Application Note

Installing and Configuring the Cisco IDS Host Sensor on Cisco CallManager Versions 3.3, 3.2, 3.1, and 3.0

Introduction

Security remains important in any company's infrastructure, especially when that infrastructure includes servers that perform call processing and networks that carry voice. The recent Code Red virus affected many companies who had taken a lax approach to security. Not only were servers that were running IIS affected, but the propagation of this virus brought entire networks to a crawl.

The Cisco® IDS Host Sensor, powered by Entercept™, provides a great tool to help meet the security challenge. Because this product does not substitute for poor network design or poor Windows security practices, ensure that a secure network and a secure Windows 2000 platform are built before adding this product. The Cisco IDS Host Sensor acts as the last line of defense that helps ensure that Cisco CallManager will be protected against intruders and various types of security and network attacks.

For information about basic security practices that should be implemented, read the Cisco IP Telephony Solution Guide chapters on security, available at

http://www.cisco.com/application/pdf/en/us/guest/netsol/ns268/c649/ccmigration_09186a00800d6805.pdf

Important: Make sure to read the "Caveats" section at the end of this document. You need to follow some important steps when using McAfee NetShield with the Cisco IDS Host Sensor Agent. Additionally, follow every step in this document. Failure to do so can result in serious network problems.

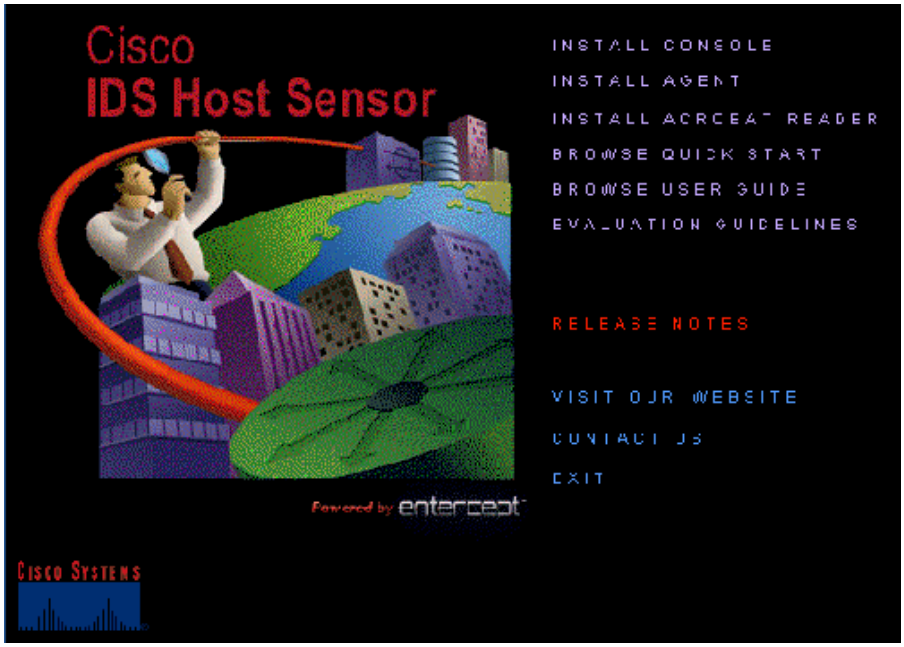
Installation Steps

For the first step install the console, where all security alerts and notifications will be sent and displayed. You can install the console on any device. Then, install the Cisco IDS Host Sensor Agent on the same server as the Cisco IDS Host Sensor Console and all Cisco CallManagers, which send their notifications to the Cisco IDS Host Sensor Console.

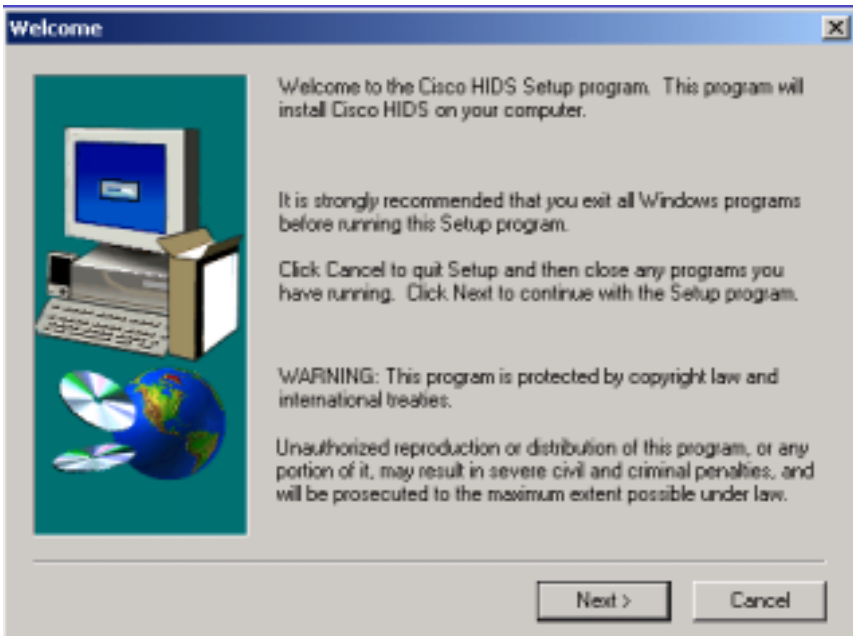
For a small deployment, you can install the Cisco IDS Host Sensor console on the Publisher server if desired. Ideally, the console should reside on a separate device.

Installing the Cisco IDS Host Sensor Console

When the CD is inserted into the CD-ROM drive, a splash screen appears. Choose the **Install Console** option as seen below.



To begin the installation, click **Next**.

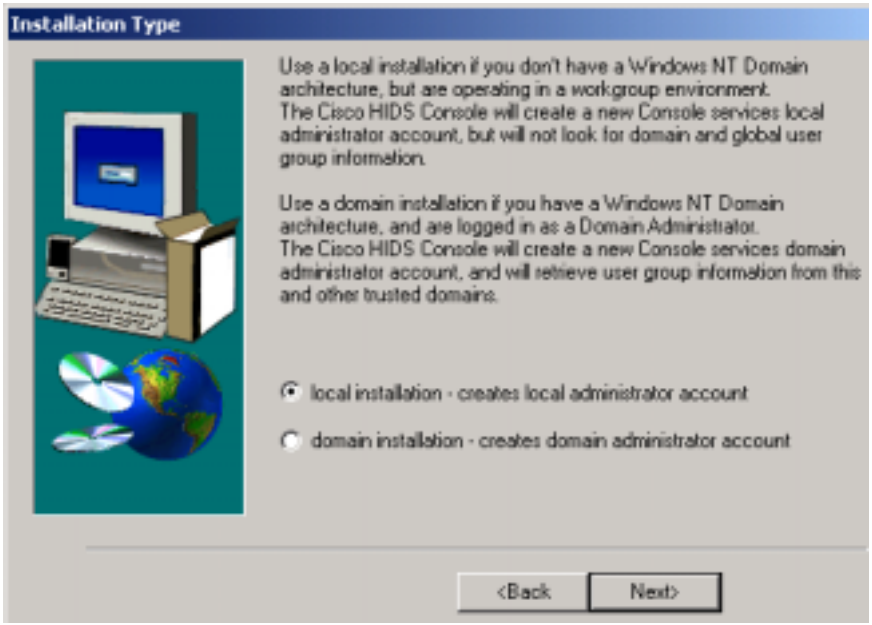


To accept the license agreement, click **Accept**.

After reading the product information, click **Next**.

After choosing the destination folder, click **Next**.

