Release Notes for Cisco Security Agent for Cisco Unity, Release 1.1(2)

Published January 23, 2004

These release notes provide download, installation, and upgrade instructions, and information on new and changed functionality, and caveats for Cisco Security Agent for Cisco Unity, Release 1.1(2).

Cisco Security Agent for Cisco Unity software is available on the Cisco Unity Crypto Software Download page at http://www.cisco.com/cgi-bin/tablebuild.pl/unity3d.

Contents

These release notes contain the following sections:

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

Introduction

Cisco Security Agent for Cisco Unity is a standalone Cisco Security Agent that is provided free of charge by Cisco Systems for use with Cisco Unity servers that meet the system requirements specified in the "System Requirements and Supported Software" section on page 2. The agent provides intrusion prevention, malicious mobile code protection, operating system integrity assurance, and audit log consolidation based on a tested set of security rules (policies). It controls system operations by allowing or denying selected system actions before system resources are accessed. This process occurs transparently and does not significantly affect overall system performance.

Caution Cisco Security Agent for Cisco Unity should not be viewed as providing complete security for Cisco Unity servers. Instead, it should be viewed as an additional line of defense that enhances security when used with other defenses such as virus-scanning software and a firewall.

The agent was created by using CiscoWorks Management Center for Cisco Security Agents and is based on the following Management Center for Cisco Security Agents version 4.0.1, build 539 policies:

- Required Windows System Module
- Common Security Module
- Common Web Server Security Module
- Restrictive MS IIS Module
- Server Module
- User Authentication Auditing Module
- Virus Scanner Module

Cisco Security Agent for Cisco Unity version 1.1(2) also includes the Unity Base Group Exceptions policy, which allows normal Cisco Unity operations that the other policies would not allow.

To add, change, delete, or view policies included in Cisco Security Agent for Cisco Unity, run CiscoWorks Management Center for Cisco Security Agents, and import the file CiscoUnity-CSA-4.0.1.539-1.1.2.export. The file is available at http://www.cisco.com/cgi-bin/tablebuild.pl/unity3d.

For more information on CiscoWorks Management Center for Cisco Security Agents and on Cisco Security Agent, refer to http://www.cisco.com/en/US/products/sw/cscowork/ps5212/index.html.

System Requirements and Supported Software

Software Requirements

- Cisco Unity version 4.0(1) or later running on the Cisco Unity server.

- Microsoft Windows 2000 Server in English or Windows 2000 Advanced Server in English running on the Cisco Unity server. Other language versions are not supported.
- If the message store is installed on the Cisco Unity server, Microsoft Exchange 2000 for the message store.
- If the message store is not installed on the Cisco Unity server, IBM Lotus Domino, Microsoft Exchange 2003, or Microsoft Exchange 2000 for the message store.

Note If you install Cisco Security Agent for Cisco Unity on a server running Windows in Japanese, the display of some non-ASCII characters will be corrupted.

Supported Optional Software

Only the following optional software has been qualified for use on a Cisco Unity server that is running Cisco Security Agent for Cisco Unity:

- Adobe Acrobat Reader, version 4 and later.
- McAfee NetShield for Microsoft Windows NT and Windows 2000, version 4.5 and later.
- Trend Micro ScanMail for Microsoft Exchange 2000, version 5 and later.
- VERITAS Backup Exec for Microsoft Windows NT and Windows 2000, version 8.5 and later.
- VERITAS NetBackup version 4.5 and later.
- Windows Automatic Update. It must be configured not to automatically download updates to the Cisco Unity server.
- WinZip, version 7 and later.

Other optional software that is supported on the Cisco Unity server is not supported when the server is running Cisco Security Agent for Cisco Unity.

Determining the Software Version

This section contains procedures for determining the version in use for the following software:

- Cisco Security Agent, page 3
- Policy for Cisco Security Agent for Cisco Unity, page 4

Cisco Security Agent

To Determine the Cisco Security Agent Version in Use

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.) 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\Cisco Systems, Inc.\System Info\CSA Agent\Version.

