



Installing and Configuring McAfee NetShield on the Cisco ICS 7750

March 15, 2002

This document describes the steps for installing and configuring McAfee NetShield on the Cisco Integrated Communications System 7750 (ICS 7750).

To access the documentation suite for the Cisco ICS 7750, go to

<http://www.cisco.com/univercd/cc/td/doc/product/voice/ics/>

To access the latest software upgrades for the Cisco ICS 7750 on Cisco.com, go to

<http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml>

Contents

This installation document includes information about the following topics:

- [Overview, page 1](#)
- [Ordering McAfee NetShield, page 2](#)
- [Installing McAfee NetShield, page 2](#)
- [Configuring McAfee NetShield, page 8](#)
- [Notes, page 15](#)

Overview

McAfee NetShield is an antivirus program that provides protection for Windows 2000 servers, such as the System Processing Engine 310 (SPE 310).

Cisco has qualified McAfee NetShield for use with Cisco CallManager and Cisco Unity. This document covers installation and configuration procedures on the Cisco ICS 7750 that is running system software release 2.x.x and Cisco CallManager 3.1.x.



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2002. Cisco Systems, Inc. All rights reserved.

For a summary of the system requirements for system software release 2.x.x on the Cisco ICS 7750, refer to the [Release Notes for System Software Release 2.x.x on the Cisco ICS 7750](#).

If McAfee NetShield is installed on an SPE 310 running Cisco Unity, the virus-scan services must be disabled before you run the Cisco Unity Setup program to speed up the installation process. You re-enable the services after the SPE 310 is configured. For details on how to disable and re-enable NetShield, refer to “Installing a Cisco Unity System” in the [Cisco Unity Installation Guide, Release 3.1](#) document.

For installation and configuration details on other platforms, refer to the following documents:

- [Using McAfee NetShield with Cisco CallManager 3.x](#)
- [Cisco Unity 3.1 System Requirements, and Supported Hardware and Software](#)

Ordering McAfee NetShield

You can purchase and download McAfee NetShield from the [McAfee website](#).

It is assumed that you have McAfee NetShield 4.5.0. If NetShield Service Pack 1 (SP1) is not included with your version of McAfee NetShield, contact McAfee to obtain it.

Installing McAfee NetShield

This section tells how to install McAfee NetShield on an SPE. The section includes the following topics:

- [Connecting Peripherals, page 2](#)
- [Setting Up Account Information, page 4](#)
- [Installing Service Pack 1 for NetShield v4.5, page 7](#)



Note For optimum protection against viruses, McAfee NetShield and SP1 should be installed on all SPEs in the Cisco ICS 7750.



Note This procedure is for a Cisco ICS 7750 that is running system software release 2.x.x or later. SPE 310s are required in order to run system software release 2.x.x or later.

Connecting Peripherals

This section tells how to use the CD-ROM drive for installing McAfee NetShield on an SPE:

-
- Step 1** Connect a monitor cable to the video port on the SPE 310, and power on the monitor.
- Step 2** Do one of the following, based on the type of peripherals you are using:
- **USB**—Connect a USB keyboard to one SPE USB port, and connect a USB mouse to the other SPE USB port.

- PS/2—Connect the “Y” splitter cable for your keyboard and mouse to the keyboard/mouse port on the target SPE, and then connect your keyboard and mouse to the available ends of the “Y” splitter cable.



Note If you are using the “Y” splitter cable to connect a PS/2 mouse and a keyboard to the SPE, the keyboard and mouse must be connected at or before the time that the SPE is restarted in order to be recognized by the operating system. This is not the case with a USB keyboard and mouse, which typically are recognized without restarting the operating system.



Note For a list of USB peripherals that have been tested on the Cisco ICS 7750, refer to the “Connecting a Monitor, Keyboard, and Mouse to the SPE Card” section in the [Cisco ICS 7750 Getting Started Guide](#).



