

Using Symantec AntiVirus Corporate Edition Workstations and Servers 10.2 with Cisco Media Experience Engine MXE 3000

INTRODUCTION

Windows 2003 servers should have virus protection, and the Cisco® Media Experience Engine 3000 (Cisco MXE 3000) is no exception. Although the installation and configuration of Symantec AntiVirus Corporate Edition Workstations and Servers 10.2 is easy, a few important steps need to be taken. This document provides information about the installation and configuration of Symantec AntiVirus Corporate Edition Workstations and Servers 10.2 on the Cisco MXE 3000.

This paper provides a detailed description of the Symantec AntiVirus Corporate Edition Workstations and Servers 10.2 for use on Cisco MXE 3000 Release 2.0.0. It describes the need for the product, a description of the product, and product features and functions.

SYMANTEC PRODUCT OVERVIEW

Symantec AntiVirus Corporate Edition Workstations and Servers 10.2 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 Symantec AntiVirus Corporate Edition Workstations and Servers 10.2.

PERFORMANCE

Testing indicated the following:

1. Symantec AntiVirus Corporate Edition Workstations and Servers 10.2 active virus scans do not add any CPU memory overhead.
2. Drive scanning takes up a lot of CPU and is not recommended during video 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 Corporate Edition Workstations and Servers 10.2; please refer to the hardware requirements section of the Symantec documentation. Symantec AntiVirus Corporate Edition Workstations and Servers 10.2 is tested with Cisco MXE 3000 Release 2.0.0 software.

INSTALLATION

Before You Begin

Symantec AntiVirus Corporate Edition Workstations and Servers 10.2 can be deployed in various configurations. Please refer to Symantec documentation for more details. The steps described here assume that a Symantec AntiVirus Server has already been deployed and configured and only describe what is required to install Symantec AntiVirus Corporate Edition client on Cisco MXE 3000.

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.

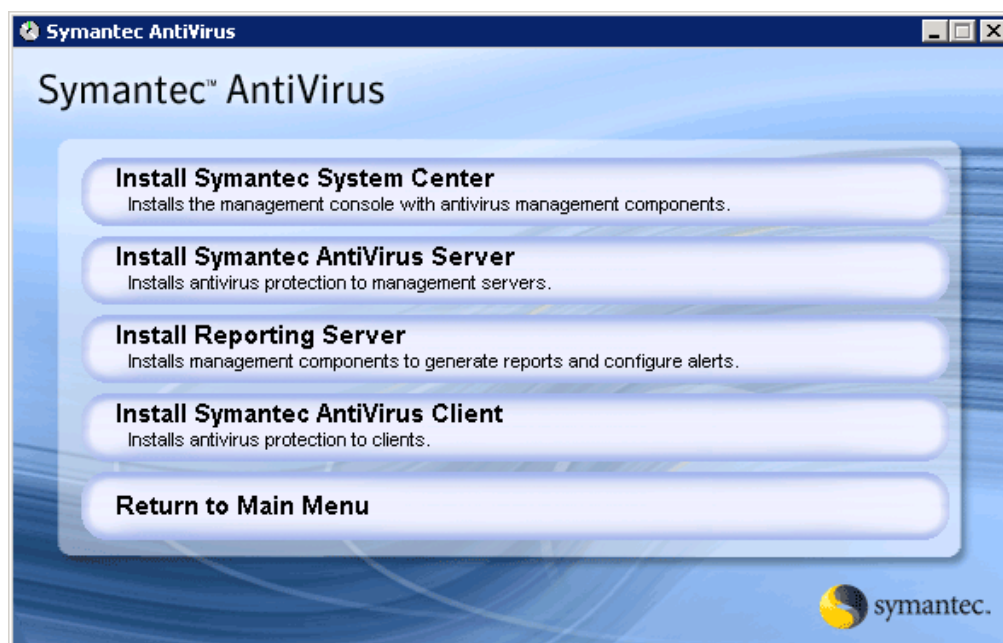
To start the installation:

