



Installing Optional Software

In this chapter, you do the following tasks in the order listed:

1. Install Cisco IDS Host Sensor, if applicable. See the [“Installing Cisco IDS Host Sensor Agent and Configuring Cisco IDS Host Sensor”](#) section on page 9-2.
2. Install optional third-party service packs, if applicable. See the [“Installing Optional Service Packs and Updates”](#) section on page 9-4.
3. Install RSA SecurID, if applicable. See the [“Installing RSA SecurID”](#) section on page 9-4.
4. Install Symantec pcAnywhere, if applicable. See the [“Installing Symantec pcAnywhere”](#) section on page 9-5.
5. Install virus-scanning utilities, if applicable. See the [“Installing Virus-Scanning Software”](#) section on page 9-7.
6. Install other optional software, if applicable. See the

When you are finished with this chapter, return to the applicable task list for your platform type to continue installing the Cisco Unity system correctly:

- [Task List for Installing Cisco Unity on a Qualified Server, page 1-2](#)
- [Task List for Installing Cisco Unity in the Cisco ICS 7750, page 1-9](#)



Note

The tasks in the list reference detailed instructions in the *Cisco Unity Installation Guide* and in other Cisco Unity documentation. Follow the documentation for a successful installation.

Installing Cisco IDS Host Sensor Agent and Configuring Cisco IDS Host Sensor

For supported versions of Cisco IDS Host Sensor Agent, refer to *Cisco Unity 4.0 System Requirements, and Supported Hardware and Software* on Cisco.com at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_pre_installation_guides_list.html.

Do the following three procedures in the order listed.



Caution

Do not install Cisco IDS Host Sensor Console on the Cisco Unity server.

To install Cisco IDS Host Sensor Agent

Follow the manufacturer instructions to install Cisco IDS Host Sensor Agent on the Cisco Unity server.

To configure Cisco IDS Host Sensor

- Step 1** On the Cisco IDS Host Sensor console server, create an agent group named Unity, and add the Cisco Unity server to the Unity agent group.
- Step 2** On the console server, create a policy named Unity.
- Step 3** Add the Unity agent group to the Unity policy.
- Step 4** For High and Medium events, in the Reaction list, click **Prevent**.
- Step 5** For Low and Info events, in the Reaction list, click **Log**.
- Step 6** On the console server, for the Unity agent group, change the security levels to **Low** for the following 11 signatures:
 - IIS Directory Traversal
 - IIS Envelope—File Access by IIS Process
 - IIS Envelope—File Access by IIS Web User
 - IIS Envelope—File Modification by IIS Process

- IIS Envelope—Registry Access by IIS Process
- IIS Envelope—File Execution by IIS Process
- IIS Shielding—Configuration File Activity
- IIS Shielding—File Execution
- IIS Shielding—Registry Access
- IIS Shielding—Service Access
- IIS Shielding—SSI File Extension Request

**Caution**

If you do not change the signatures, the Cisco Unity Administrator, Cisco Personal Communications Assistant (PCA), Cisco Unity Assistant, Cisco Unity Inbox, and Status Monitor will not function correctly. In addition, Event Viewer event properties will be inaccessible.

- Step 7** By default, an agent will operate in On-Warning mode after installation. We recommend that you run the agent in On-Warning mode for one week after installation, and then adjust other security levels as appropriate. Do not change the security levels that you set to Low in [Step 6](#).
-

If McAfee NetShield is installed on the Cisco Unity server, you need to exclude from scanning the directory in which the Cisco IDS Host Sensor Agent was installed, so that Cisco IDS Host Sensor will work properly.

To exclude the Cisco IDS Host Sensor Agent directory from scanning

- Step 1** In the status bar, right-click the **NetShield** icon, and click **Properties**.
- Step 2** Click the **Exclusions** tab.
- Step 3** Click **Add**.
- Step 4** In the File, Folder, or Drive to Exclude box, enter the name of the directory in which the Cisco IDS Host Sensor Agent was installed (Program files\Cisco IDS is the default directory).
- Step 5** Check the **Include Subfolders** check box.
- Step 6** Check the **Exclude from Inbound** check box.

- Step 7** Check the **Exclude from Outbound** check box.
 - Step 8** Click **OK** to close the Add Exclusion Item dialog box.
 - Step 9** Click **OK** to close the NetShield Properties dialog box.
-

Installing Optional Service Packs and Updates

We recommend that you install all optional third-party service packs and updates qualified for use with Cisco Unity. If you have not already installed such service packs and updates, do so now.

For information on supported optional third-party service packs and updates, refer to *Compatibility Matrix: Required and Optional Third-Party Service Packs*, at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_pre_installation_guides_list.html.

Installing RSA SecurID

For supported versions of RSA SecurID, refer to *Cisco Unity 4.0 System Requirements, and Supported Hardware and Software* on Cisco.com at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_pre_installation_guides_list.html.