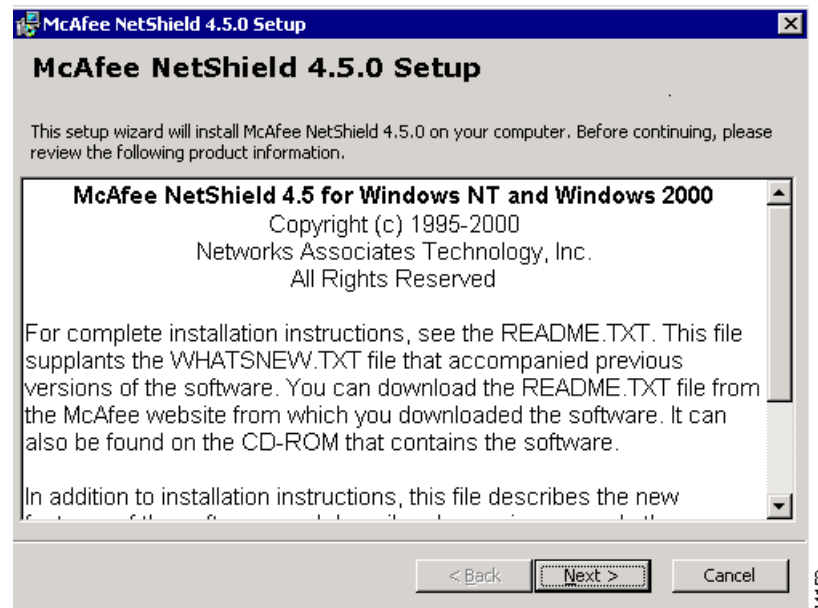
Caution It is strongly recommended that you close all open programs before proceeding to install this software.

- Step 3** Place the McAfee NetShield CD in the CD-ROM drive.
- Step 4** On the target SPE, use Windows Explorer to navigate to the CD-ROM drive.
- Step 5** Navigate to Setup.exe on the McAfee NetShield CD.
- Step 6** Double-click **Setup.exe**.

The files are extracted to the target SPE.

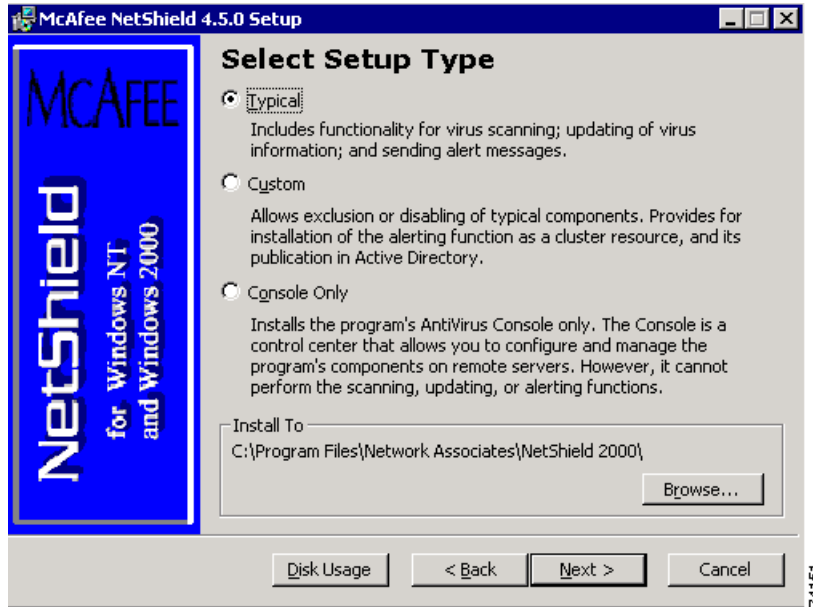
The NetShield 4.5.0 setup screen appears. See [Figure 1](#).

Figure 1 McAfee NetShield 4.5.0 Setup



- Step 7** Click **Next**.
- Step 8** In the **Select Setup Type** window, click the **Typical Installation** radio button. See [Figure 2](#).

Figure 2 Select Setup Type



Step 9 Click **Next**.

Step 10 Continue with the [“Setting Up Account Information”](#) section on page 4.

Setting Up Account Information

Follow these steps to set up account information for McAfee NetShield on the Cisco ICS 7750:

Step 1 Check the **Use System Account** check box in the Account Information window. See [Figure 3](#).

Figure 3 Account Information





Note The System Account enables access to local resources only.