Step 4 Close Regedit.

Policy for Cisco Security Agent for Cisco Unity

To Determine the Policy Version in Use for Cisco Security Agent for Cisco Unity

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.) 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\Cisco Systems, Inc.\System Info\Unity-CSA Policy\Version.

Step 4 Close Regedit.

Notes on Using Cisco Security Agent for Cisco Unity

The following sections contain information on using Cisco Security Agent for Cisco Unity:

Cisco Security Agent Service Must Be Disabled for Specific Tasks

The Cisco Security Agent service must be disabled and stopped in the following situations:

- Before you use any Cisco Unity tool in:
  - Cisco Unity Tools Depot.
  - The CommServer\Utilities directory.
  - The CommServer\TechTools directory.
- Before you use any Cisco Unity tool that you download from CiscoUnityTools.com.

- Before you install any software on the Cisco Unity server.
- Before you upgrade any software, including Cisco Unity, on the Cisco Unity server. This also applies to automatic upgrades (for example, installing service packs by using group policy objects or custom scripts). Cisco Security Agent for Cisco Unity allows supported virus-scanning applications to automatically download and install upgrades to virus-scanning components.
- Before you add, change, or delete values in the Windows registry.
- Before you change Windows system or boot files.

Caution Do not stop the Cisco Security Agent service by using the net stop command or the Cisco Security Agent icon in the taskbar. These methods are not supported.

Caution When you disable and stop the Cisco Security Agent service, you must re-enable and start it before it can monitor the Cisco Unity server again.

For instructions on disabling and re-enabling the service, see the "Disabling and Re-enabling the Cisco Security Agent Service" section on page 8.

Cisco Security Agent Taskbar Icon Available Only for First Windows Logon

If two people log on to Windows on the Cisco Unity server—one at the server and the other by using Windows Terminal Services, or both by using Terminal Services—only the first person to log on will have access to the Cisco Security Agent icon.

Locations in Which Cisco Security Agent Logs Events

Cisco Security Agent logs events in the following three locations:

Windows application event log	Events that are generated by Cisco Security Agent have an event source of CSAgent.
Securitylog.txt	Cisco Security Agent logs one event per line. (You may have to turn off word wrap in your text editor.) We recommend that each administrator who logs on to the Cisco Unity server add a shortcut for Securitylog.txt to the Windows desktop. The file is located in the <InstallDirectory>\Cisco\CSAgent\Log directory.
CSA Control Panel	To display the CSA Control Panel, double-click the Cisco Security Agent taskbar icon, and click the Messages tab. Only events that have occurred since you logged on to Windows appear in the CSA Control Panel.

Downloading Cisco Security Agent for Cisco Unity 1.1(2)

To Download Cisco Security Agent for Cisco Unity 1.1(2)

Step 1 Confirm that the computer you are using has up to 20 MB of hard-disk space for the download file and the installed files.

Step 2 On a computer with a high-speed Internet connection, go to the Cisco Unity Crypto Software Download page at http://www.cisco.com/cgi-bin/tablebuild.pl/unity3d.

Step 3 Click **CiscoUnity-CSA-4.0.1.539-1.1.2-K9.exe**.

Step 4 Follow the on-screen prompts to complete the download.

Step 5 If you plan to install Cisco Security Agent for Cisco Unity from a compact disc, burn the CD.

Installing Cisco Security Agent for Cisco Unity 1.1(2)

Note If you are upgrading Cisco Security Agent for Cisco Unity to version 1.1(2), see the "Upgrading to Cisco Security Agent for Cisco Unity 1.1(2)" section on page 7.

We recommend that you install Cisco Security Agent for Cisco Unity after regular business hours because the installation will affect Cisco Unity performance. In addition, when the installation completes, you must restart the Cisco Unity server for Cisco Security Agent for Cisco Unity to start working.

