



Using McAfee NetShield with Cisco CallManager 3.X

Application Note

Enterprise Voice, Video Business Unit
August 30, 2002

Table of Contents

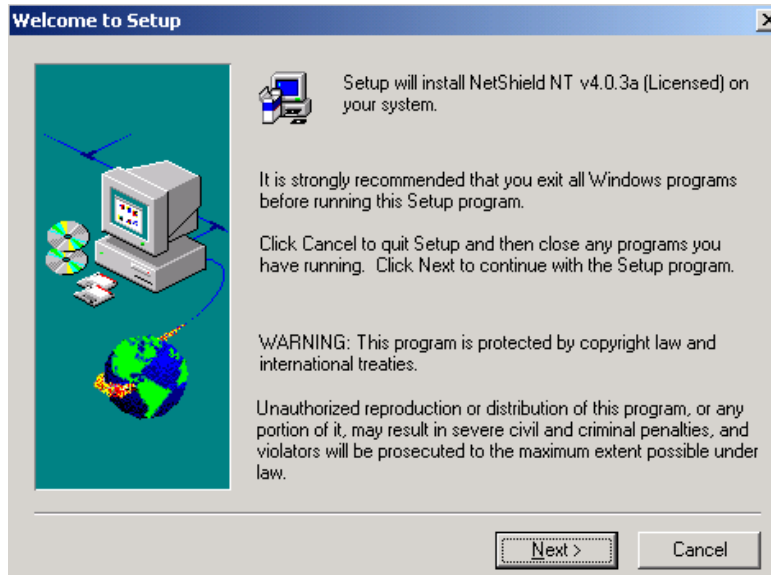
Table of Contents	2
Introduction	3
Installation	3
Configuration	7
Scheduled File Scanning Can Have a Negative Impact on the Server	7
Using Cisco IDS Host Sensor and McAfee NetShield	7

Introduction

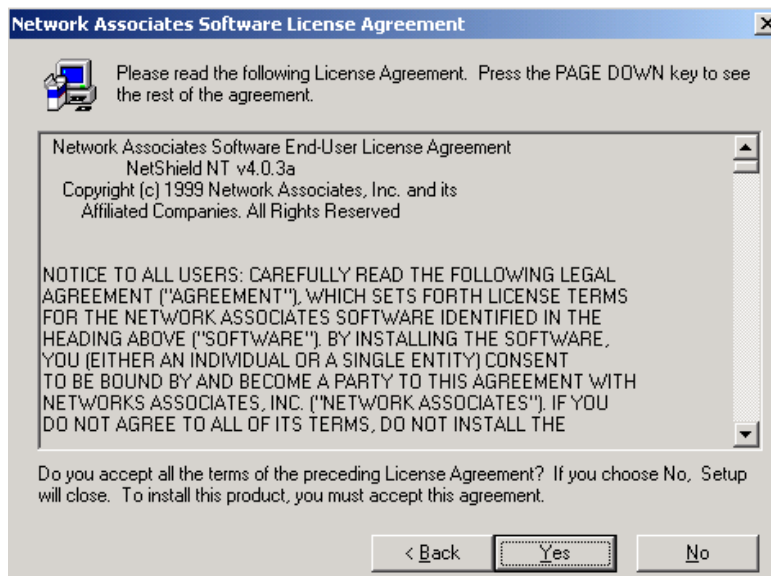
Any Windows 2000 Server needs to have virus protection and the Cisco CallManager is no exception. While the installation and configuration of McAfee NetShield is very easy, there are a few important steps that need to be taken. This document will provide information on the installation and configuration of McAfee NetShield 4.x (including the newest 4.5.0 release) on the Cisco CallManager platform.