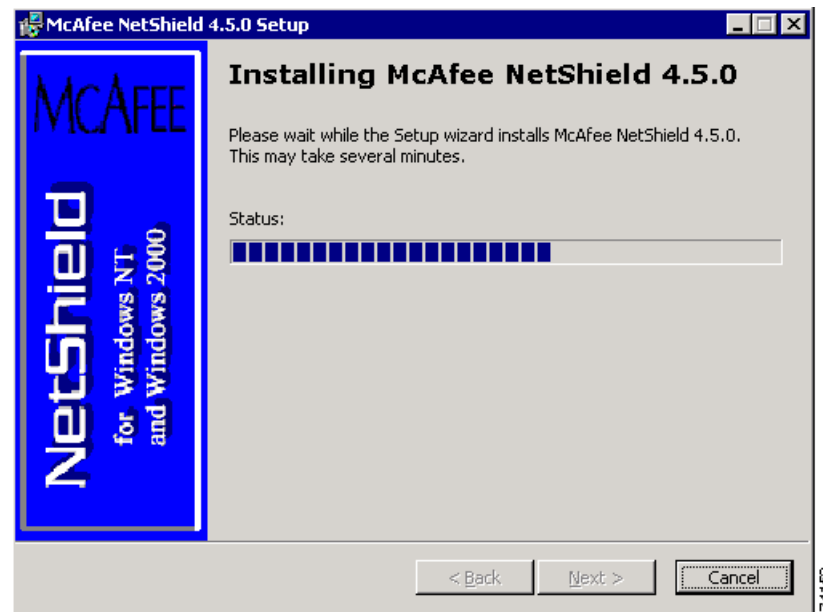


Note The Use Same Account for Alert Manager check box is selected by default.

Step 2 Click **Next**.

The NetShield installation wizard installs McAfee NetShield 4.5.0, updates the registry entries, starts up the services, and removes any backup files. See [Figure 4](#).

Figure 4 Installing McAfee NetShield 4.5.0



Step 3 Click **Next**.

The **Installation Successful** window shows a message that McAfee NetShield 4.5.0 has been successfully installed.

Step 4 Check the **Run AutoUpdate** and **Run On-Demand Scan** check boxes. See [Figure 5](#).

Figure 5 Installation Successful

**Note**

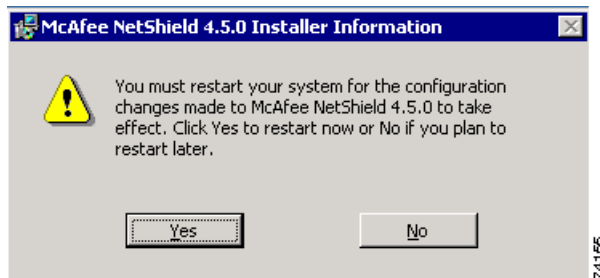
AutoUpdate can be configured to retrieve virus definition, or .DAT, file updates from a local computer. These virus definition files contain up-to-date virus signatures and other information that McAfee NetShield uses to protect your computer against computer viruses. Download and install the most current set of .DAT files to ensure optimum antivirus protection for your network. Auto Update procedures will be addressed later in this document.

Step 5 Click **Yes** to complete the installation and to restart your SPE. See [Figure 6](#).

**Note**

Be sure to disconnect the CD-ROM drive from the SPE before you restart the system.

Figure 6 Restart Your Computer



Installing Service Pack 1 for NetShield v4.5

The version of McAfee NetShield that you are using might include SP1. This service pack includes the latest patches for the McAfee NetShield 4.5.0 software. If your copy of McAfee NetShield does not include SP1, you must install it now. Otherwise, go to [Configuring McAfee NetShield, page 8](#).