Caution Do not install Cisco Security Agent for Cisco Unity by using Windows Terminal Services or the installation will fail.

To Install Cisco Security Agent for Cisco Unity 1.1(2)

Step 1 Log on to the Cisco Unity server by using an account that is a member of the Administrators group or the Local Administrators group.

Step 2 Confirm that the server has at least 20 MB of hard disk space available for the download file and the installed files.

Step 3 If Cisco IDS Host Sensor or another intrusion-detection application is installed on the Cisco Unity server, uninstall the application before installing Cisco Security Agent for Cisco Unity. Refer to the Cisco IDS Host Sensor or other applicable documentation.

Step 4 If Windows Automatic Update is configured to automatically download updates from the Microsoft website, disable it.

Step 5 If virus-scanning software is installed on the Cisco Unity server, disable and stop the scanning services:

a. On the Windows Start menu, click **Programs** > **Administrative Tools** > **Services**.

b. In the right pane, double-click the name of the first virus-scanning service.

c. On the General tab, in the Startup Type list, click **Disabled**. This prevents the service from starting when you restart the server.

d. Click **Stop** to stop the service immediately.

e. Click **OK** to close the Properties dialog box.

f. Repeat Step b through Step e for each of the remaining virus-scanning services.

g. When the services have been disabled, close the Services MMC.

Step 6 In Windows Explorer, browse to the directory to which you downloaded the Cisco Security Agent for Cisco Unity file, and double-click **CiscoUnity-CSA-4.0.1.539-1.1.2-K9.exe**.

Step 7 Follow the on-screen prompts.

Caution Do not change any of the default values, or the Cisco Security Agent may not function properly.

Step 8 When the installation completes, click **Yes, I Want to Restart My Computer Now**, and click **Finish**.

Cisco Security Agent for Cisco Unity begins to work as soon as you restart the Cisco Unity server. You do not need to configure the application.

Step 9 If virus-scanning software is installed on the Cisco Unity server, re-enable and start the scanning services:

a. On the Windows Start menu, click **Programs** > **Administrative Tools** > **Services**.

b. In the right pane, double-click the name of the first virus-scanning service.

c. On the General tab, in the Startup Type list, click **Automatic** to re-enable the service.

d. Click **Start** to start the service.

e. Click **OK** to close the Properties dialog box.

f. Repeat Step b through Step e for each of the remaining virus-scanning services.

g. When the services have been disabled, close the Services MMC.

Upgrading to Cisco Security Agent for Cisco Unity 1.1(2)

Use the task list in this section to upgrade to version 1.1(2) of the Cisco Security Agent for Cisco Unity. The tasks refer to sections in these release notes.

Upgrade Task List

1. Download the software. See the "Downloading Cisco Security Agent for Cisco Unity 1.1(2)" section on page 6.
2. Disable the Cisco Security Agent service. See the procedure ""To Disable and Stop the Cisco Security Agent Service" in the "Disabling and Re-enabling the Cisco Security Agent Service" section on page 8.

3. Uninstall the previous version. See the "Uninstalling Cisco Security Agent for Cisco Unity" section on page 9.
4. Install version 1.1(2). See the "Installing Cisco Security Agent for Cisco Unity 1.1(2)" section on page 6. When the installation is complete, the Cisco Security Agent service is enabled automatically.

Disabling and Re-enabling the Cisco Security Agent Service

The Cisco Security Agent service must be disabled and stopped before you install or upgrade any software on the Cisco Unity server. (For information on other situations in which you must disable the Cisco Security Agent service, see the "Cisco Security Agent Service Must Be Disabled for Specific Tasks" section on page 4.)

Caution When you disable and stop the Cisco Security Agent service, you must re-enable and start it before it can monitor the Cisco Unity server again.

Caution Do not stop the Cisco Security Agent service by using the net stop command or the Cisco Security Agent icon in the taskbar. These methods are not supported.