Follow the manufacturer instructions to install RSA SecurID.

The installation task list alerts you when to configure RSA SecurID later in the installation process. (You will refer to the “Enhanced Phone Security” chapter of the *Cisco Unity System Administration Guide*, which is available on Cisco.com at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_administration_guide_books_list.html).

Installing Symantec pcAnywhere

For supported versions of Symantec pcAnywhere, refer to *Cisco Unity 4.0 System Requirements, and Supported Hardware and Software* on Cisco.com at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_pre_installation_guides_list.html.

Follow the manufacturer instructions to install pcAnywhere. See also the “[Recommended Configuration for pcAnywhere](#)” section, below.

The remote-access software can be installed on the Cisco Unity server in addition to Windows Terminal Services (which is the default remote-access software for the Cisco Unity server and is included with Windows 2000). Use an external modem with pcAnywhere.

Recommended Configuration for pcAnywhere

We recommend that you do the following three procedures in the order listed to configure pcAnywhere to avoid video problems, screen-refresh problems, and a possible problem with the server not responding after pcAnywhere disconnects.

To configure pcAnywhere so that it does not start automatically when you restart the server

-
- Step 1** On the Windows Start menu, click **Programs > Symantec pcAnywhere**.
 - Step 2** In the pcAnywhere toolbar, click **Hosts**.
 - Step 3** Right-click the **Modem** icon or the host that is configured for a modem, and click **Properties**.
 - Step 4** In the pcAnywhere Host Properties dialog box, click the **Settings** tab.
 - Step 5** In the Host Startup section, uncheck the **Launch with Windows** check box.
 - Step 6** Click **OK** to close the pcAnywhere Host Properties dialog box.
-

To avoid a pcAnywhere video problem, we recommend that you change the pcAnywhere video mode. (The problem is described in Symantec Knowledge Base article 2001040615242112.)

To change the pcAnywhere video mode to Compatibility

- Step 1** In pcAnywhere, on the pcAnywhere Tools menu, click **Options**.
 - Step 2** On the Host Operation tab, under Video Mode Selection, click **Compatibility**.
 - Step 3** Click **OK**.
 - Step 4** Exit pcAnywhere.
-

To avoid a pcAnywhere problem with slow or partial screen refreshes on multiprocessor host computers, and a possible problem in which the host computer stops responding when pcAnywhere disconnects, we recommend that you add a registry entry that sets pcAnywhere to run on one or more specific processors. (The problem is described in Symantec Knowledge Base article 199861984643.)

Be aware that setting pcAnywhere to run on a specific processor may affect performance on the Cisco Unity server if someone uses pcAnywhere to access the server during peak hours.

To set pcAnywhere to run on one or more specific processors

- Step 1** Start Regedit.



Caution

Changing the wrong registry key or entering an incorrect value can cause the server to malfunction. Before you edit the registry, confirm that you know how to restore it if a problem occurs. (Refer to the “Restoring” topics in Registry Editor Help.) Note that a typical backup of the Cisco Unity server does not back up the registry. Also note that for Cisco Unity failover, registry changes on one Cisco Unity server must be made manually on the other Cisco Unity server, because registry changes are not replicated. If you have any questions about changing registry key settings, contact Cisco TAC.

- Step 2** If you do not have a current backup of the registry, click **Registry > Export Registry File**, and save the registry settings to a file.
- Step 3** Expand the key
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\Host

Step 4 Add a DWORD value named **ProcessorMask**, and set the value depending on which processor you want to use (for example, to make pcAnywhere run on the second processor only, set ProcessorMask to 2):

- 0 All processors
- 1 First processor
- 2 Second processor
- 4 Third processor
- 8 Fourth processor

To allow pcAnywhere to run on more than one processor, set the value of ProcessorMask to the sum of the corresponding values. (For example, to make pcAnywhere run on the third and fourth processors, set ProcessorMask to 12 [4 + 8]).

Step 5 Either stop and restart the pcAnywhere host service or restart the Cisco Unity server.

Installing Virus-Scanning Software

Follow the manufacturer instructions to install virus-scanning software.

For information on supported software, refer to the “Supported Virus-Scanning Software” section in *Cisco Unity 4.0 System Requirements, and Supported Hardware and Software* on Cisco.com at

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_pre_installation_guides_list.html.

Note that scanning individual Exchange mailboxes can affect the performance of Cisco Unity.

**Caution**

Do not configure virus-scanning software to block WAV attachments, or voice messages will be stripped of their recordings.

Installing Other Optional Software

Follow the manufacturer instructions to install other optional software.

For information on supported software, refer to the “PART 3: Supported Software for Use with Cisco Unity 4.0(x)” section in *Cisco Unity 4.0 System Requirements, and Supported Hardware and Software* on Cisco.com at

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_pre_installation_guides_list.html.