Caution

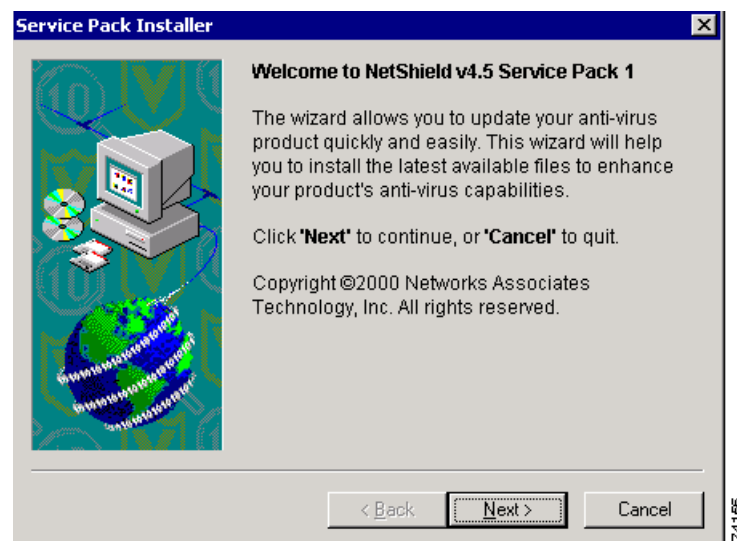
It is strongly recommended that you close all open programs before you start to install this service pack.

Follow these steps to install SP1 on your SPE:

- Step 1** With the McAfee NetShield CD in the CD-ROM drive and connected to the target SPE, use Windows Explorer to navigate to the CD-ROM drive.
- Step 2** Navigate to NNTSP1.exe on the McAfee NetShield CD.
- Step 3** Double-click **NNTSP1.exe** to install SP1 on the SPE.

The Service Pack Installer wizard appears. See [Figure 7](#).

Figure 7 Service Pack Installer



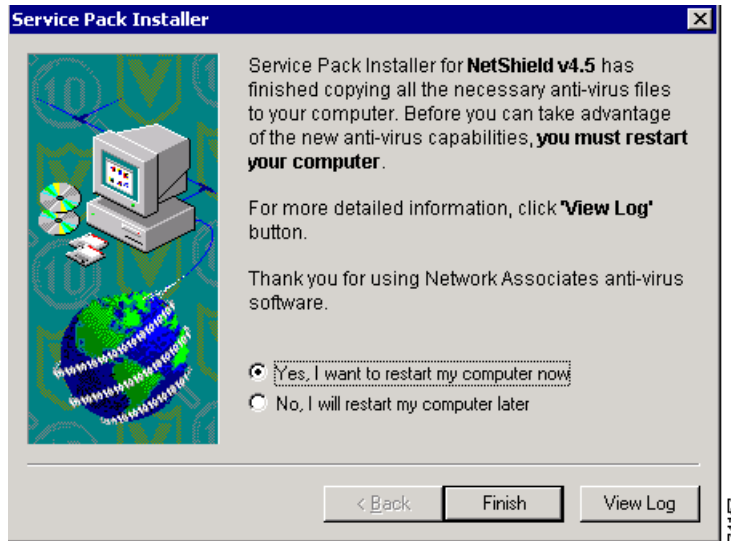
- Step 4** Click **Next**.
You must restart your SPE after the Service Pack Installer has completed successfully.
- Step 5** Click **Yes** to restart your SPE.
- Step 6** Click **Finish**. See [Figure 8](#).



Note

Disconnect the CD-ROM drive from the SPE before you restart your system.

Figure 8 Service Pack Installation Successful



Step 7 Continue with the [“Configuring McAfee NetShield”](#) section on page 8.

Configuring McAfee NetShield

This section tells how to configure McAfee NetShield on the Cisco ICS 7750. The section includes the following topics:

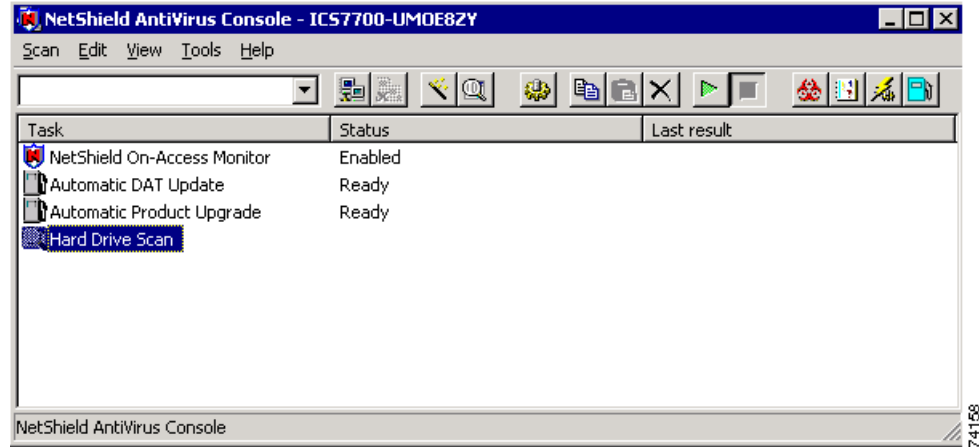
- [Configuring the NetShield Console, page 8](#)
- [Configuring the NetShield Scheduler, page 10](#)
- [Configuring the Alert Manager, page 13](#)