Installation

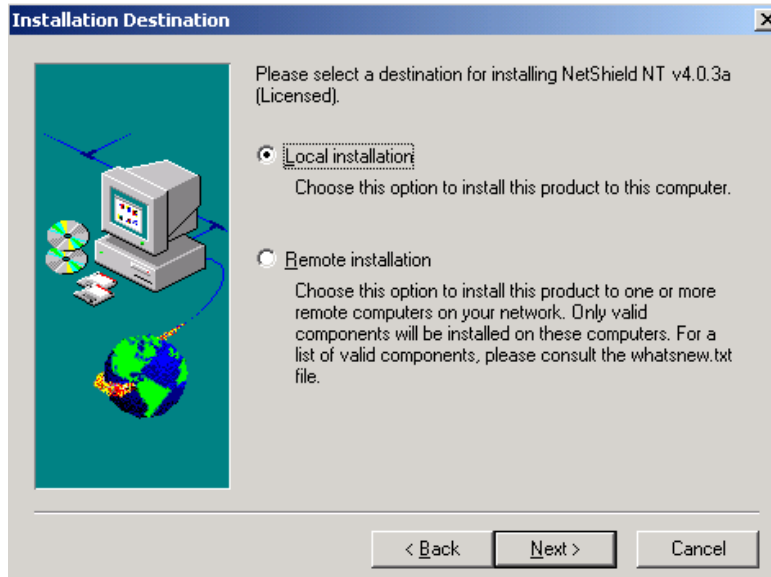
Double-click the setup.exe executable. Click **Next**.



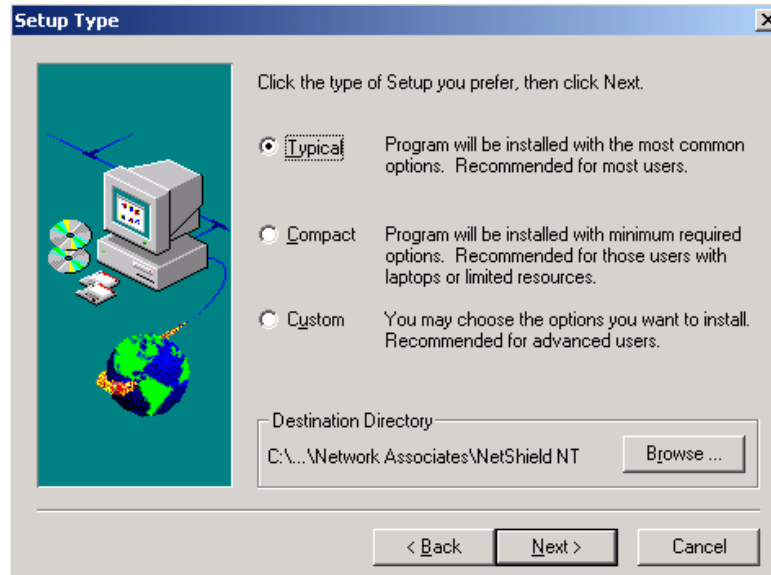
Read the License Agreement and click **Yes**.



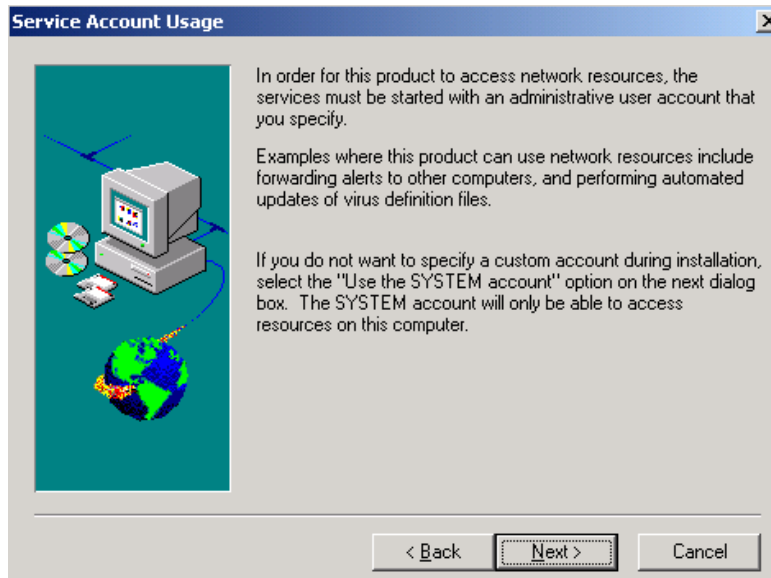
To install on the local computer, select Local installation and click **Next**.