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

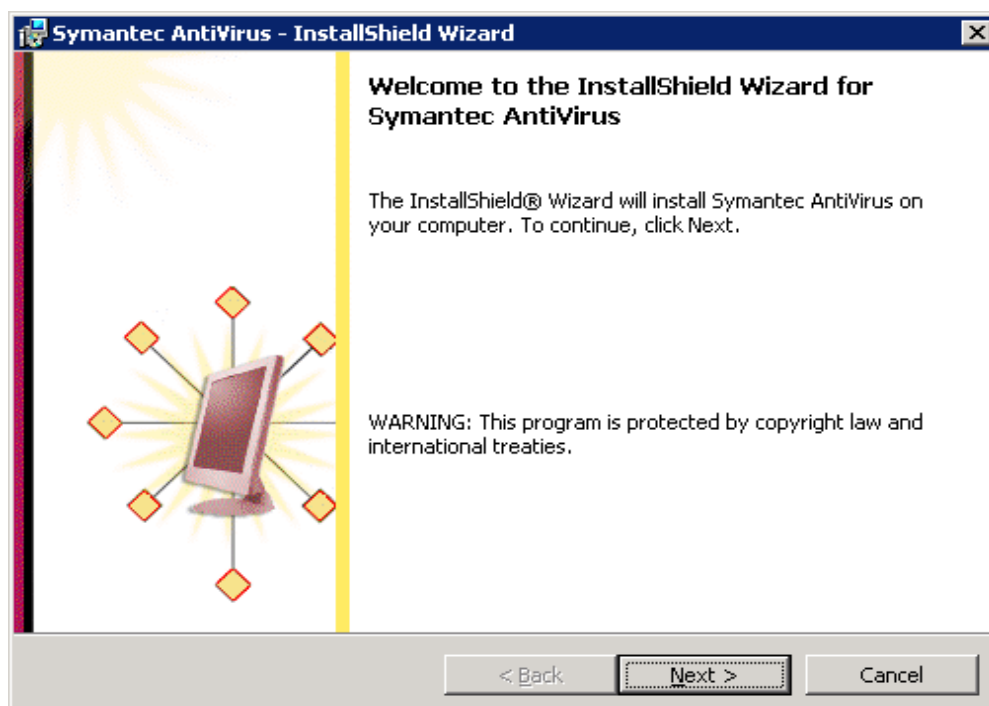
Figure 1. Symantec AntiVirus Window



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

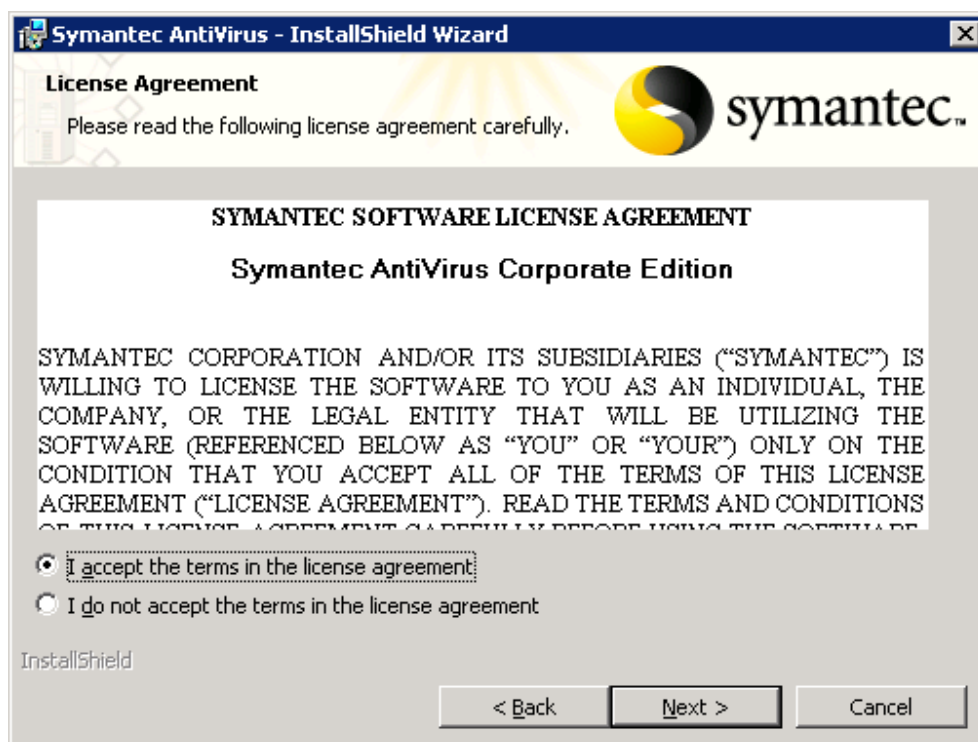
Figure 2. Symantec AntiVirus Client Installation

Step 7. Click Next (Figure 3).