Configuring the NetShield Console

Follow these steps to configure the McAfee NetShield console on the Cisco ICS 7750 SPE:

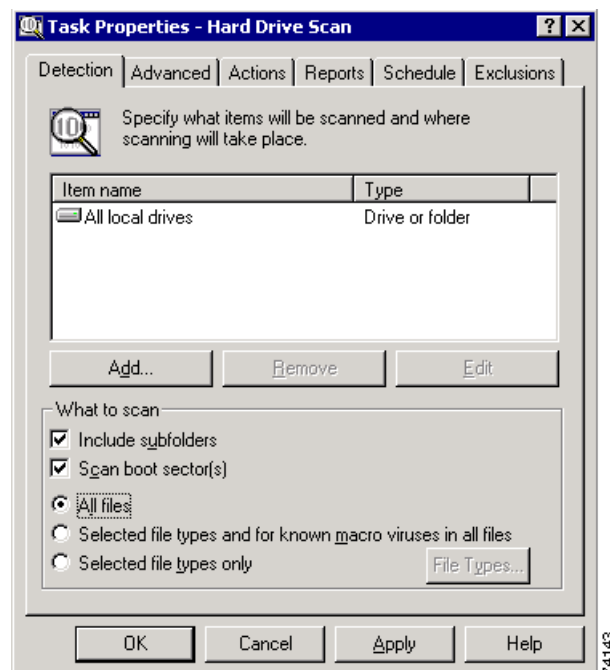
-
- Step 1 Connect your peripherals as described in the [“Connecting Peripherals”](#) section on page 2.
- Step 2 On the target SPE, choose **Start > Programs > Network Associates > NetShield Console**.
The NetShield console window opens.
- Step 3 From the menu bar, choose **Scan > New Task** to add a scan task and assign a name, such as **Hard Drive Scan**. See [Figure 9](#).

Figure 9 NetShield Console



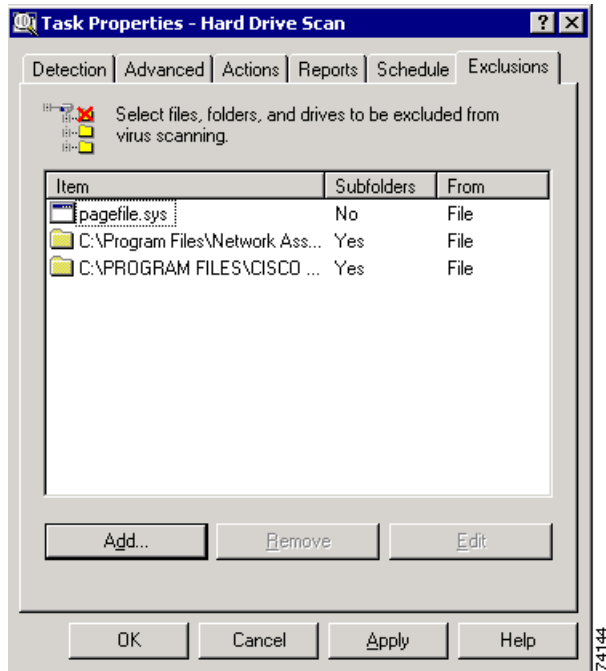
- Step 4 Right-click **Hard Drive Scan**. Choose **Properties**.
- Step 5 Click the **Detection** tab.
- Step 6 Click **Add** to add the hard drive (C: drive) for scanning.
- Step 7 Click the **All Files** radio button.
- Step 8 Click **Apply**. Click **OK**. See Figure 10.