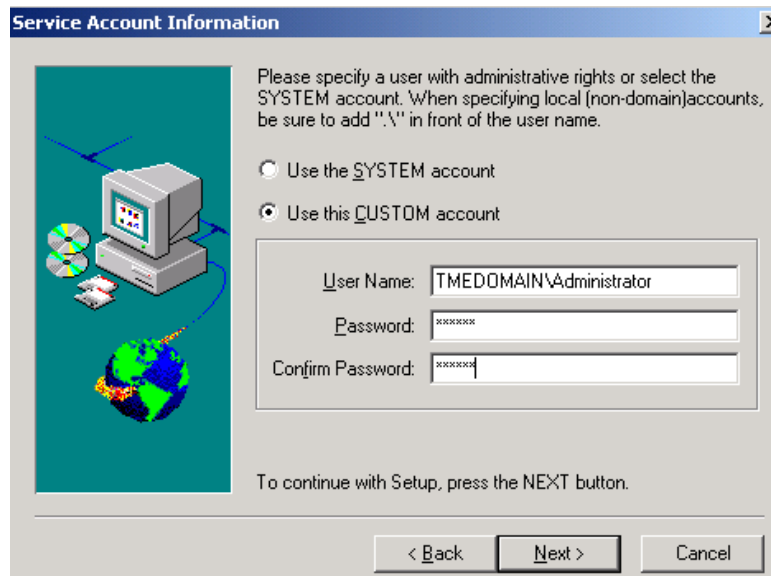
Select Typical for the Setup type and click **Next**.



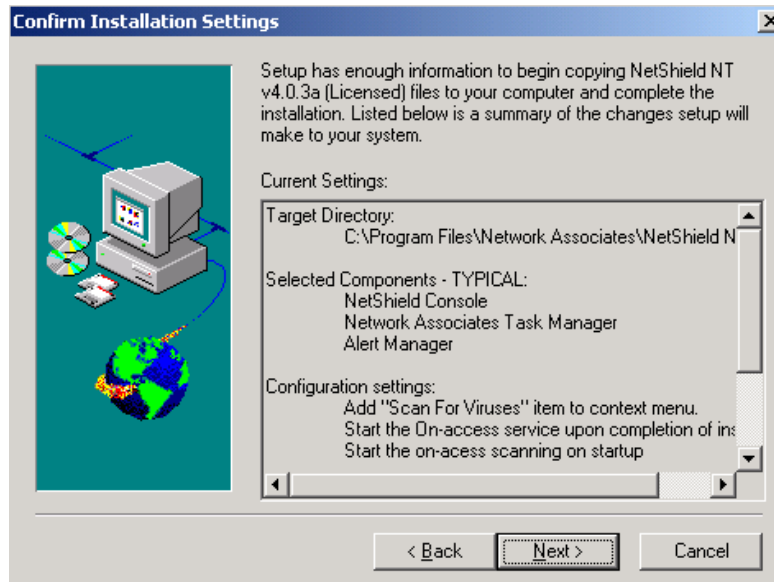
The Service Account Usage screen describes important information about network access to resources. If you want to be able to have this server be able to access other network resources for alerting and automated updates of virus definition, you may want to use a Domain User with appropriate access as the Service Logon Account. Click **Next**.



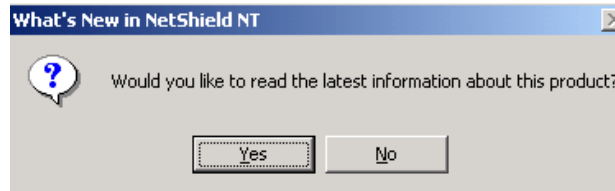
If you only need local access, select Use the System account. If you need network access to resources as explained above, then put in a Domain User Name and password. Click **Next**.



