATION

For normal operation on Cisco CallManager 3.0, the default settings for Symantec AntiVirus are fine. There are two important considerations, however.

Scheduled File Scanning Can Negatively Affect the Server

There is a difference between the protection Symantec AntiVirus offers by running in the background and scheduled file scanning of the entire directory structure. Scheduled file scanning is very processor-intensive, and it can affect call processing if it occurs during high-volume traffic. Therefore, it is critical to schedule a complete file scan only during the middle of the night or other nonpeak times.

Known Symantec and Windows Problem

There is a known problem with Symantec and Windows NT, 2000, and XP that could cause the server to restart or blue screen. This problem is usually seen when using Terminal Services to access the server because of a problem with Windows Kernel consumption when Symantec is scanning files. This problem can be avoided by editing a registry key. Use extreme caution in editing Windows registry, because incorrect changes to the registry could result in permanent data loss or damaged files. Modify only the key that is specified:

1. Click Start>Run.
2. Run Regedit.exe to open the Windows registry.
3. Browse to the registry key:
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Norton AntiVirus NT\Auto-Protect\InternalSettings
4. With InternalSettings highlighted, pull down New, and choose DWORD value.
5. Type KStackMinFree as the new DWORD value.
6. Right-click the KStackMinFree value, and then click Modify. Set the Base to Hexadecimal, and type 2200 in the Value data field.

To restart the antivirus service:

1. Click Start>Program>Administrative Tools>Services.
2. Locate the Symantec AntiVirus service.
3. Stop and then restart the antivirus service.

Changes to the KStackMinFree value take effect after the service is restarted.

Disable Antivirus Software During Cisco CallManager Installations and Upgrades

During the installation of Cisco CallManager or an upgrade of Cisco CallManager or Cisco Unified CallManager, you will be prompted to disable antivirus software prior to continuing. You can disable antivirus software by right-clicking the Symantec icon in the task bar and disabling the virus scan software.

UNINSTALLATION

Uninstalling Symantec AntiVirus

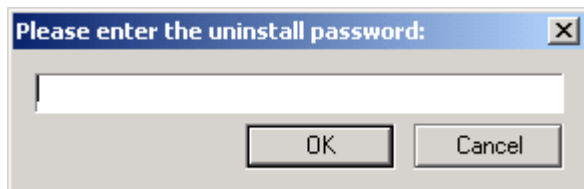
If you need to remove Symantec AntiVirus from your computer, you can use the Add/Remove Programs option from the Windows Control Panel or the Uninstall Symantec AntiVirus option from the Programs menu.

During uninstall, Windows may indicate that it is installing software. This is a standard Microsoft installation message and can be disregarded.

To uninstall Symantec AntiVirus from the Windows Control Panel:

1. On the Windows taskbar, click Start > Settings > Control Panel.
2. In the Control Panel, double-click Add/Remove Programs.
3. In the list of currently installed programs, click Symantec AntiVirus.
4. In Windows 2000, click Remove.
5. Click Yes to confirm that you want to uninstall the product.
6. Enter the Symantec AntiVirus Server console password (Figure 11).

Figure 11. Uninstall Password Window



7. If you are prompted for a restart, then restart the server.



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco.com Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic
Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy
Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2006 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

Printed in USA

C25-353461-01 09/06