

# Installing and Configuring the Cisco IDS Host Sensor on Cisco CallManager 3.0 and 3.1

Document ID: 17736

---

## Introduction

### Prerequisites

- Requirements
- Components Used
- Conventions

### Installation Procedure

- Install the Cisco IDS Host Sensor Console
- Install the Cisco IDS Host Sensor Agent

### Configuration Procedures

- Create Agent Groups
- Create the Security Policies
- Modify the Access Levels for the Security Signatures
- Activate the Agents

### Upgrade Cisco CallManager and Install New Software

### Caveats

- Use Cisco Host IDS Sensor Agent and McAfee NetShield

### Related Information

---

## Introduction

Security is important in any company's infrastructure. When that infrastructure includes servers performing call processing and networks carrying voice, the importance is even more clear. The recent Code Red virus was a wake-up call to many companies who had taken a lax view of security. Not only were servers running IIS affected, but whole networks were brought to a crawl by the propagation of this virus.

The Cisco IDS Host Sensor, powered by Entercept, is a great weapon in the security war. It must be emphasized that this product is not a substitute for poor network design and poor Windows security practices. A secure network and a secure Windows 2000 platform must first be built before adding this product. The Cisco IDS Host Sensor is the last line of defense that helps ensure that the Cisco CallManager will be protected against hacks and attacks of many kinds.

## Prerequisites

### Requirements

There are no specific requirements for this document.

### Components Used

The information in this document is based on these software and hardware versions:

- Cisco CallManager 3.0 and 3.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure

that you understand the potential impact of any command.

## Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

## Installation Procedure

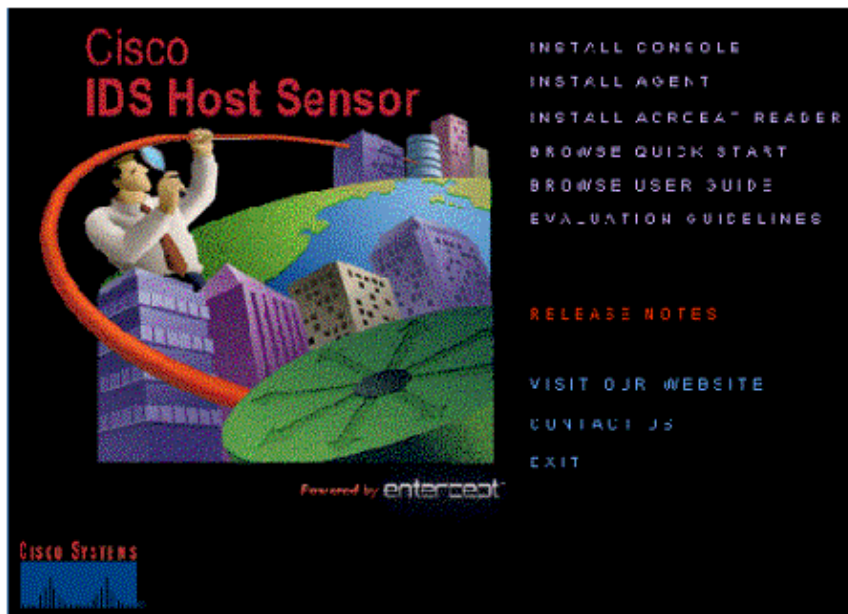
The installation of the Cisco IDS Host Sensor is fairly simple. The first step is to install the Console. The Console is the place where all security alerts and notifications will be sent and displayed. This can be installed on any machine. The next step is to install the Cisco IDS Host Sensor Agent on the same server as the Cisco IDS Host Sensor Console, and on all of the Cisco CallManagers. They would then send their notifications to the Cisco IDS Host Sensor Console.

For a small deployment, the Cisco IDS Host Sensor Console can be installed on the Publisher if desired. Ideally, the Console should reside on a separate machine.

### Install the Cisco IDS Host Sensor Console

Complete these steps:

1. When the CD is inserted into the CD-ROM drive, a splash screen will appear. Choose the **Install Console** option.

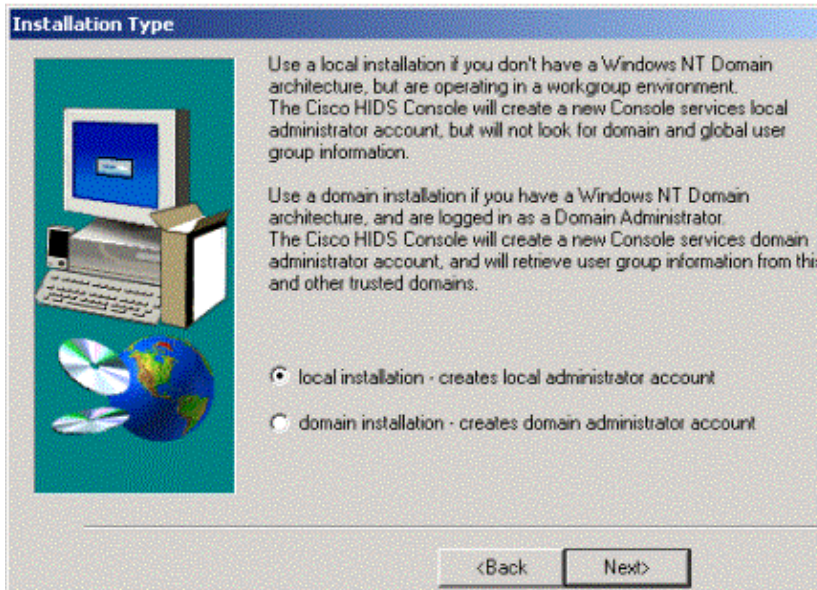


2. Click **Next** to begin the install.



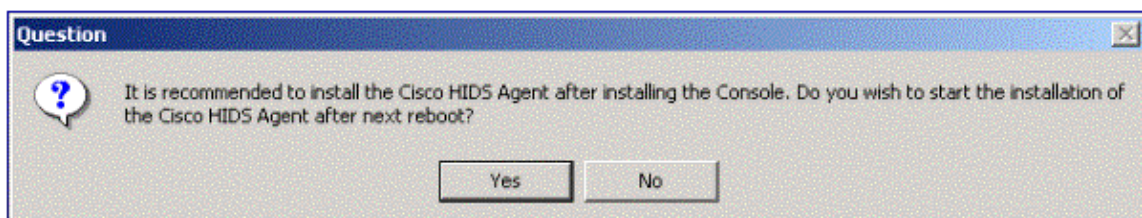
3. Click **Accept** to accept the License Agreement.
4. Click **Next** after reading the product information and after choosing the Destination Folder.