Figure 10 Task Properties—Hard Drive Scan



- Step 9 Click the **Exclusions** tab.
- Step 10 Click **Add**.
- Step 11 At the prompt, enter **c:\program files\cisco IDS** to exclude this directory from virus scanning.
- Step 12 Click **Apply**. Click **OK**. See Figure 11.

Figure 11 Hard Drive Exclusions



Configuring the NetShield Scheduler

Follow these steps to configure the McAfee NetShield scheduler to schedule your antivirus disk scanning activity:

- Step 1 Click the **Schedule** tab to schedule your disk scanning activity.
- Step 2 Check the **Enable Scheduler** check box.
- Step 3 Click the applicable **Run** radio button to designate frequency.
- Step 4 Enter a start time in the **Start at** field.

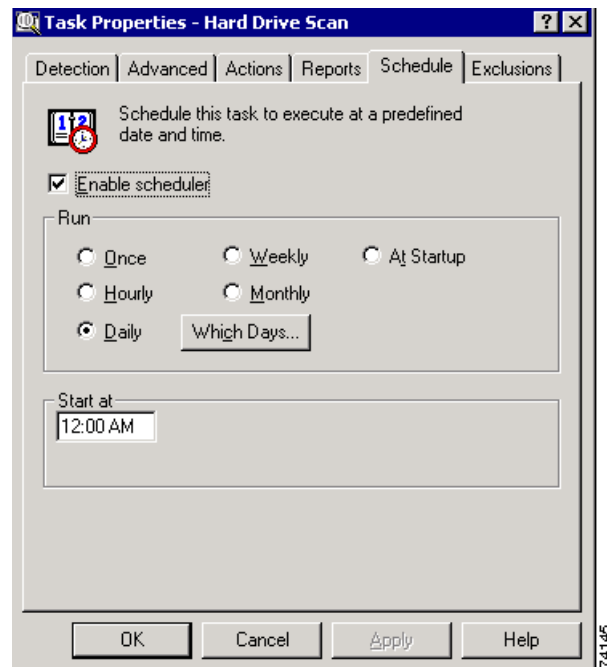


Caution

Schedule this activity to run at midnight or another off-peak time, as NetShield disk scanning increases CPU usage to almost 100% and may significantly affect the performance of the system and any installed applications. Call processing or voice-mail processing might be affected while disks are being scanned for viruses.

Step 5 Click **Apply**. Click **OK**. See [Figure 12](#).

Figure 12 *Hard Drive Scheduler*



Step 6 Click **Cancel** to return to the NetShield Console.

Step 7 Click **Hard Drive Scan**.

Step 8 From the menu bar, choose **Tools > Automatic Update** to select the Automatic DAT Update method.



Note Automatic Update sets the scheduling of a convenient time for the SPE to download updated virus definition files. To ensure successful operation, keep the most recent DAT-xxxx.ZIP file in a central location (on a PC or on one of the SPEs). For the most recent virus definition file, refer to the [McAfee website](#).

Step 9 Click the **Update Options** tab.

Step 10 Click the **Copy from a local network computer** radio button.

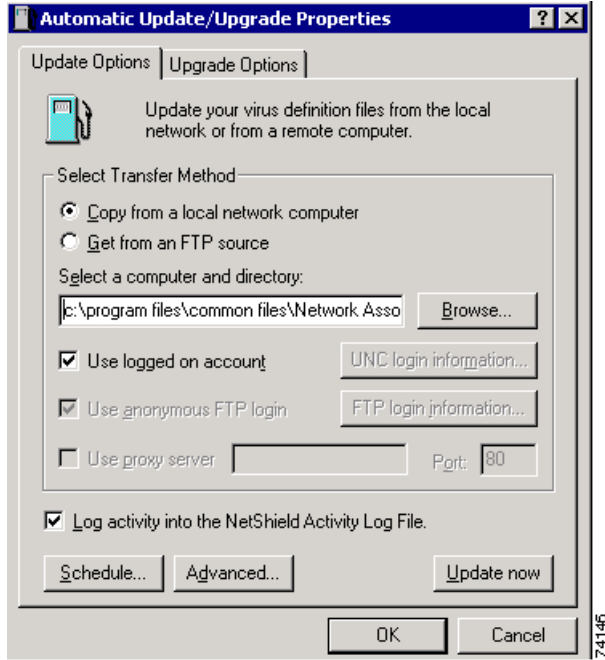
Step 11 Check the **Use logged on account** check box.