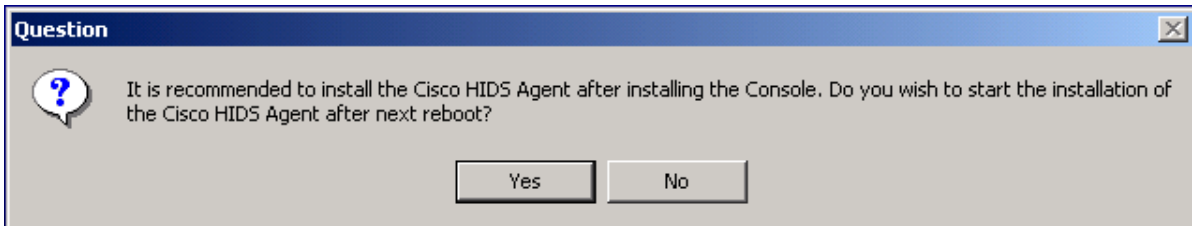
Note: If you have followed the recommended security practices for Windows 2000 Cisco CallManager environments, the Cisco CallManager cluster should be part of a domain. If so, choose **domain installation**. If the servers are not a part of the domain, choose **local installation** and then click **Next**.



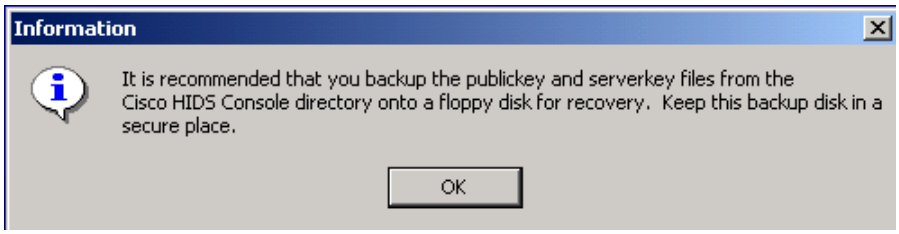
After selecting the program folders, click **Next**.

After reviewing the current settings, click **Next**.

Note: The Cisco IDS Host Sensor Agent should run on the same device as the Cisco IDS Host Console. The Cisco IDS Host Console also needs protection. Click **Yes**.



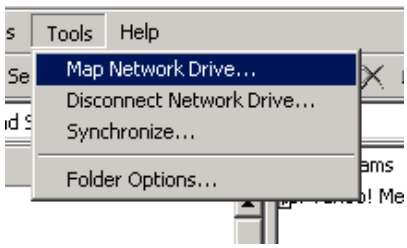
The serverkey and publickey files reside in the c:\Program Files\Cisco IDS\Console directory. Keep these keys in a safe backup location. Click **OK**.



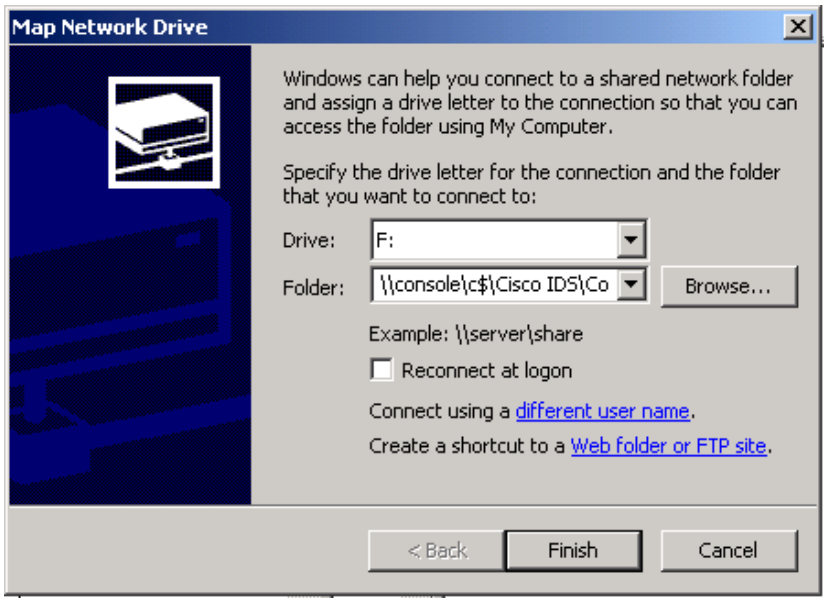
If prompted, restart your server.

Installing the Cisco IDS Host Sensor Agent

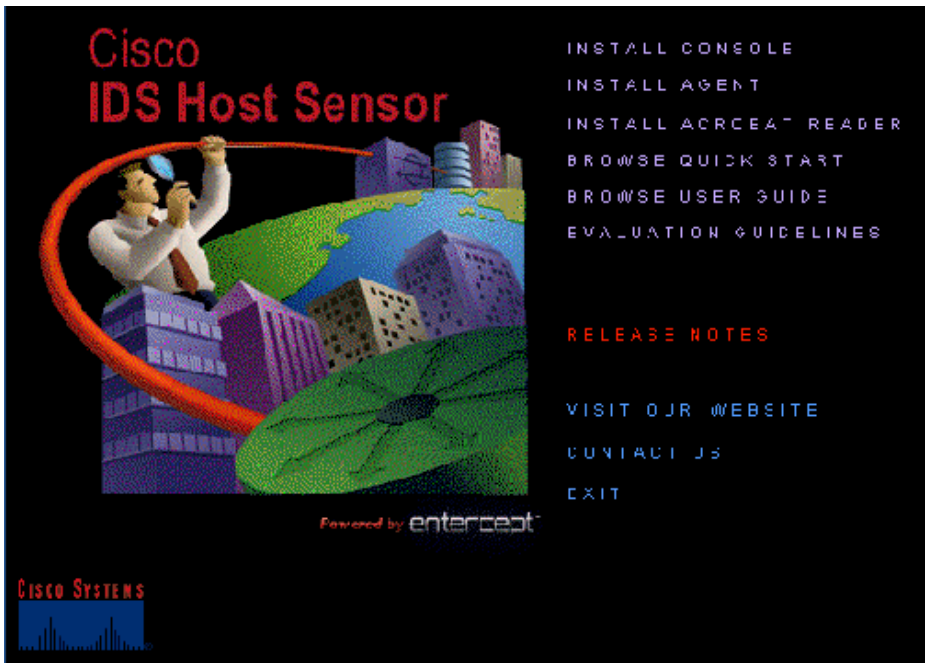
Before installing the Cisco IDS Host Sensor Agent on a separate device, make sure to map a drive to the Cisco IDS Host Console. Open Windows Explorer. Choose **Tools > Map Network Drive**.



In the Folder dialog box, enter the full Universal Naming Convention name and path of the Cisco IDS Host Sensor Console and its corresponding directory (similar to \\console-pc\c$\Program Files\Cisco IDS\Console). Click **Finish**. Later, you will be prompted to enter the drive letter to obtain a key.



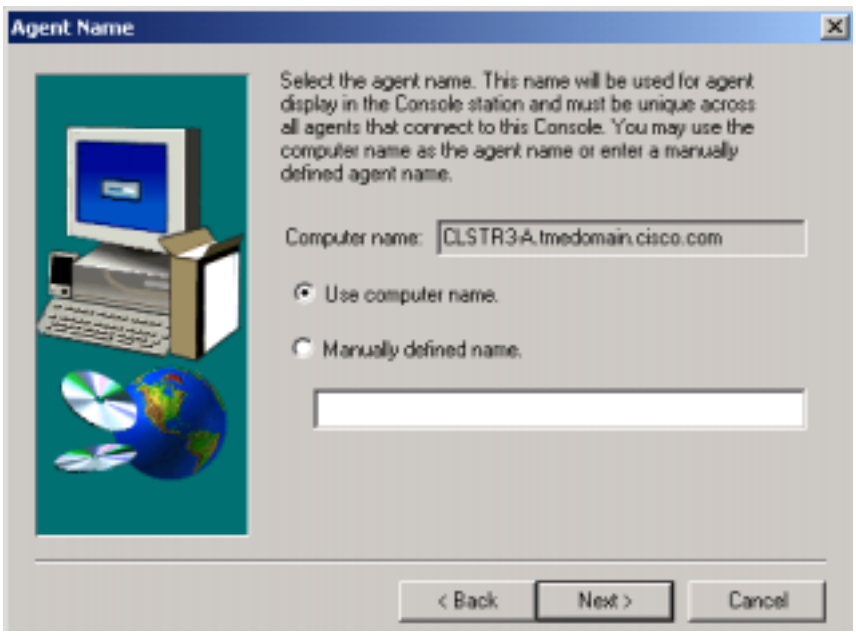
If you are installing only the Cisco IDS Host Sensor Agent, you put in the CD and start with this same splash screen. Click the **Install Agent** option as shown below. If you are installing more than the Console, you will immediately move to the agent installation screen on the next page.