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

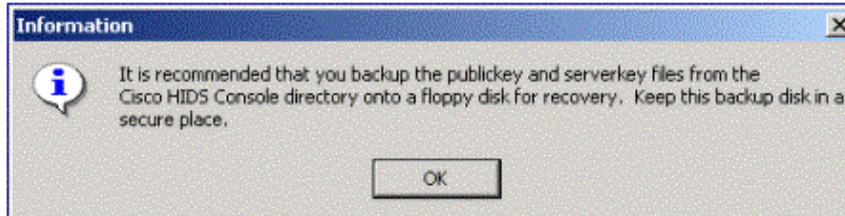


5. Click **Next** after selecting the Program Folders and after reviewing the current settings.

**Note:** You want the Cisco IDS Host Sensor Agent to run on the same machine as the Cisco IDS Host Console. The Cisco IDS Host Console needs protection, too. Click **Yes**.



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

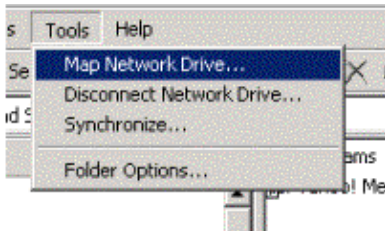


If prompted, restart your server.

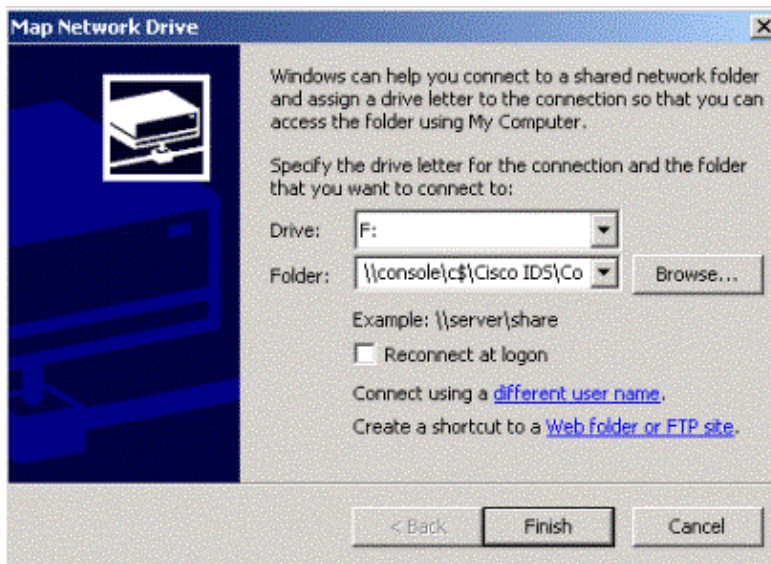
## Install the Cisco IDS Host Sensor Agent

Use this procedure to install the Cisco IDS Host Sensor Agent.

1. Before installing the Cisco IDS Host Sensor Agent on a separate machine, it is important to map a drive to the Cisco IDS Host Console. Open up the File Explorer. Select **Tools > Map Network Drive**.

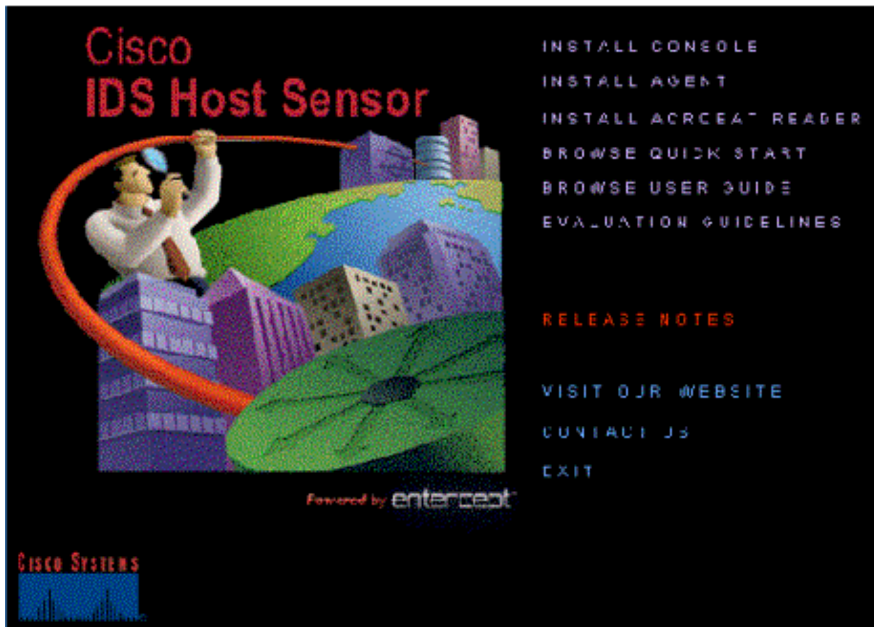


2. In the dialog, put the full UNC name and path of the Cisco IDS Host Sensor Console and its corresponding directory; for example: \\console-pc\c\$\Program Files\Cisco IDS\Console.
3. Click **Finish**. Later, you will be prompted to enter the drive letter to obtain a key.

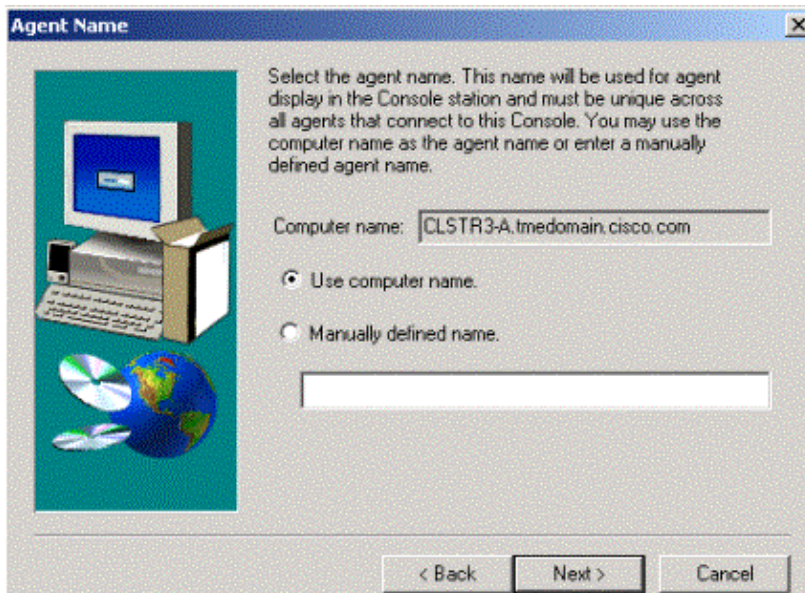


4. If you are only installing the Cisco IDS Host Sensor Agent, you will put in the CD and start with this same splash screen. Click the **Install Agent** option.