Figure 3. Symantec AntiVirus InstallShield Wizard

Step 8. Accept the License Agreement and Click Next (Figure 4).

Figure 4. Symantec AntiVirus InstallShield Wizard



Step 9. Now select the Setup Type as "Complete" and Click Next (Figure 5).

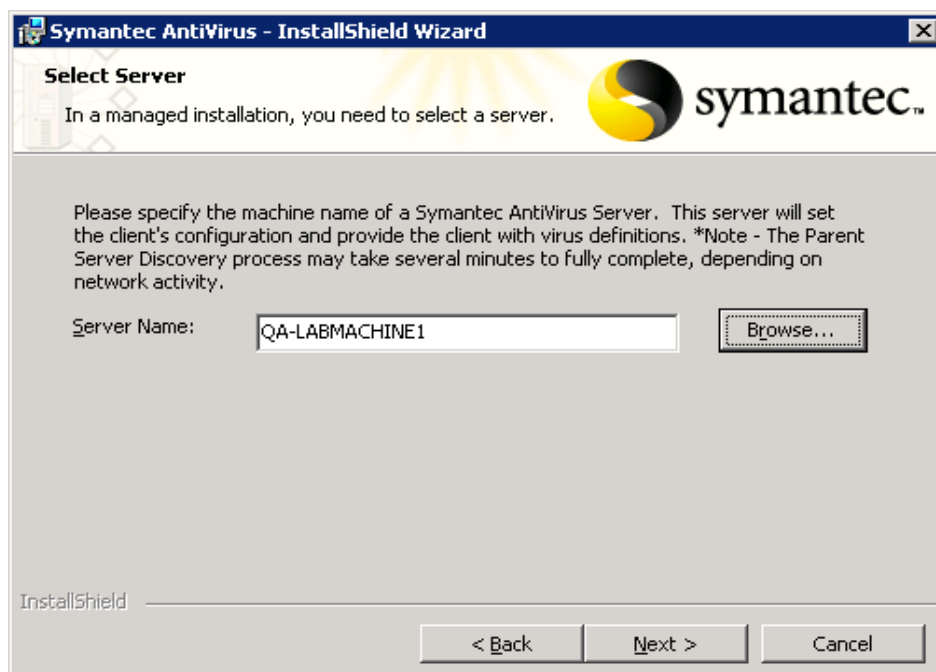
Figure 5. Symantec AntiVirus Setup Type



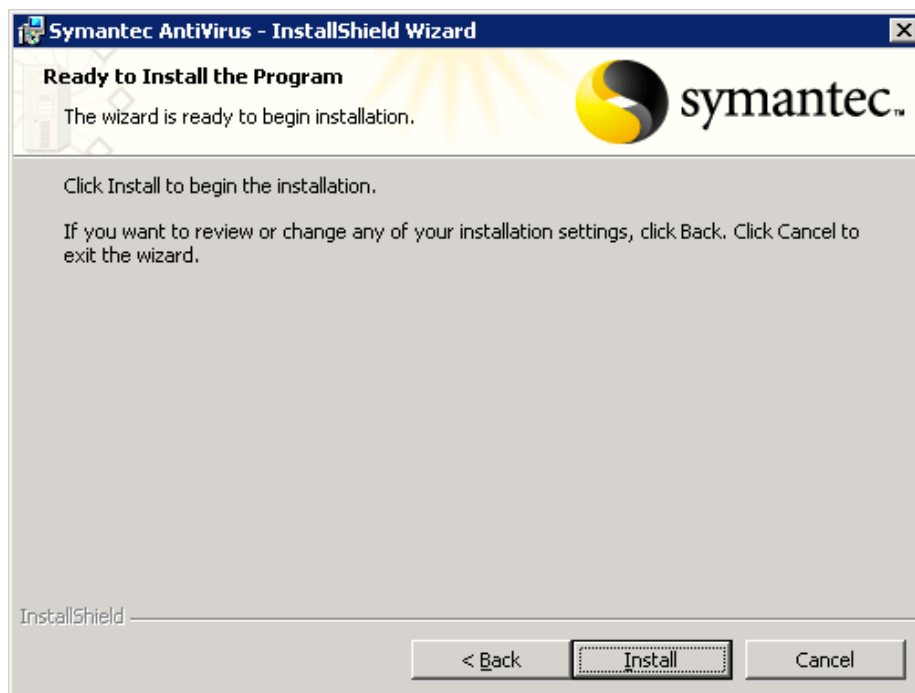
Step 10. Select the Network Setup Type as "Managed" and Click Next (Figure 6).