To Disable and Stop the Cisco Security Agent Service

Step 1 On the Windows Start menu, click **Programs** > **Administrative Tools** > **Services**.

Step 2 In the right pane, double-click **Cisco Security Agent**.

Step 3 On the General tab, in the Startup Type list, click **Disabled**. This prevents the service from starting when you restart the server.

Step 4 Click **Stop** to stop the service immediately.

Step 5 Click **OK** to close the Cisco Security Agent Properties dialog box.

Step 6 When the service has been disabled, close the Services MMC.

To Re-enable and Start the Cisco Security Agent Service

Step 1 On the Windows Start menu, click **Programs** > **Administrative Tools** > **Services**.

Step 2 In the right pane, double-click **Cisco Security Agent**.

Step 3 On the General tab, in the Startup Type list, click **Automatic** to re-enable the service.

Step 4 Click **Start** to start the service.

Step 5 Click **OK** to close the Cisco Security Agent Properties dialog box.

Step 6 When the service has been re-enabled, close the Services MMC.

Uninstalling Cisco Security Agent for Cisco Unity

To Uninstall Cisco Security Agent for Cisco Unity

Step 1 Right-click the **Cisco Security Agent** icon in the Windows taskbar, and click **Suspend Security**.

If the icon does not appear in the taskbar, on the Windows Start menu, click **Programs** > **Administrative Tools** > **Services**, and stop the **Cisco Security Agent** service.

Step 2 On the Windows Start menu, click **Programs** > **Cisco Systems** > **Uninstall Cisco Security Agent**.

Step 3 Click **Yes** to confirm that you want to uninstall Cisco Security Agent for Cisco Unity.

Step 4 Click **Yes** again to restart the Cisco Unity server.

New and Changed Functionality—Release 1.1(2)

This section contains information about new and changed functionality for Cisco Security Agent for Cisco Unity, Release 1.1(2) only. Refer to the release notes of the applicable version for information about new and changed functionality in earlier versions of Cisco Security Agent for Cisco Unity. Release notes for all versions of Cisco Security Agent for Cisco Unity are available on Cisco.com at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

Version 1.1(2) Compiled with Cisco Security Agent Version 4.0.1.539

Cisco Security Agent for Cisco Unity is compiled with Cisco Security Agent version 4.0.1, build 539.

Caveats

This section describes Severity 1, 2, and select Severity 3 caveats.

If you have an account with Cisco.com, you can use Bug Toolkit to find more information on the caveats in this section, in addition to caveats of any severity for any release. Bug Toolkit is available at the website http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Note that this section contains caveat information for Cisco Security Agent for Cisco Unity version 1.1(2), and for Cisco Security Agent versions 4.0 and 4.0(1) that may affect Cisco Security Agent for Cisco Unity. For caveat information for earlier versions of Cisco Security Agent for Cisco Unity, refer to the applicable release notes. Release notes for all versions of Cisco Security Agent for Cisco Unity are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

Open Caveat—Release 1.1(2)

Table 1 Cisco Security Agent for Cisco Unity, Release 1.1(2) Open Caveat

Caveat Number	Severity	Description
CSCed14125	2	Cisco Security Agent running on a multi-processor Cisco Unity server causes a blue screen. After the system has been running for some time (varies from a couple of days to several weeks), the server will blue screen. The problem occurs on systems running Windows 2000 Advanced Server, with and without the /3GB switch. **Workaround** Disable Cisco Security Agent.

Resolved Caveats—Release 1.1(2)

Table 2 Cisco Security Agent for Cisco Unity, Release 1.1(2) Resolved Caveats

Caveat Number	Severity	Description
CSCok07184	1	COM rule not invoked with dynamic application class.
CSCeb87973	2	Non-standard DACL patterns cause increased kernel memory usage.
CSCec06809	2	Agent process leventmgr.exe uses increasing memory over time.
CSCec68211	2	BSOD after chose terminate from Troj Dect. rules popup.
CSCec71872	2	(CSA-Pilot) Hang transferring files from file share w/netshim.
CSCin47432	2	VMS2.2-BT: FQDN is required to connect to CiscoWorks.
CSCec53589	3	Not able to start JRUN with CSA Agent installed.