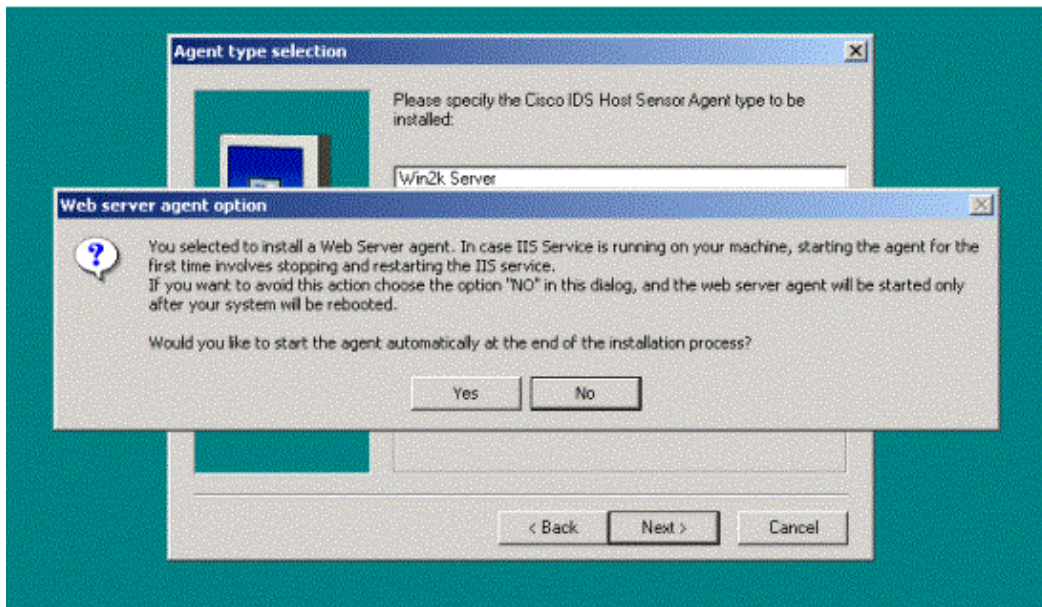
If you are continuing on from the Console installation, you immediately move to the Agent installation screen on the next page.



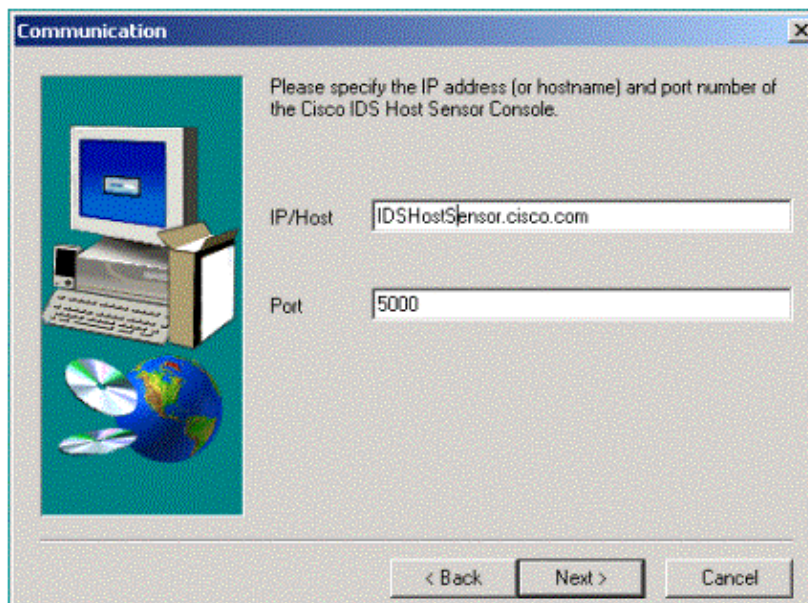
5. Read the Welcome screen, enter the Name and Company and click **Next**.
6. Select **Use Computer Name** and click **Next**.



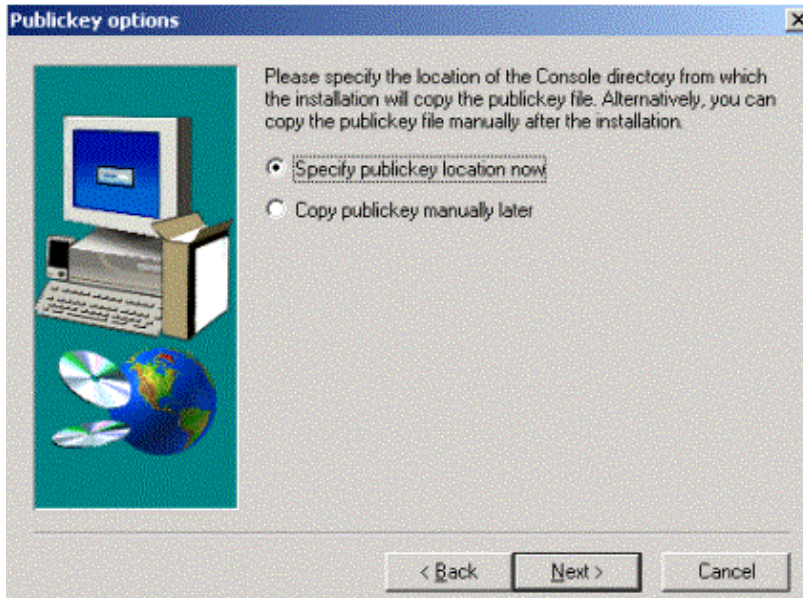
7. Select **Win2k Web Server** and click **Next**.
8. Click **Yes** so the agent will automatically start at the end of the installation.



9. Select the **Destination Location**, then click **Next**.
10. Put in the hostname or IP Address of the Cisco IDS Host Console and click **Next**.

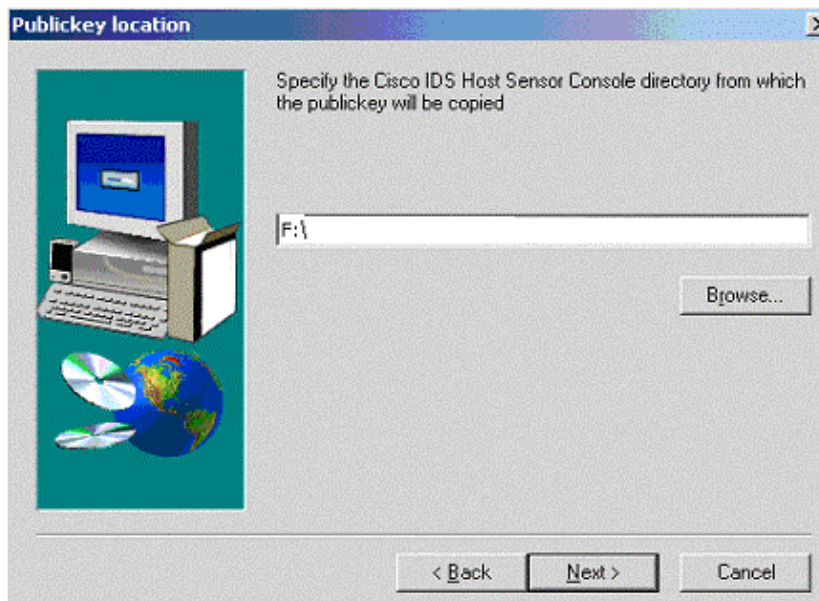


11. Review the current settings, then click **Next**.
12. Choose **Specify publickey location now** and click **Next**.



13. Specify the new drive that was mapped.

If the full path to the remote Console directory was mapped, then `f:\` should be the only thing that needs to be entered in the box below. Click **Next**.