Step 12 In the **Select a computer and directory** field, enter `c:\program files\common files\Network Associates\VirusScan Engine\4.0.x.x`. See [Figure 13](#).



Note If your Cisco ICS 7750 has Internet connectivity, NetShield can be configured to retrieve the .DAT files directly from McAfee using FTP. See the NetShield documentation that came with your software, or refer to the [McAfee website](#) for further information.

Figure 13 Automatic Update

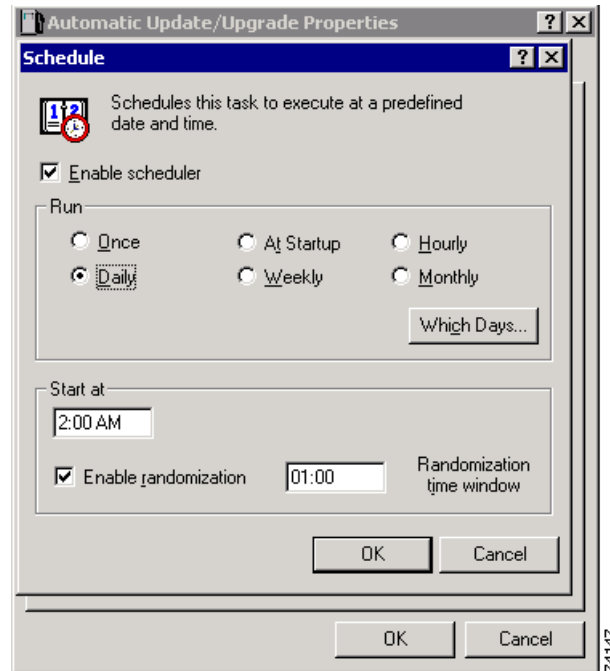


- Step 13 Click **Schedule**.
- Step 14 Check the **Enable Scheduler** check box.
- Step 15 Click the applicable **Run** radio button to designate frequency.
- Step 16 Enter a start time in the **Start at** field. See [Figure 14](#).



Note Although this update is not CPU-intensive and does not take much time to run, it should be scheduled when no disk scanning is occurring.

Figure 14 Automatic Update Scheduler



Step 17 Click **OK**.



Note The scan and automatic .DAT files update tasks can be scheduled or executed on demand.



Note Be sure to use the automatic NetShield software update feature to ensure that the latest NetShield software is being used at all times.

Step 18 Click **Cancel** to return to the NetShield console.

Configuring the Alert Manager

The Alert Manager configuration designates the location to which alerts will be sent to track activity on the Cisco ICS 7750.

Follow these steps to configure the Alert Manager for McAfee NetShield:

Step 1 From the NetShield console, click **Hard Drive Scan**.

Step 2 From the menu bar, choose **Tools > Alerts**.



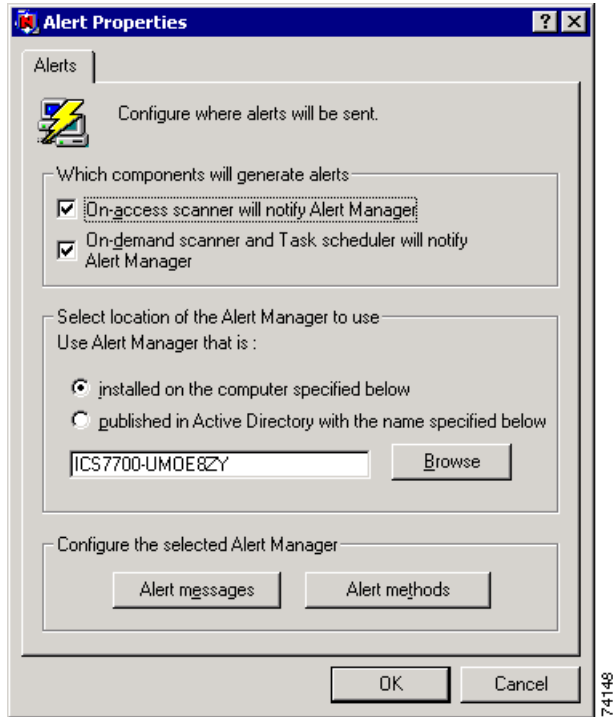
Note You can also configure the Alert Manager from the target SPE by choosing **Start > Programs > Network Associates > Alert Manager Configuration**.