After reading the welcome screen, click **Next**.

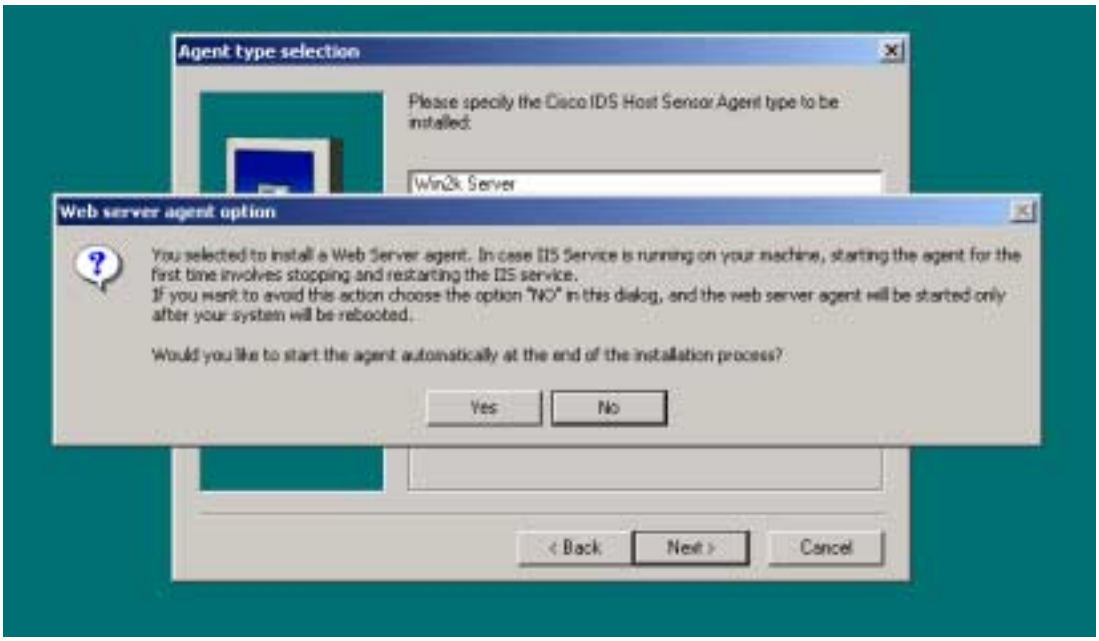
After entering your name and company, click **Next**.

Choose **Use Computer Name** and click **Next**.



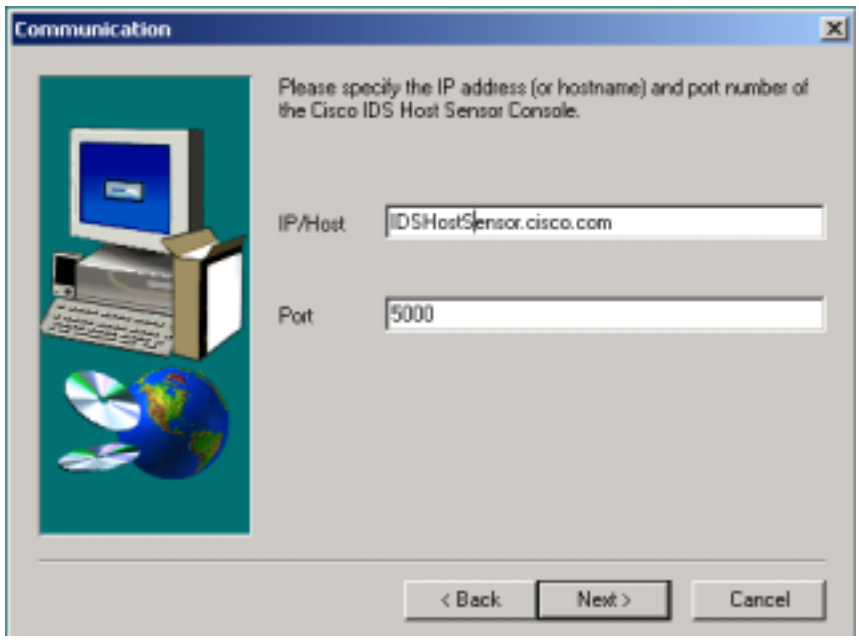
Choose **Win2k Server** and click **Next**.

Click **Yes,** so the agent will automatically start at the end of the installation.



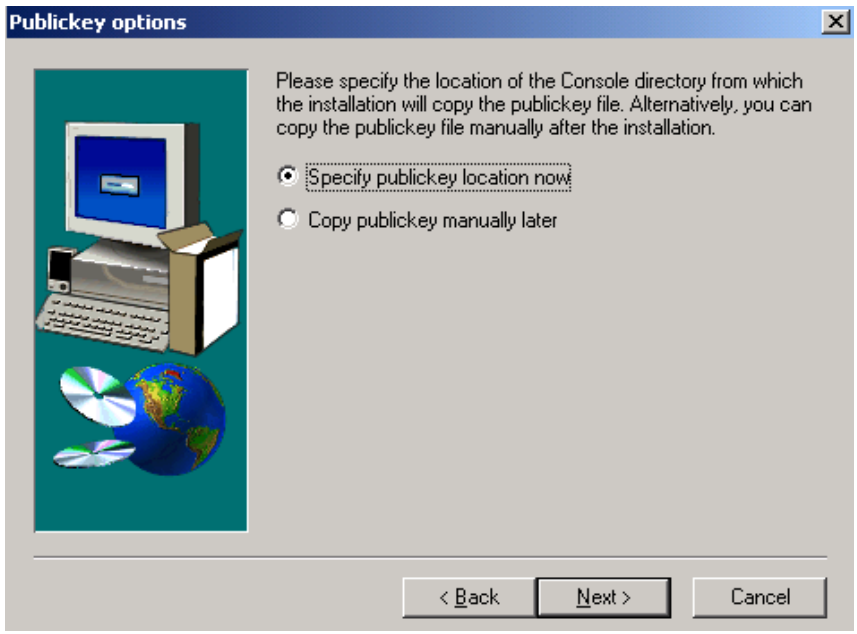
After choosing the destination location, click **Next**.

Enter the host name or IP address of the Cisco IDS Host Sensor Console and then click **Next**.

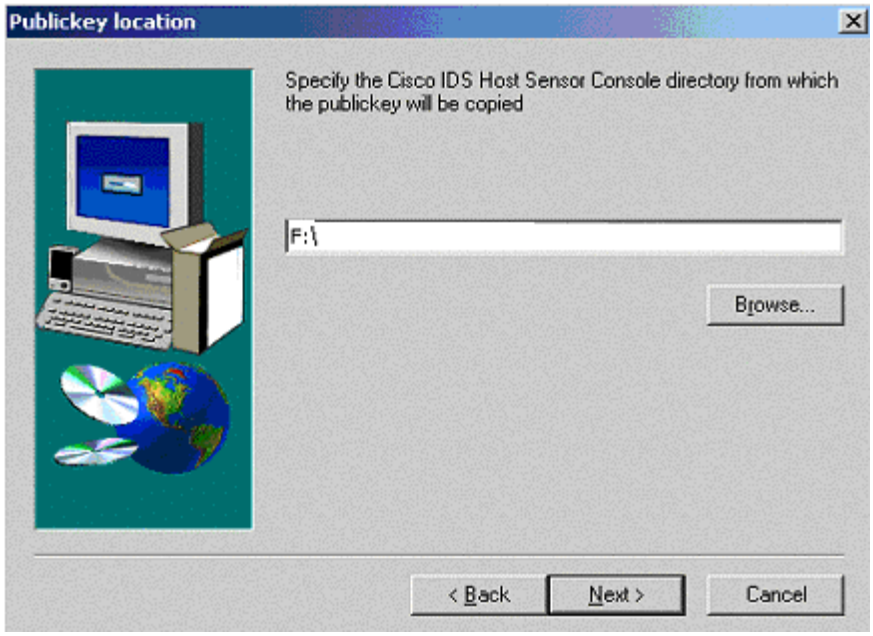


After reviewing the current settings, click **Next**.