## Configuration Procedures

### Create Agent Groups

Complete these steps to create agent groups.

1. Open the console and click **Agents** in the quick-select panel on the left.

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

2. Select **New Agent Group** from the Agent menu, or click **New Agent Group**.

The Agent Group Properties box is displayed.

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

Two windows are displayed. The first is labeled All Agents, and the second is labeled Agents in Group.

4. Highlight the agents you want to be in the group in the left window (hold select to pick more than one) and click **Add**.

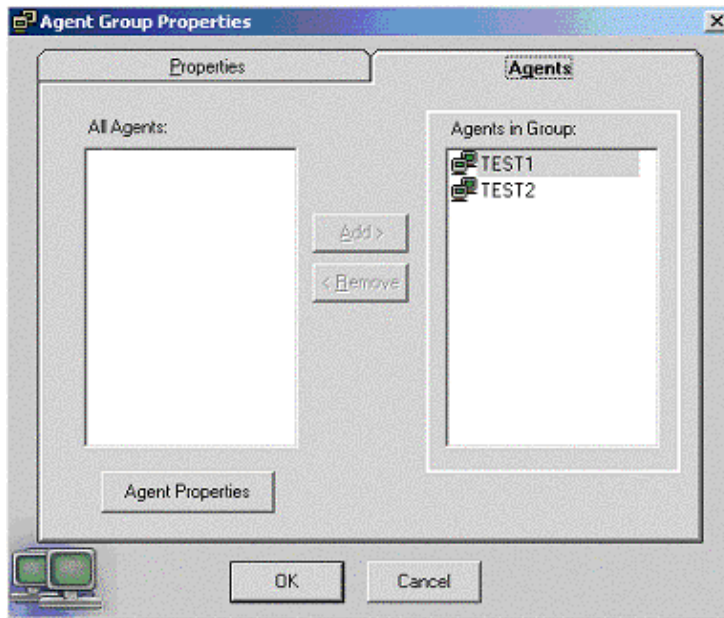
Once the agents are in the new group, remove the agents from the group labeled New Agents.

5. Two Agent Groups are created.

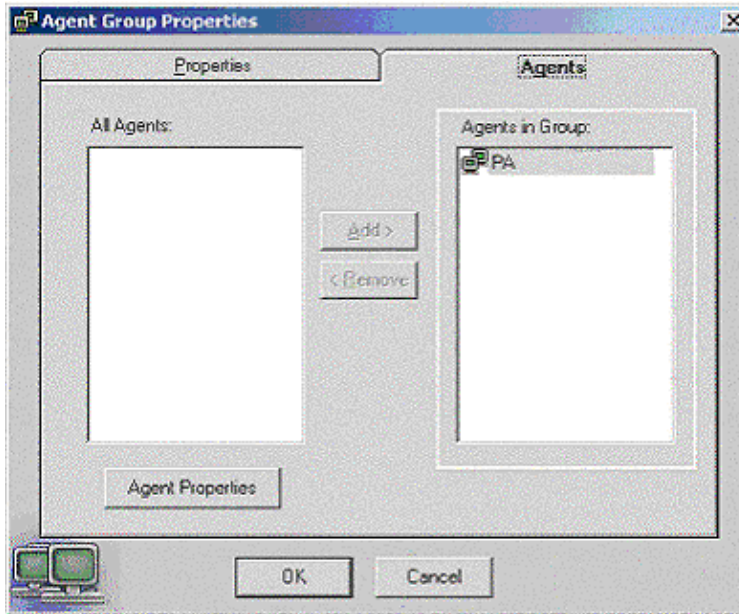
Create the types of Agents you need in your deployment.

- ◆ CallManagers group servers in CallManager cluster (publisher and subscribers).
- ◆ Productivity Application Servers group for Personal Assistant Server

A sample of each of the Agent Group Properties pages is shown below.



**CallManager Agent Group Properties 1 (Test1 and Test2 are example names of two different IDS Agents running on two different CallManagers)**

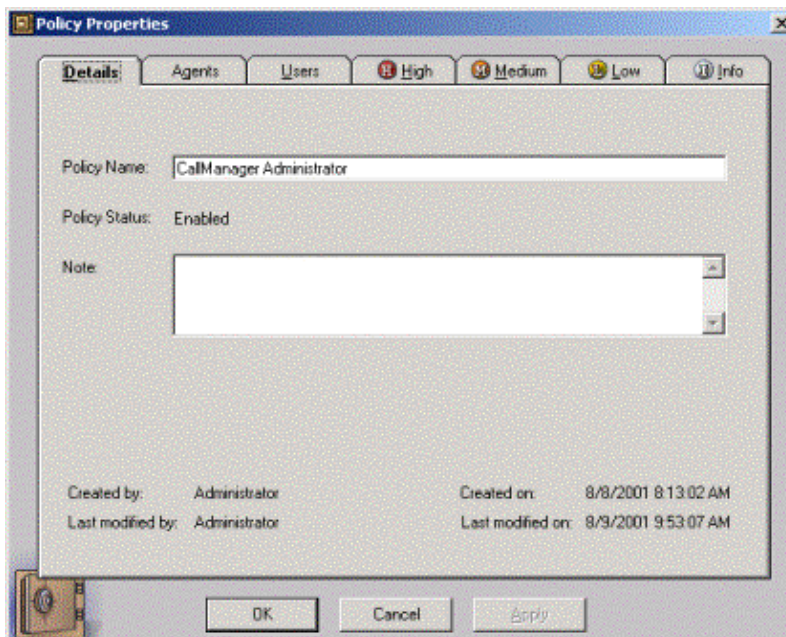


Productivity Applications Servers Group 1 (PA is an example of an IDS Agent running on a PA server)

## Create the Security Policies

Use this procedure to create security policies.