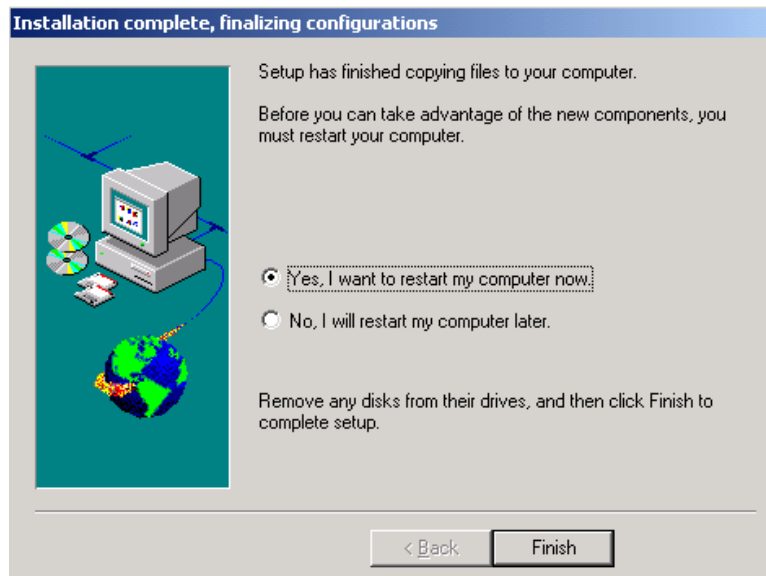
Click **Next**.



If you want to read about what is new in NetShield, click **Yes**. Otherwise, click **No**.



To complete the installation, select 'I want to restart my computer now' and click **Finish**.



Configuration

For normal operation on Cisco CallManager 3.X, the default settings for McAfee NetShield are fine. There are two important considerations, however.

Scheduled File Scanning Can Have a Negative Impact on the Server

There is a difference between the protection NetShield offers by running in the background and scheduled file scanning of the entire directory structure. Scheduled file scanning is very processor intensive. This could potentially impact call processing if this occurred during high volume traffic. As such, it is critical to only schedule a complete file scan during the middle of the night or other non-peak time schedules.

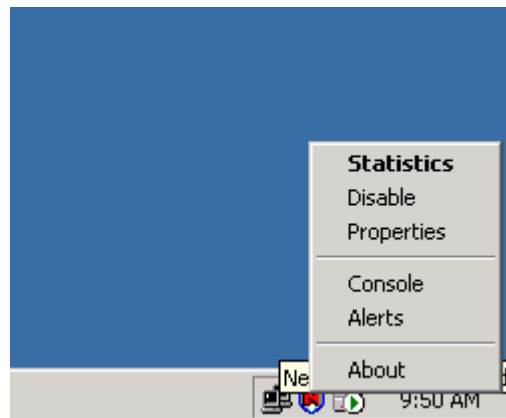
Using Cisco IDS Host Sensor and McAfee NetShield

NOTE: It is important to note that in order for McAfee and the Cisco Host IDS Sensor to co-exist on the same server, McAfee should be configured to not scan the directory where the Cisco Host IDS Sensor or Console is configured.

Once McAfee is installed, the icon will appear in the system tray as shown below.



Right Click on the 'N' icon and select **Properties**.



This will bring up the NetShield Properties Panel. The settings shown below are the default settings for McAfee NetShield. You can safely select the 'All Files' option under the 'What to Scan' section if you desire that functionality.