Choose **Specify publickey location now** and click **Next**.



The next figure shows where to specify the new drive that was mapped. If the full path to the remote Console directory was mapped, enter F:\ in the box and click **Next**.



Configuration Steps

Step 1. Create the Agent Groups.

Open the Console and click the **Agents** button in the quick-select panel on the left.

Note: Use **Administrator/Administrator** as the default username and password; passwords are case-sensitive.

From the **Agent** menu**,** choose **New Agent Group** or click the **New Agent Group** button.

The Agent Group Properties box displays.

Enter the agent group name in the field that is titled **Group Name** and click the tab that is labeled **Agents**.

Two windows display. **All Agents** identifies the first window, and **Agents in Group** identifies the second window.

In the left window, highlight the agents that you want to be in the group (hold select to pick more than one and click the **Add** button). After the agents are in the new group, remove the agents from the group that is labeled **New Agents**.

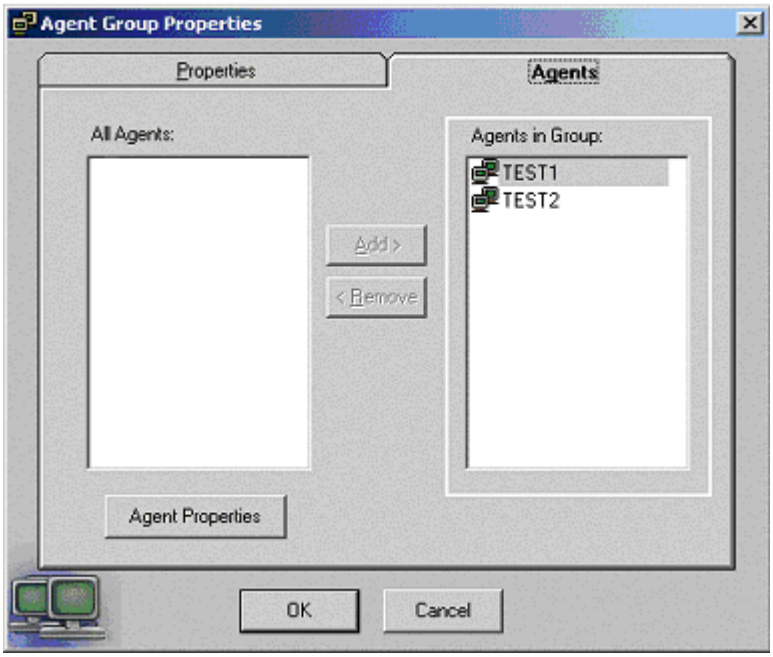
Two Agent Groups should be created. Create the types of agents that you need in your deployment.

Cisco CallManagers—Group servers in a Cisco CallManager cluster (publisher and subscribers)

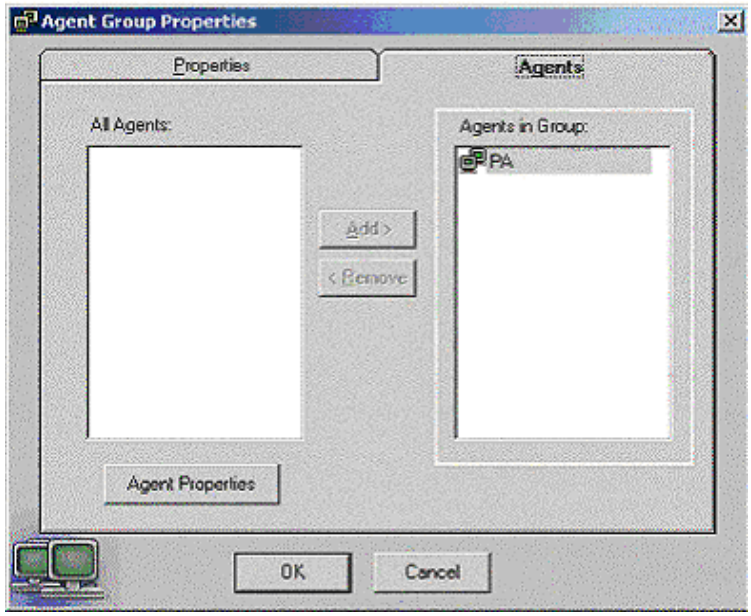
Productivity application servers—Group for personal assistant server

The following screenshots show examples of each Agent Group Properties page:

Cisco CallManager Agent Group Properties 1 (TEST1 and TEST2 represent example names of two different Cisco IDS agents that are running on two different Cisco CallManagers.)



Productivity Applications Server Group Properties 1 (PA represents an example of a Cisco IDS agent that is running on a productivity applications server.)

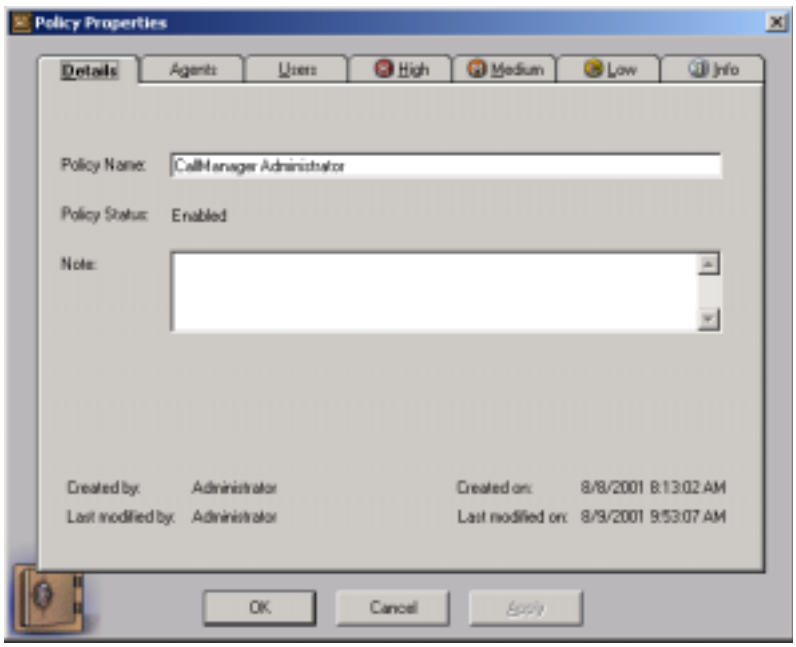


Step 2. Create the Security Policies.

Click the **Policies** button on the quick-select panel.

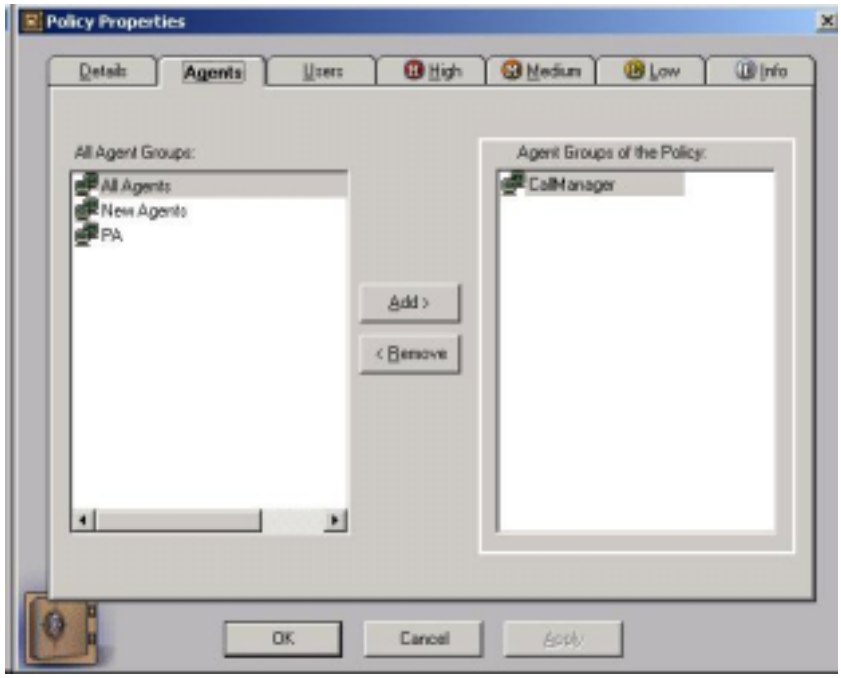
Choose **New** from the **Policies** menu or click the **New Policy** button.