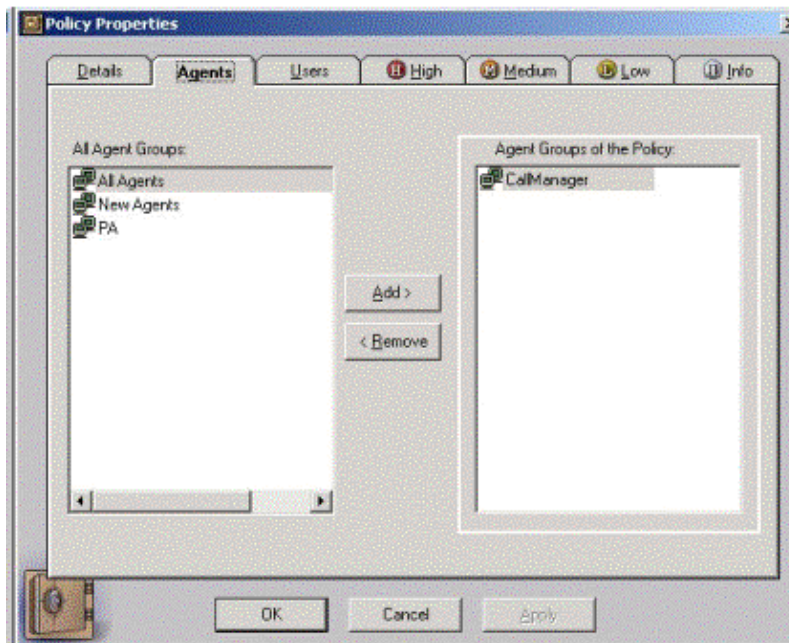
1. Click the **Policies** button on the quick select panel and select **New** from the Policies menu or click the **New Policy** button. The Policy Properties windows is displayed.
2. Enter the policy name in the field labeled Policy Name.



3. Click the **Agents** tab.

Two windows are displayed. The window on the left is labeled All Agent Groups, and the window on the right is labeled Agent Groups of the Policy.

4. Highlight the agent groups you want to be in this policy, and click the **Add** button.

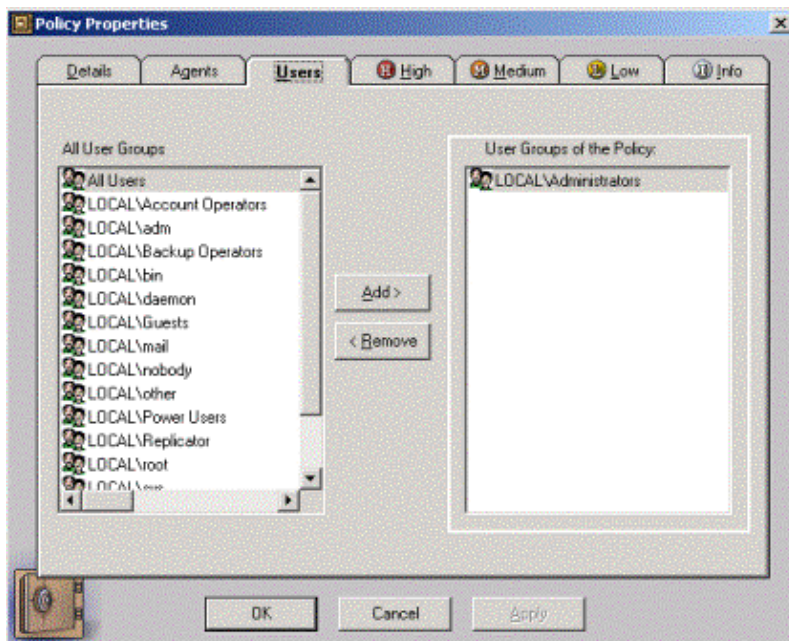


5. Click the **Users** tab.

Two windows are displayed. The left window is labeled All User Groups, and the right is labeled User Groups of the Policy.

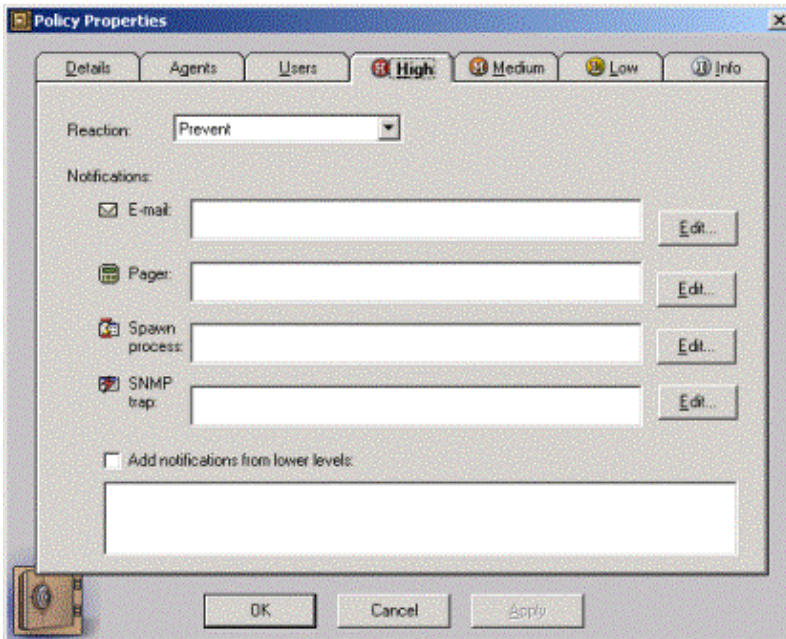
6. Highlight **All Users** in the User Groups of the Policy windows and click the **Remove** button.