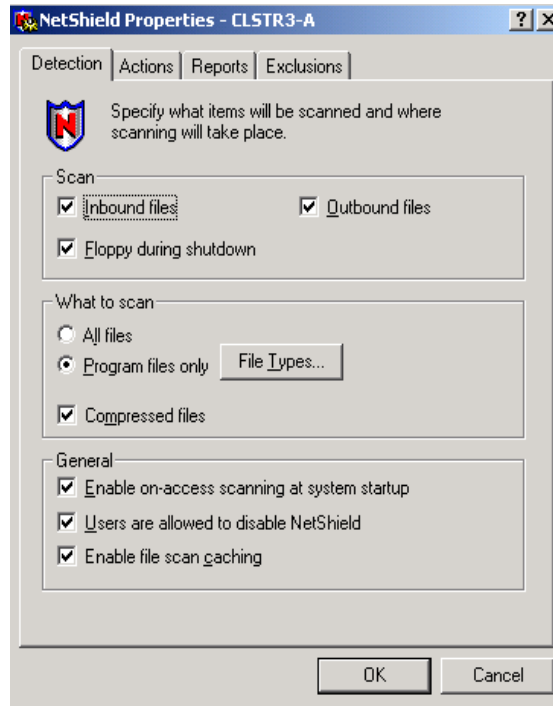


Figure 1 - McAfee NetShield v4.03 Properties

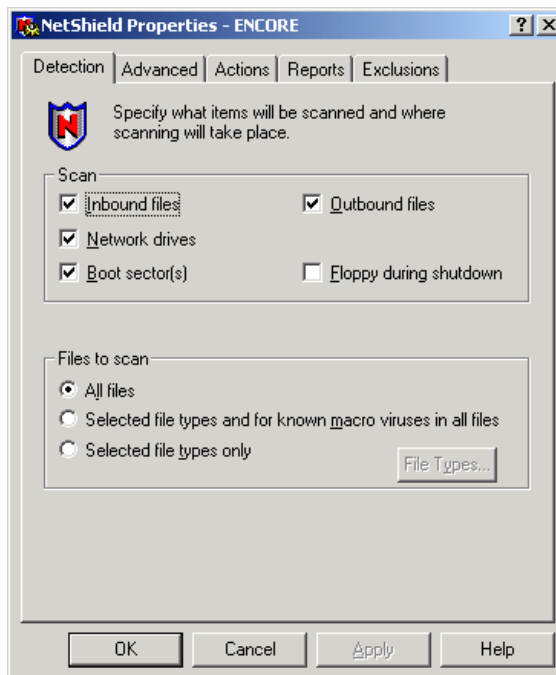
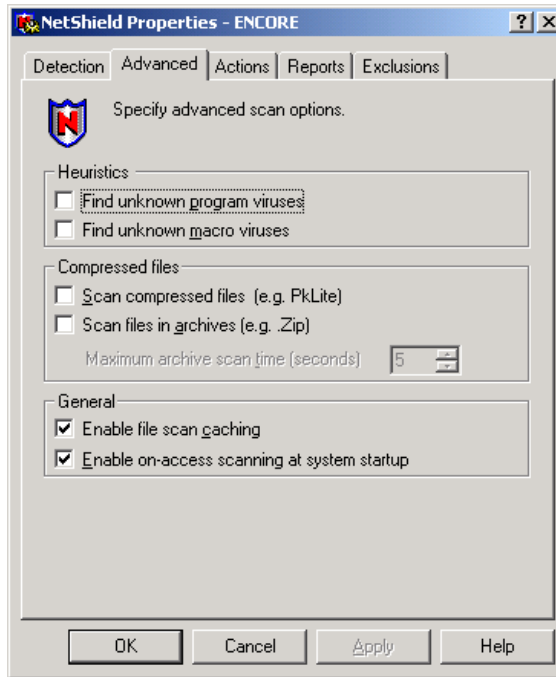


Figure 2 - McAfee NetShield v4.5 Properties

Select the Advanced Tab (if available). Uncheck the boxes under Heuistics.



Select the Exclusions Tab. Click the **Add** button and choose the C:\Program Files\Cisco IDS directory. When finished, it should look like this.