The **Policy Properties** window displays. Enter the policy name in the **Policy Name** field.



Click the **Agents** tab. Two windows display. The label for the window on the left specifies All Agent Groups, and the label for the window on the right specifies Agent Groups of the Policy.

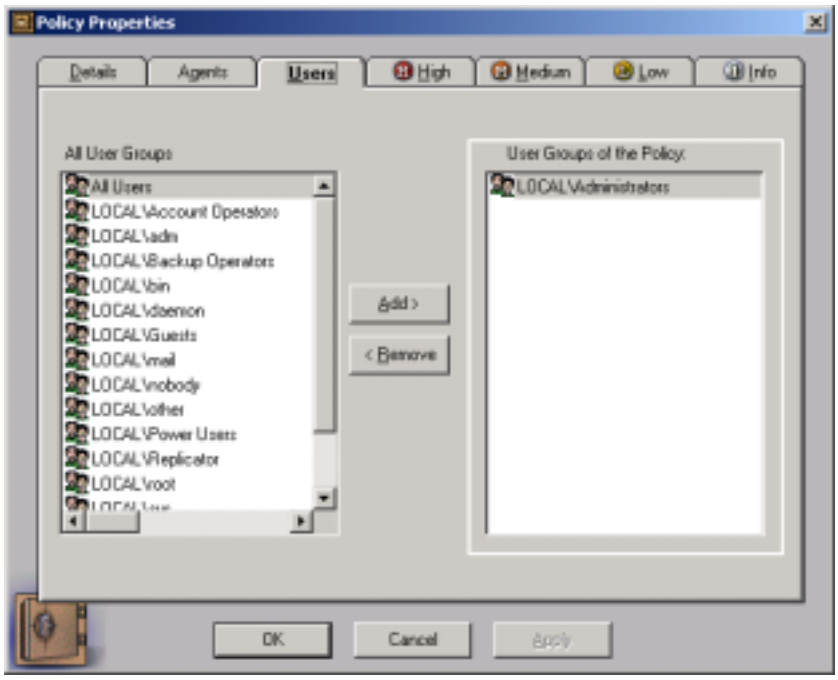
Highlight the agent groups on the left that you want to be in this policy and click the **Add** button.



Click the **Users** tab. Again, two windows display. The label for the left window specifies All User Groups and the label for the right window specifies User Groups of the Policy.

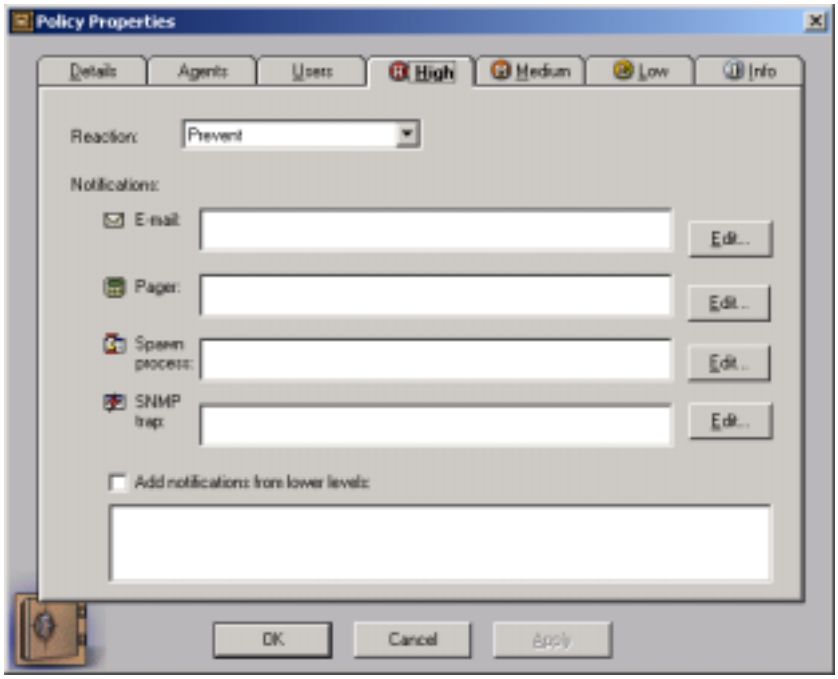
Highlight **All Users** in the User Groups of the Policy windows and click the **Remove** button.

Highlight **LOCAL\Administrators** in the All User Groups list and click the **Add** button.



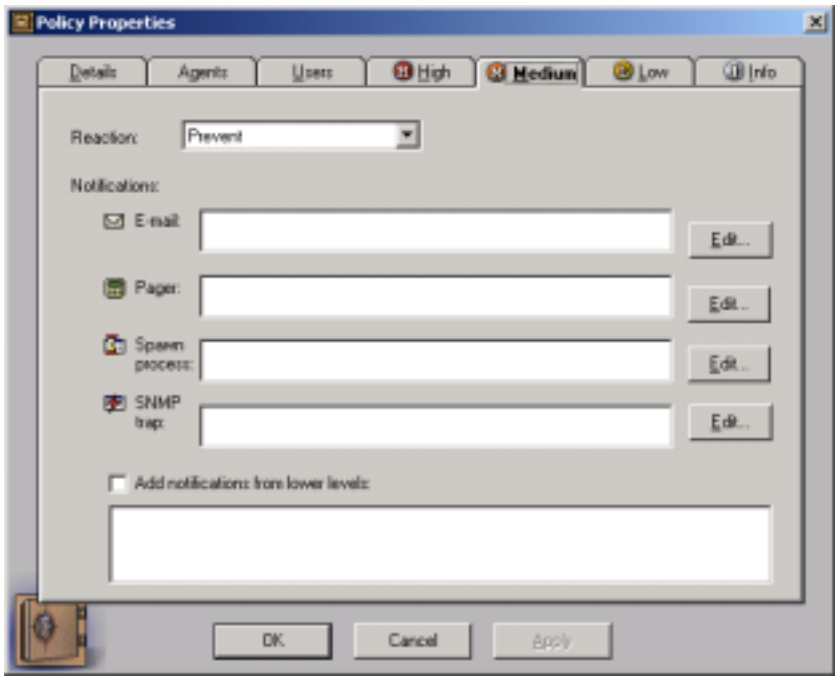
Click the **High** tab. Several fields display.

From the Reaction drop-down box, choose **Prevent**.



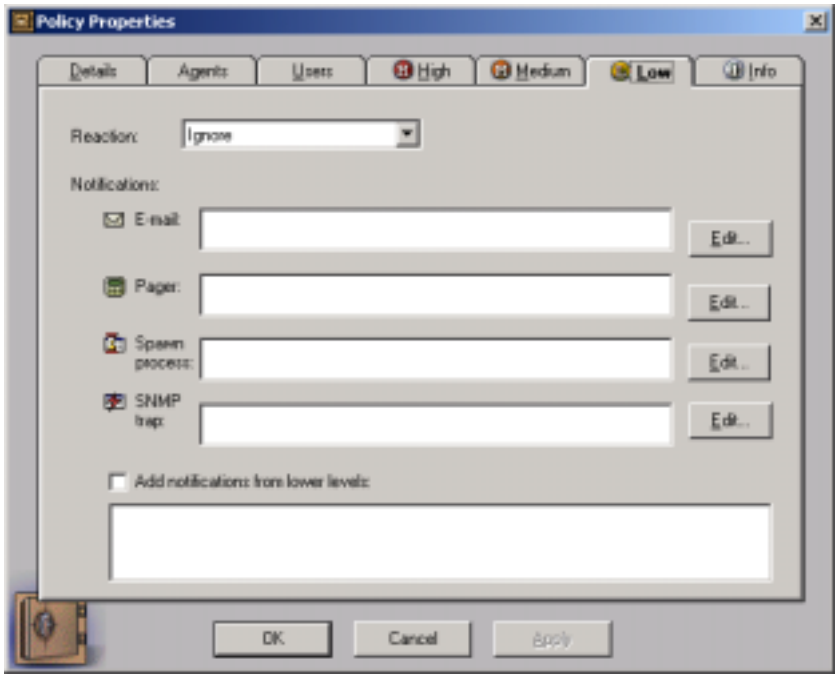
Click the **Medium** tab.