Figure 6. Network Setup Type

Step 11. Enter the Symantec AntiVirus Server Name and Click Next (Figure 7).

Figure 7. Selecting Symantec AntiVirus Server Name

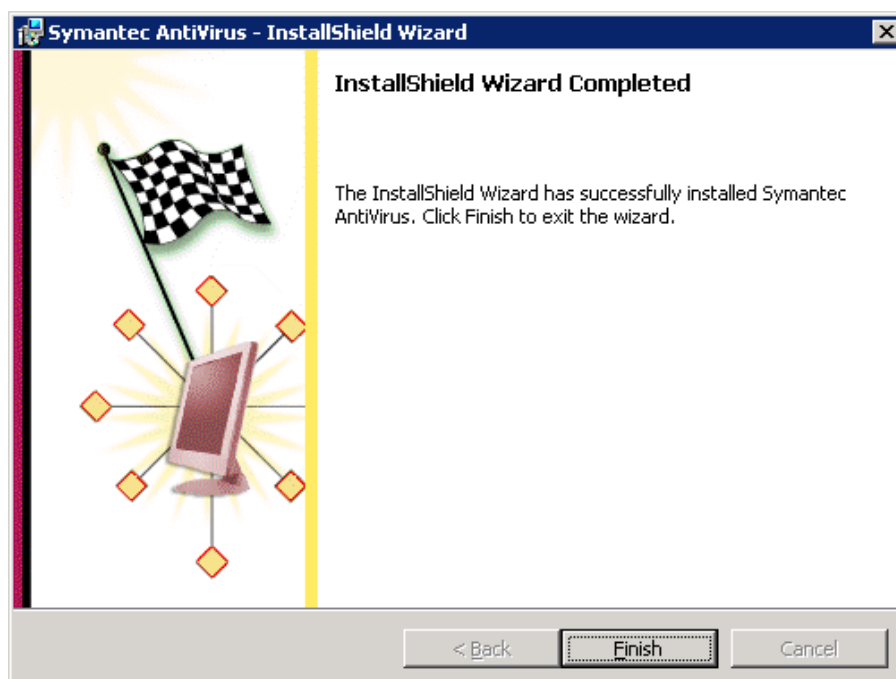
Step 12. Click Install (Figure 8).

Figure 8. Installing Symantec AntiVirus

Step 13. When the installation (Figure 9) is completed, click Finish (Figure 10).

Figure 9. Symantec AntiVirus Installation

Figure 10. Installation Complete



Step 14. When installation is finished, it will prompt you to restart (Figure 11).

Figure 11. Installer Information Screen Shot



CONFIGURATION

For normal operation on Cisco MXE 3000, 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 video 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.

To restart the antivirus service:

Step 1. Click Start>Program>Administrative Tools>Services.

Step 2. Locate the Symantec AntiVirus service.

Step 3. Stop and then restart the antivirus service.

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:

Step 1. On the Windows taskbar, click Start > Settings > Control Panel.

Step 2. In the Control Panel, double-click Add/Remove Programs.

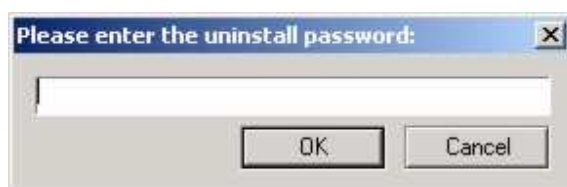
Step 3. In the list of currently installed programs, click Symantec AntiVirus.

Step 4. In Windows 2003, click Remove.

Step 5. Click Yes to confirm that you want to uninstall the product.

Step 6. Enter the Symantec AntiVirus Server console password (Figure 12).

Figure 12. Uninstall Password Window



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



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CODA, CODP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0809R)

August 25, 2009