7. Highlight **LOCAL/Administrators** in the All User Groups windows and click the **Add** button.

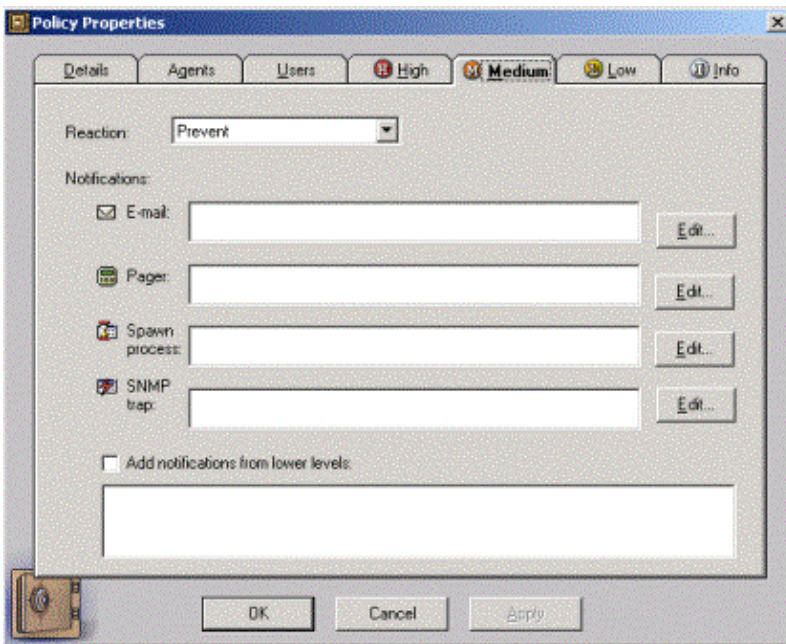


8. Click the **High** tab. Several fields are displayed.

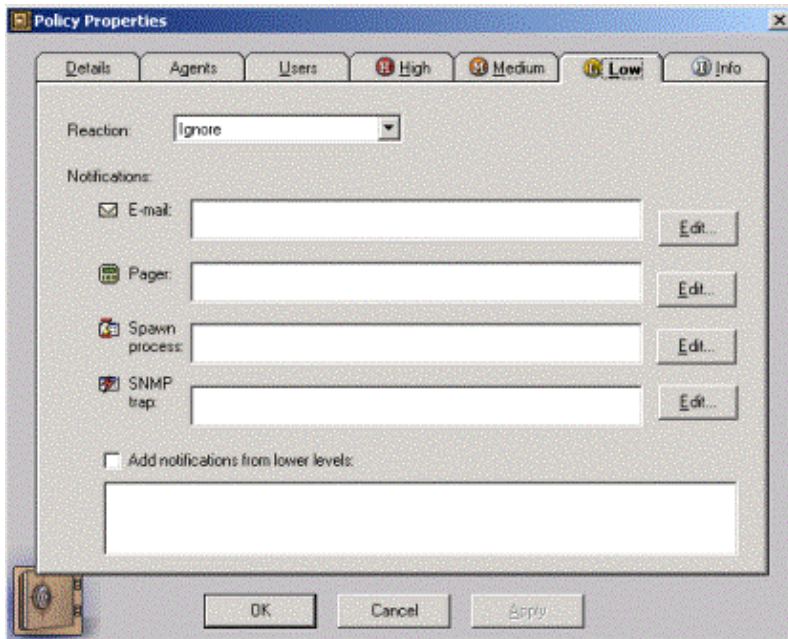
9. Select **Prevent** from the Reaction drop down box.



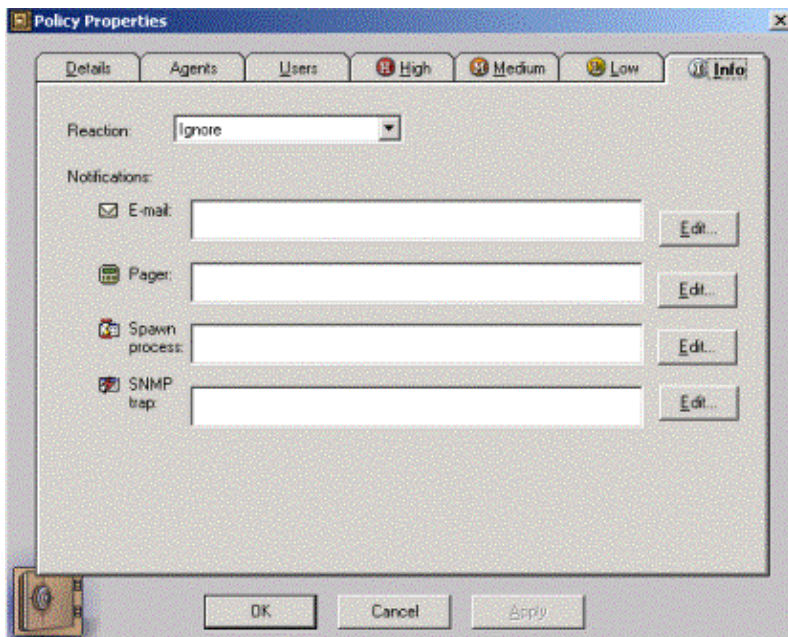
10. Click the **Medium** tab.
11. Select **Prevent** from the Reaction drop down box.



12. Click the **Low** tab.
13. Select **Ignore** from the Reaction drop down box.



14. Click the **Info** tab.
15. Select **Ignore** from the Reaction drop down box.



16. If you have Productivity Servers, repeat the same steps outlined above.

In total, assuming you had all of these types of servers, the following two policies are created:

- ◆ CallManager Administrator contained the CallManager Agent Group
- ◆ Productivity Apps contained the Productivity Applications Server Group

## Modify the Access Levels for the Security Signatures

Once the Agent Groups and Security Policies are created, it is time to modify the Access Levels on the security signatures. This step is extremely important. Here, you assign proper access to critical processes that run on the server.

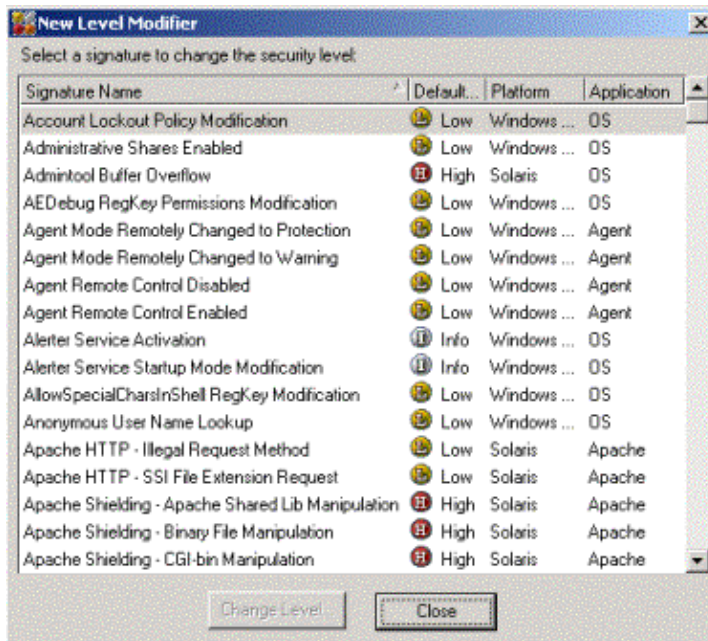


**Caution:** If you do not make these modifications, it could prevent the Cisco CallManager or

Productivity Apps from running correctly.

1. Click the **Levels** button on the quick select panel on the left.
2. Select **New** from the Levels menu or click the **New Level Modifier** button.

A window titled New Level Modifier opens, displaying a list of the security signatures.



3. Highlight the signature to be modified and click the **Change Level** button, or double-click it.
4. Click the **Security Level** tab and select **For Specific Groups** under Current Security Level.

A new window appears displaying the current list of groups and their security level.