From the Reaction drop-down box, choose **Prevent**.



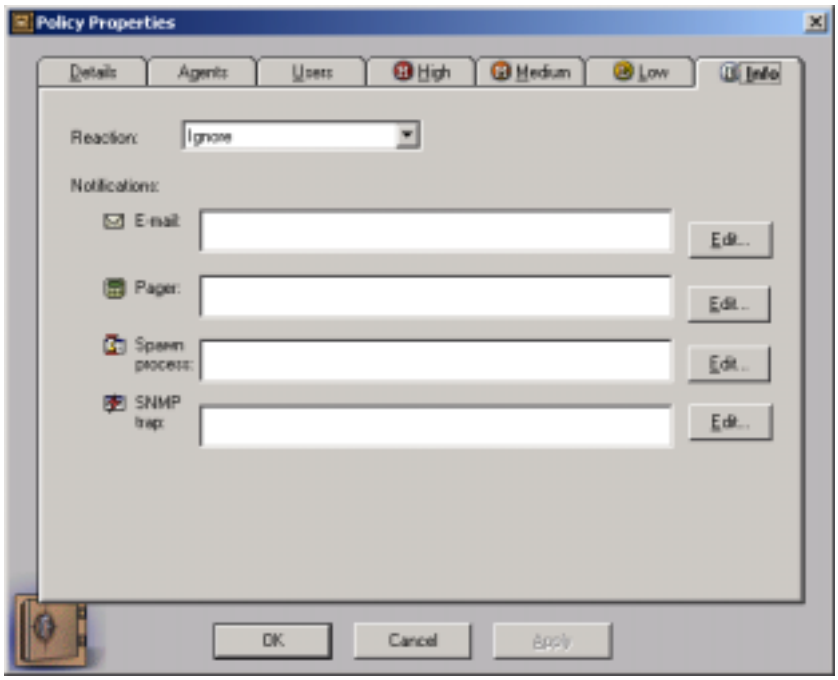
Click the **Low** tab.

From the Reaction drop-down box, choose **Ignore**.



Click the **Info** tab.

From the Reaction drop-down box, choose **Ignore**.



If you have productivity servers, repeat the same steps that were previously outlined above for each server.

Assuming you had all these types of servers, the following two policies were created:

Cisco CallManager Administrator—Contains the Cisco CallManager Agent Group.

Productivity applications servers—Contains the Productivity Applications Server Group.

Step 3. Modify the Access Levels for the Security Signatures.

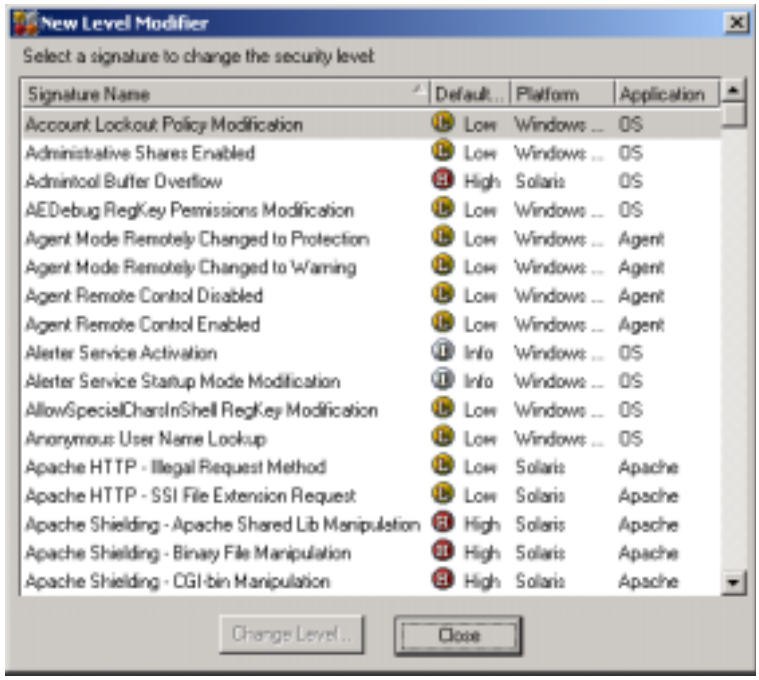
Note: Because this step is extremely important, be sure to complete it correctly.

After the agent groups and security policies are created, you need to modify the access levels on the security signatures. You will assign proper access to critical processes that run on the server. If you do not make these modifications, Cisco CallManager or productivity applications may not run correctly.

On the quick-select panel on the left, click the **Levels** button.

From the Levels menu, choose **New** or click the **New Level Modifier** button.

The New Level Modifier window displays a list of the security signatures.



Highlight the signature to be modified and click the **Change Level** button or double-click it.

Click the **Security Level** tab and choose **For Specific Groups** under Current Security Level.

A new window displays the current list of groups and their security levels.

You need to modify the following list of signatures. For these signatures, set the security level to **low**. Failure to do so will disable Cisco CallManager.

IIS Envelope—File Access by IIS Process

Cisco CallManager—Needed to access admin pages

IIS Envelope—File Access by IIS Web User

Cisco CallManager—Needed for Cisco CallManager maintenance (view trace files, for example)

IIS Envelope—File Execution by IIS Web User

Cisco CallManager—Needed for CallManager maintenance (view trace files, for example)

IIS Envelope—File Modification by IIS Process

Cisco CallManager—Needed for Web access to admin pages

IIS Envelope—File Modification by IIS Web User

Cisco CallManager—Needed for Web access to admin pages

IIS Envelope—Registry Access by IIS Process

Cisco CallManager—Needed for JTAPI logins, and other [ ]

IIS Envelope—Registry Access by IIS Web User

Cisco CallManager—Needed to access Java application through Web interface (Admin Serviceability Tool, for example)

IIS Jet Database Command Execution

Cisco CallManager—Used to update database when logged into Cisco CallManager user pages

IIS Shielding—Service Access

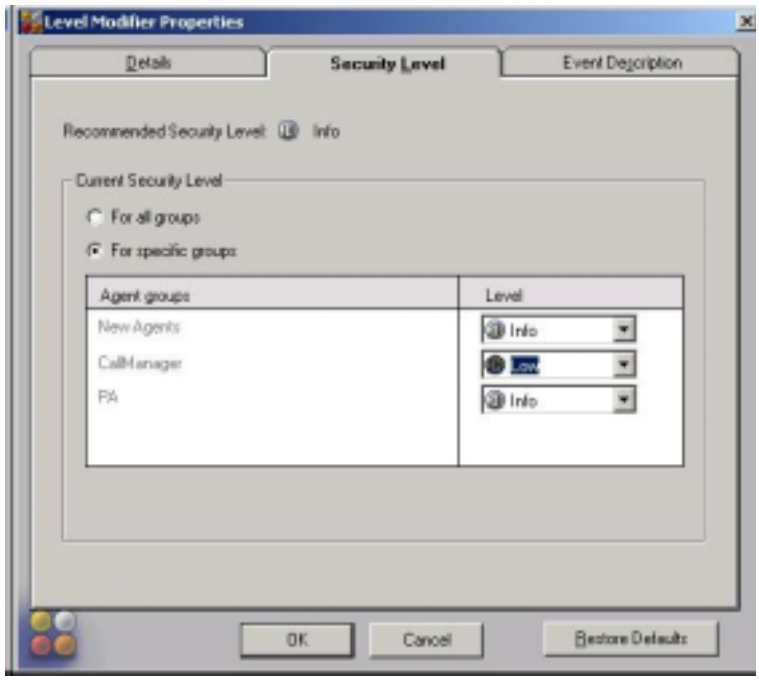
Cisco CallManager—Needed for system maintenance (restarting services, for example)