The Alert Properties window appears. See [Figure 15](#).



Note By default, the host name of the Cisco ICS 7750 SPE appears as the location to be used by Alert Manager.

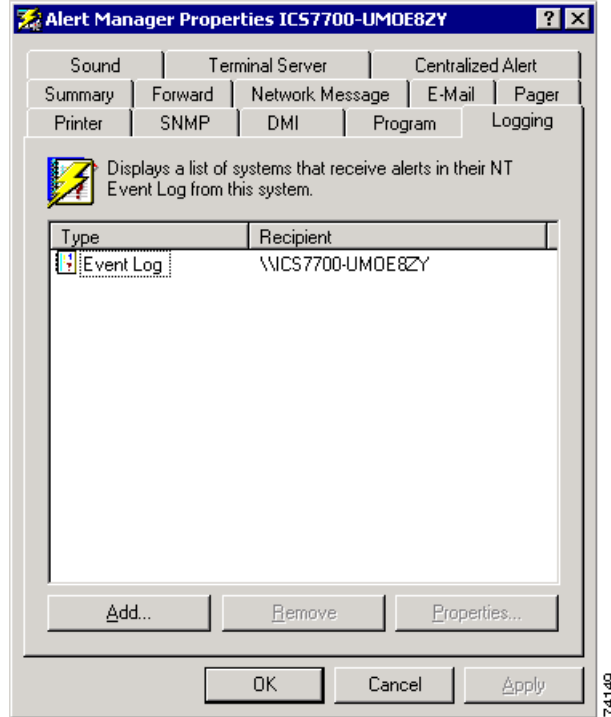
Figure 15 Alert Manager Configuration Alert Properties



Step 3 Choose **Alert Methods**.

Step 4 Click the appropriate tab to change desired parameters. See [Figure 16](#).

Figure 16 Alert Manager Logging



Note Local event logging is set by default under the **Logging** tab. All alerts to the Event Viewer log are logged on the target SPE. If this default setting is acceptable, no further action is required.

Step 5 Click **Cancel** to exit the **Alert Manager Configuration**.

Notes

The following are important notes about issues that apply to the Cisco ICS 7750:

- The NetShield configuration can be performed by using the NetShield console on each of the SPEs in the Cisco ICS 7750 or by using the NetShield console on one SPE and connecting to other SPEs. A central console installed on an external PC can also be used, in which case the PC can function as a .DAT file server and software upgrade server.
- The disk-scanning task consumes significant system resources. Therefore, it is strongly recommended that this task be scheduled during off-peak hours. If there are insufficient off-peak hours to allow for scheduled scanning, it is recommended that scanning be done during regular scheduled times for system maintenance.
- While the disks are being scanned, please make sure that no other ICS System Manager operations, such as ICSCfg, are running at the same time.

Related Documentation

Use this installation document with the following documents listed in the following sections:

Cisco ICS 7750 Documents

The documents described in this section are available on Cisco.com and on CD:

- On Cisco.com, starting under the **Service & Support** heading navigate to **Technical Documents > Voice/Telephony > Cisco ICS 7750**
- On the Documentation CD-ROM (order number DOC-CONDOCCD=) navigate to **Product Documentation > Voice/Telephony > Cisco ICS 7750**

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

<http://www.cisco.com>

Translated documentation is available at the following URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

<http://www.cisco.com/tac>

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

<http://www.cisco.com/register/>

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

<http://www.cisco.com/tac/caseopen>

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

This document is to be used with the documents listed in the [“Related Documentation”](#) section.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, 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, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, 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. (0711R)

Copyright © 2002, Cisco Systems, Inc.
All rights reserved.