Troubleshooting

The following sections contain information on troubleshooting Cisco Security Agent for Cisco Unity:

Problems with Cisco Unity or Errors from Cisco Security Agent

Do the procedure in this section, if you encounter any of the following problems after installing Cisco Security Agent for Cisco Unity:

- Problems with Cisco Unity that cannot otherwise be explained.
- Cisco Security Agent errors in the Windows event log or in the Cisco Security Agent log file, <Drive>:\Program Files\Cisco\CSAgent\log\securitylog.txt.
- Cisco Security Agent error messages displayed on the screen.

If you cannot determine the cause of a Cisco Security Agent log entry or error message, contact Cisco TAC.

To Troubleshoot Problems with Cisco Unity or Errors from Cisco Security Agent

Step 1 In the Windows taskbar, right-click the **Cisco Security Agent** icon, and click **Suspend Security**.

Step 2 Perform the operation that caused the error message.

Step 3 In the Windows taskbar, right-click the **Cisco Security Agent** icon, and click **Resume Security**.

Step 4 Perform the operation that caused the error message.

Step 5 If the operation completes successfully with the Cisco Security Agent suspended and continues to fail with the Cisco Security Agent enabled, confirm that all of the software running on the Cisco Unity server is listed as supported in the "System Requirements and Supported Software" section on page 2.

If unsupported software is installed on the server, remove the unsupported software and repeat this procedure.

Step 6 If you are unable to resolve the problem, contact Cisco TAC and send them the Cisco Security Agent log file, <Drive>:\Program Files\Cisco\CSAgent\log\securitylog.txt.

Second Attempt to Install Software Fails Without a Warning

In the following case, an attempt to install software will fail without a warning:

1. You tried to install software without first disabling and stopping the Cisco Security Agent service.
2. Cisco Security Agent displayed the message

   "Cisco Security Agent: A problem was detected, press one of the action buttons below. Are you installing/uninstalling software? If not, this operation is suspicious."
3. You clicked **No**.
4. You disabled and stopped the Cisco Security Agent service.
5. You tried again to install the software installation, but nothing happened.

When you clicked No in Step 3., your answer was cached in memory. The cache is cleared automatically after an hour. To clear the cache immediately so you can install the software now, do the following procedure.

To Clear the Cisco Security Agent Memory Cache So You Can Install Software

Step 1 In the Windows taskbar, double-click the **Cisco Security Agent** icon.

Step 2 Click the **Advanced** tab.

Step 3 Click **Clear**.

Step 4 Close the Cisco Security Agent Control Panel.

Step 5 Before you retry installing software on the server, disable the Cisco Security Agent service. See the procedure "To Disable and Stop the Cisco Security Agent Service" section on page 8.

Step 6 After you install the software, re-enable the Cisco Security Agent service. See the procedure "To Re-enable and Start the Cisco Security Agent Service" section on page 8.

Cisco Unity Documentation

For descriptions and URLs of Cisco Unity documentation on Cisco.com, refer to *About Cisco Unity Documentation*. The document is shipped with Cisco Unity and is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/about/aboutdoc.htm.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

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

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit e-mail comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

The Cisco TAC website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year. The Cisco TAC website is located at this URL:

http://www.cisco.com/tac

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

http://tools.cisco.com/RPF/register/register.do

Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

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

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

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

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is "down" or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Go to this URL to visit the company store:

  http://www.cisco.com/go/marketplace/

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://cisco.com/univercd/cc/td/doc/pcat/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

  http://www.cisco.com/en/US/learning/index.html