Note: For Cisco CallManager 3.2 and 3.3, add these two signatures:

IIS Envelope—File Execution by IIS Process

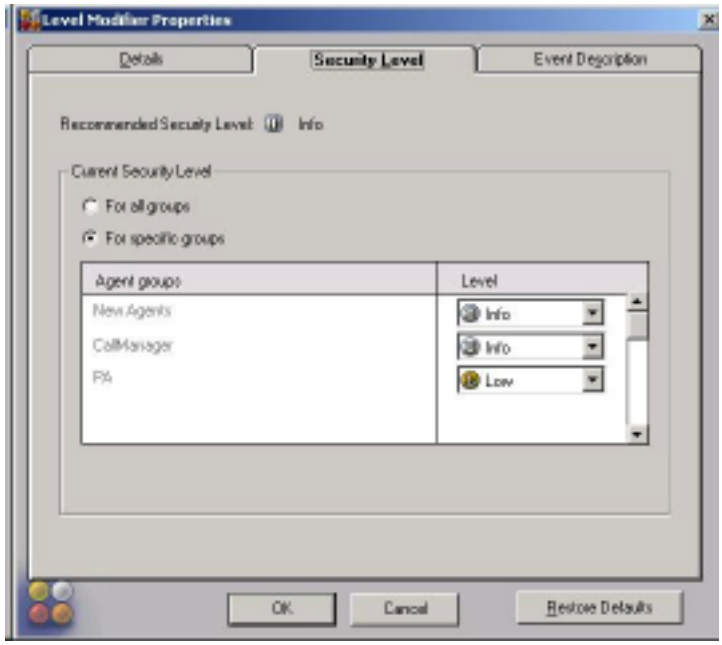
IIS Shield—Illegal Request

All access-level modifications for Cisco CallManager display as shown in the following figure.



IIS Shielding—File Access

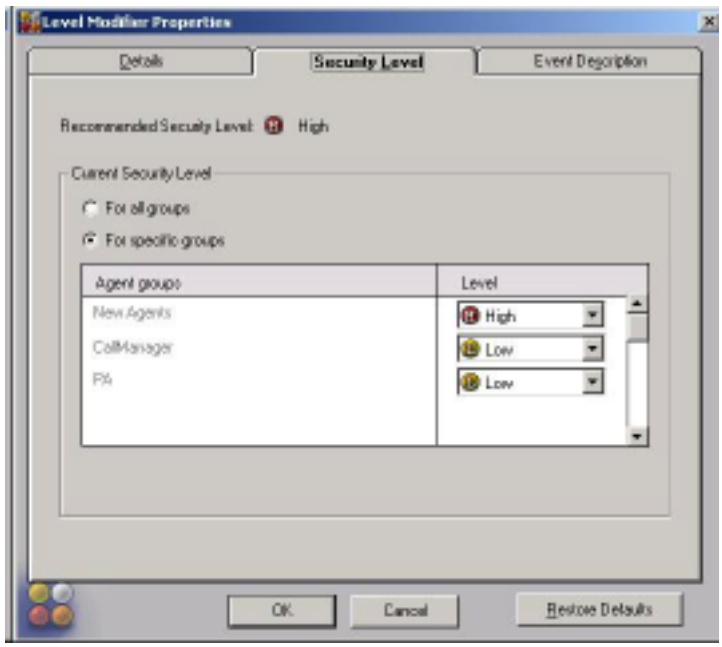
Personal Assistant—Used to update the database by using admin pages. Set the level to **low**.



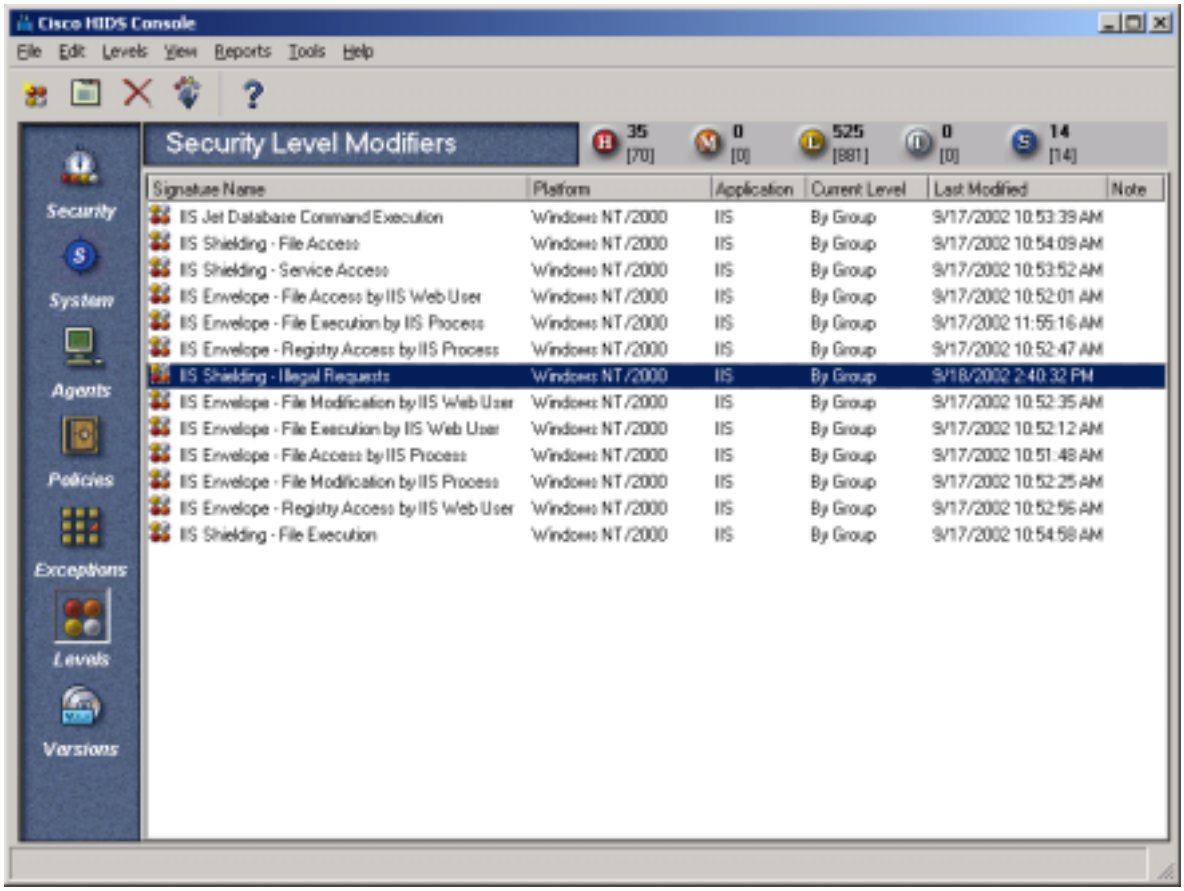
IIS Shielding—File Execution

Cisco CallManager—Needed for system maintenance (restarting services). Set the level to **low**.

Personal Assistant—Used to update database by using admin pages. Set the level to **low**.