5. Modify the following list of signatures.

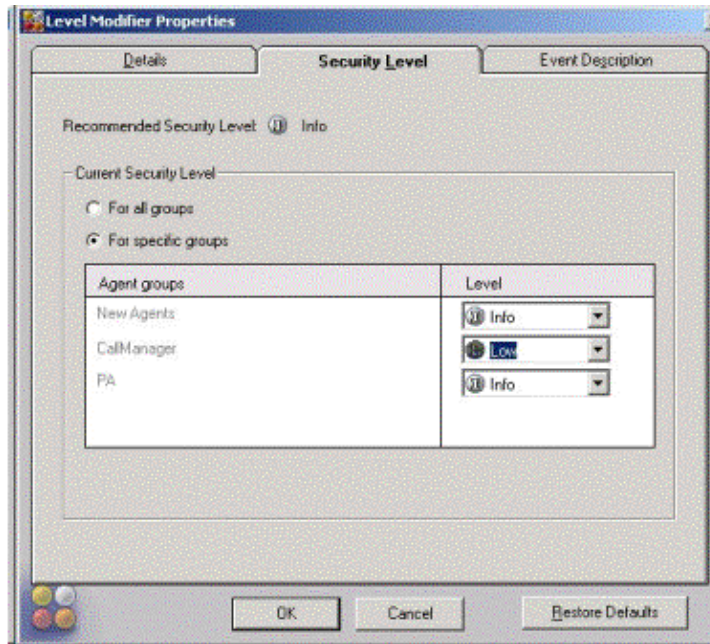
For these signatures, set the security level to **LOW**.



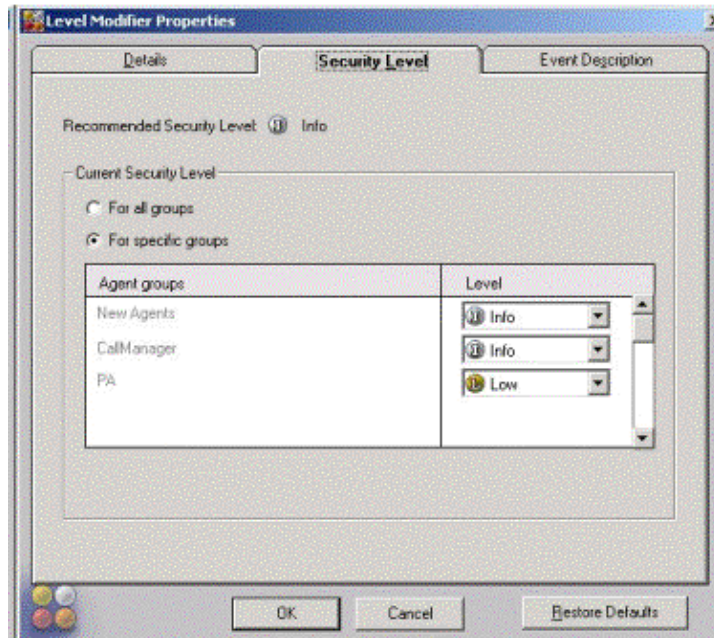
**Caution:** Failure to set the security level to LOW will result in the Cisco CallManager becoming dysfunctional.

- ◆ **IIS Envelope File Access by IIS Process** – CallManager needed to access admin pages
- ◆ **IIS Envelope File Access by IIS Web User** – CallManager needed for CallManager maintenance (view trace files)
- ◆ **IIS Envelope File Execution by IIS Web User** – CallManager needed for CallManager maintenance (view trace files)
- ◆ **IIS Envelope File Modification by IIS Process** – CallManager needed for web access to admin pages
- ◆ **IIS Envelope File Modification by IIS Web User** – CallManager needed for web access to admin pages
- ◆ **IIS Envelope Registry Access by IIS Process** – CallManager needed for JTAPI logins
- ◆ **IIS Envelope Registry Access by IIS Web User** – CallManager – needed to access java application via web interface (Admin Serviceability Tool)
- ◆ **IIS Jet Database Command Execution** – CallManager used to update database when logged into CallManager user pages
- ◆ **IIS Shielding Service Access** – CallManager needed for system maintenance (restarting services)

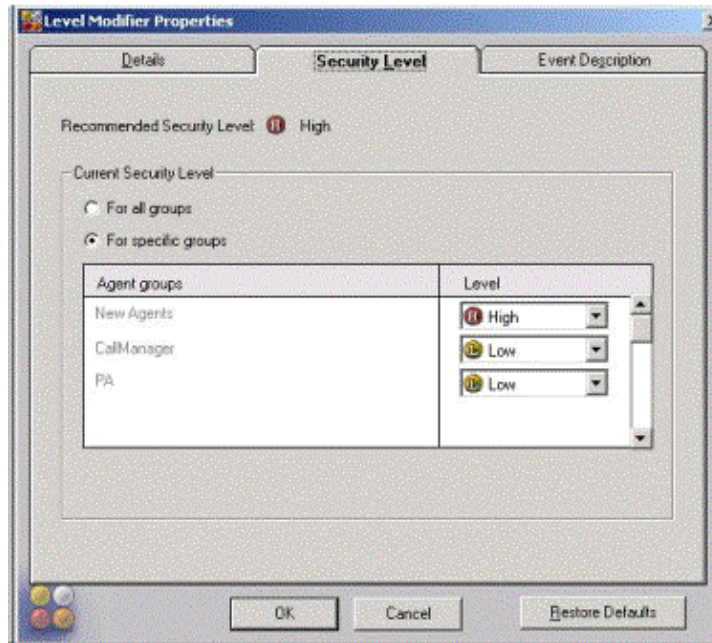
All Access Levels Modifications for CallManager will look like this.



- ◆ **IIS Shielding File Access** – Personal Assistant used to update database via admin pages. Set the Level to LOW.



- ◆ **IIS Shielding File Execution** – CallManager needed for system maintenance (restarting services). Set the level to LOW. Personal Assistant used to update database via admin pages. Set the level to LOW.



## Activate the Agents

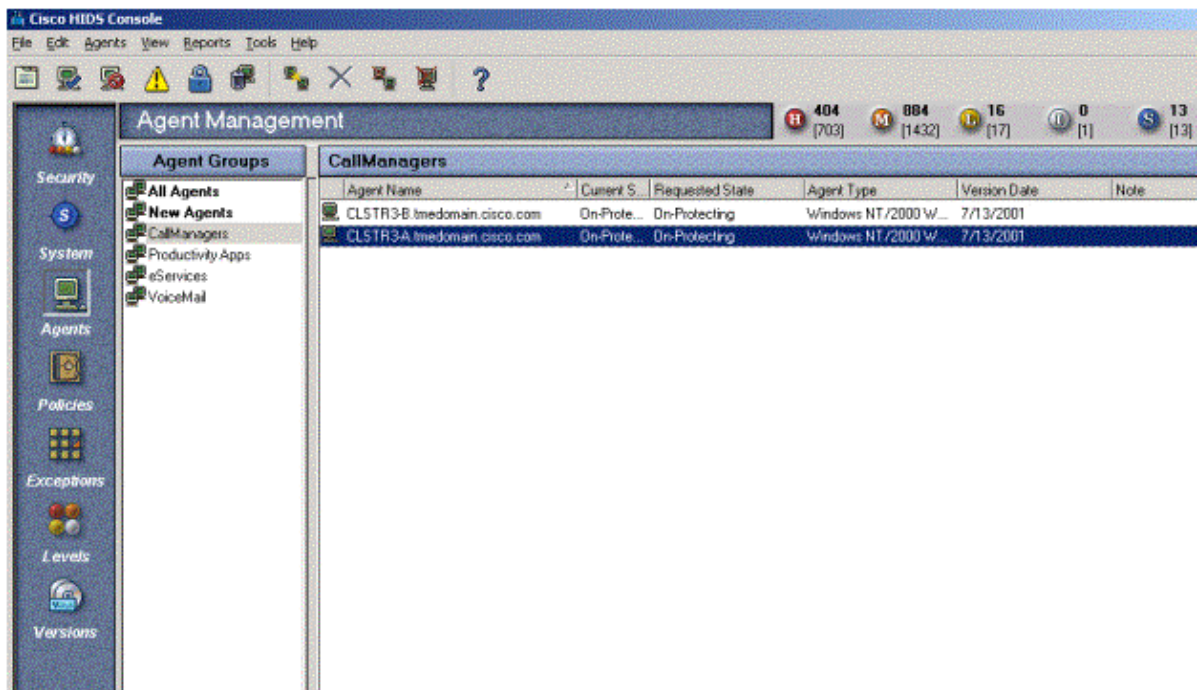
After you complete access level modification, it is time to activate the agents. To do this:

1. Click the **Agents** icon on the left hand side of the screen.
2. Click the **All Agents** group.
3. Right-click the first Agent in the list and select **Set To Protection Mode**.

Repeat this step for all agents. The Agents screen shows each agent in On-Protecting Mode, as shown below.



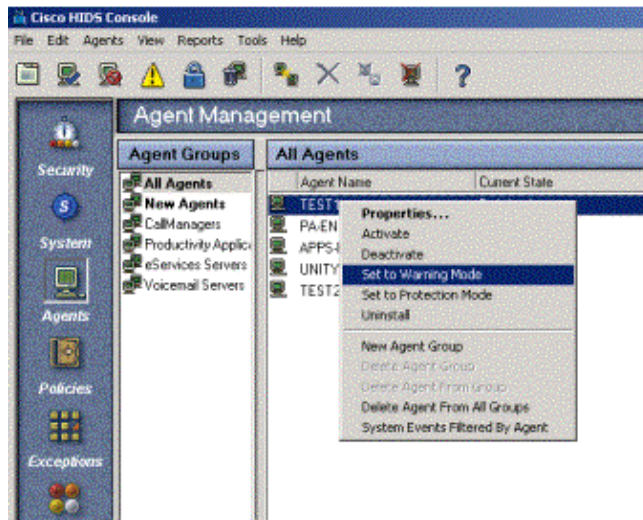
**Caution:** If you do not complete this step, the Cisco IDS Host Sensor Agent is not blocking the attacks.



# Upgrade Cisco CallManager and Install New Software

Any installation of new software on the Cisco CallManager requires the IDS Agent to be set to **On Warning** mode instead of Protecting mode. This includes upgrades to the CallManager, as well as installations of other plugins such as ART or BAT.

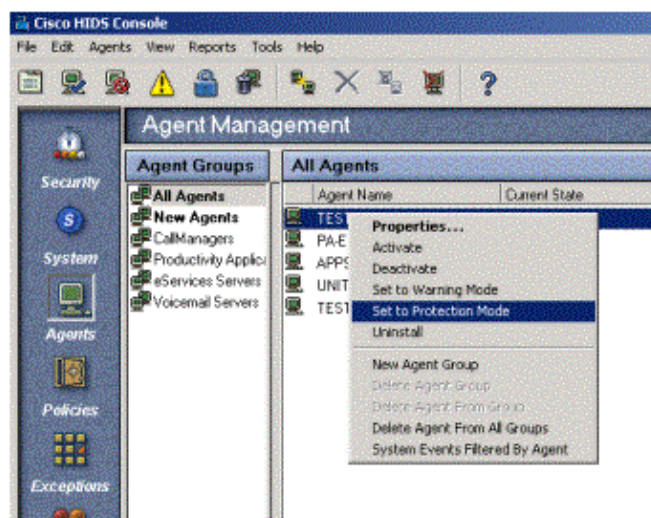
Prior to performing an upgrade, the agent associated with the Cisco CallManager should be put in an **On Warning** mode. In an On–Warning mode the agent will not attempt to interfere with the install package.



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



**Caution:** If you do not do this, your server will not be protected against attacks.

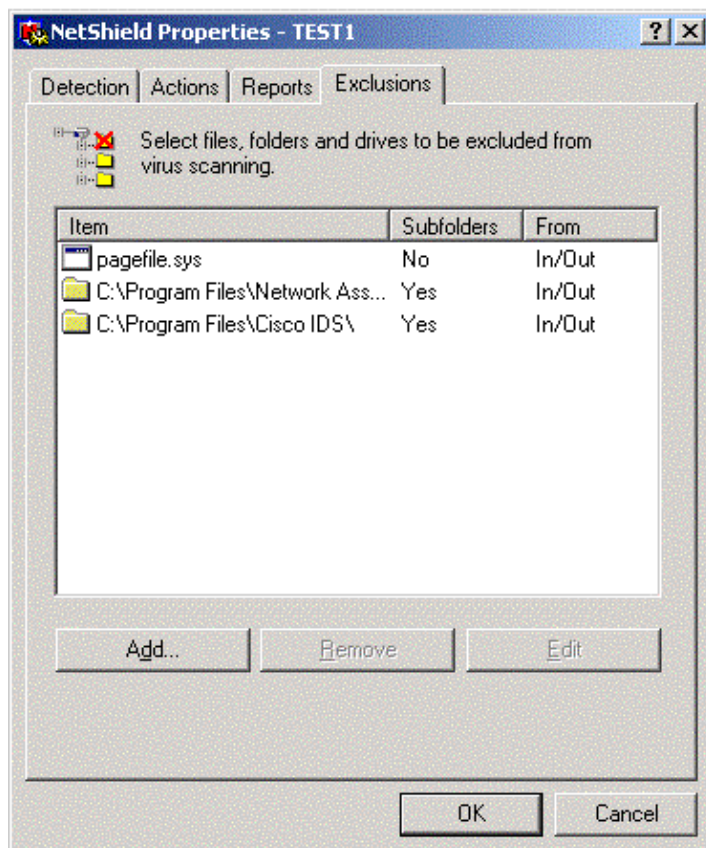


## Caveats

### Use Cisco Host IDS Sensor Agent and McAfee NetShield

**Note:** In order for McAfee NetShield and the Cisco Host IDS Sensor Agent to co–exist on the same server, McAfee should be configured to not scan the directory where the Cisco Host IDS Sensor Agent or Console

are installed. An example is shown below.



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.

---

## Related Information

- [Voice Technologies](#)
- [Voice, Telephony and Messaging Devices](#)
- [Recommended Reading: Troubleshooting Cisco IP Telephony](#)
- [Technical Support – Cisco Systems](#)

---

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Feb 02, 2006

Document ID: 17736

---