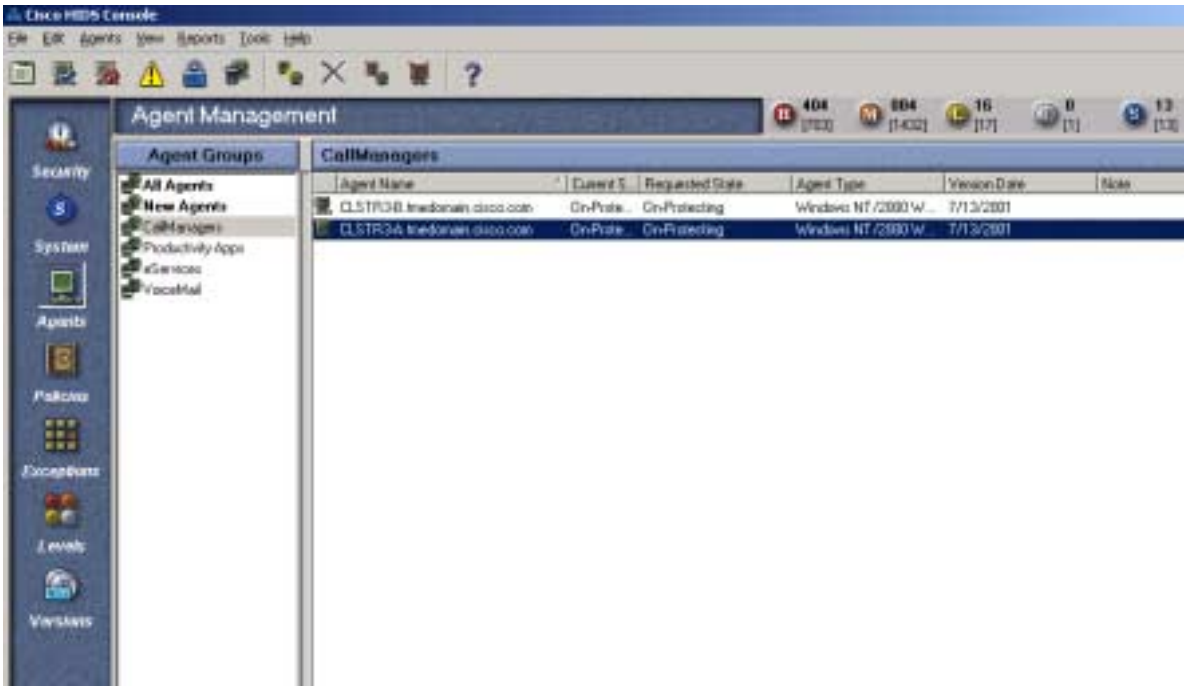
The new signatures, including the ones that were added for Cisco CallManager 3.2 and 3.3, display as shown in the following figure.



Step 4. Activate the Agents.

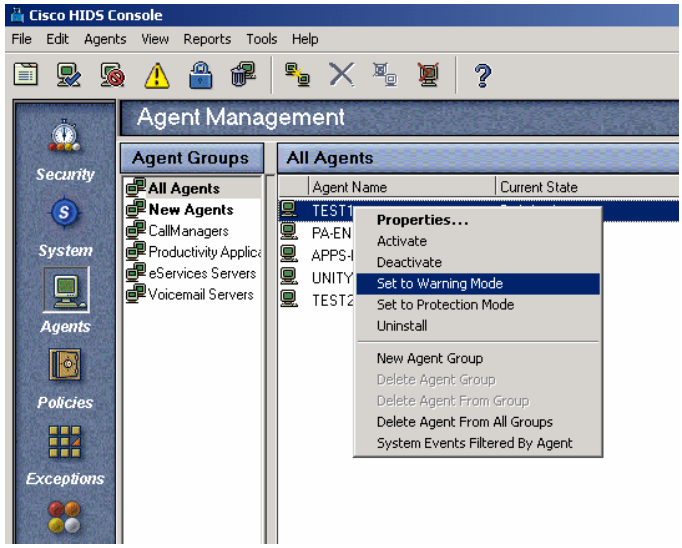
To activate the agents, click the **Agents** icon on the left side of the screen. Next, click the **All Agents** group. Right-click the first agent in the list and choose **Set To Protection Mode**. Repeat this step for all agents. The Agent Management screen will now show each agent in On-Protecting Mode as shown below.

Important: If you do not complete this step, the Cisco IDS Host Sensor Agent will not block attacks.

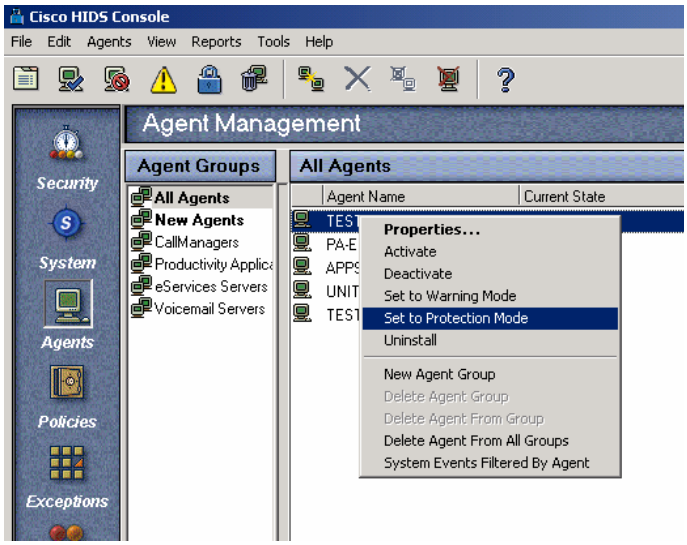


Upgrading Cisco CallManager and Installing New Software

Any installation of any new software on the Cisco CallManager requires the Cisco IDS Agent to be set to **Warning** mode instead of **Protection** mode. This includes upgrades to Cisco CallManager as well as installations of other plugins, such as the Administrative Reporting Tool (ART) or Bulk Administration Tool (BAT). Prior to performing an upgrade, the agent that is associated with the Cisco CallManager should be put in **Warning** mode. In **Warning** mode, the agent will not attempt to interfere with the install package.



After Cisco CallManager or other application plugin successfully has been upgraded or installed, restart the server. Finally, return the agent to **Protection** mode.

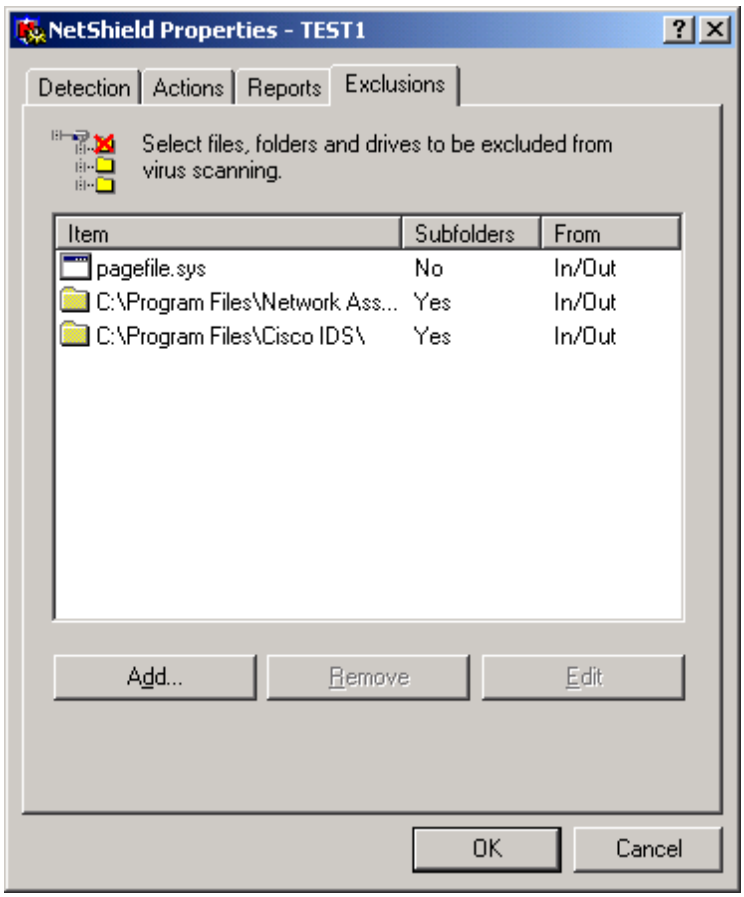


Important: You must return the agent to protection mode; otherwise, your server will not be protected.

Caveats

Using Cisco Host IDS Sensor Agent and McAfee NetShield

For McAfee NetShield and the Cisco Host IDS Sensor Agent to coexist on the same server, configure McAfee to not scan the directory where the Cisco Host IDS Sensor Agent or Console is installed. The following figure shows an example:



The full path that should be excluded is c:\Program Files\Cisco IDS\. Include all subfolders for this directory, so McAfee will not scan any directory or file under the Cisco IDS folder.

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.
Capital Tower
168 Robinson Road
#22-01 to #29-01
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 Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia 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

203020.B/ETMG 02/03