



Release Notes for Cisco Unity Bridge Release 3.1(1)

Revised May 21, 2009 (Originally published June 16, 2006)

These release notes describe download and upgrade instructions, new and changed requirements and support, new and changed functionality, limitations and restrictions, and open and resolved caveats for Cisco Unity Bridge Release 3.1(1).

Access the latest Bridge software upgrades on the Cisco Unity Bridge Software Download page at <http://www.cisco.com/cgi-bin/tablebuild.pl/unity-bridge>.

Contents

These release notes contain the following sections:

- [System Requirements, and Supported Hardware and Software, page 2](#)
- [Determining the Software Version, page 2](#)
- [Downloading the Software for a Cisco Unity Bridge Installation or Upgrade, page 3](#)
- [Upgrading to Cisco Unity Bridge 3.1\(1\), page 5](#)
- [New and Changed Requirements and Support—Release 3.1\(1\), page 5](#)
- [New and Changed Functionality—Release 3.1\(1\), page 7](#)
- [Installation and Upgrade Notes, page 7](#)
- [Limitations and Restrictions, page 8](#)
- [Caveats, page 8](#)
- [Documentation Updates, page 9](#)
- [Cisco Unity Documentation, page 10](#)
- [Obtaining Documentation, page 10](#)
- [Documentation Feedback, page 11](#)
- [Cisco Product Security Overview, page 11](#)



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

© 2006 Cisco Systems, Inc. All rights reserved.

- [Obtaining Technical Assistance, page 12](#)
- [Obtaining Additional Publications and Information, page 14](#)

System Requirements, and Supported Hardware and Software

The following documents list the most current Cisco Unity Bridge requirements and are available on Cisco.com:

- *Cisco Unity Bridge 3.1 System Requirements, and Supported Hardware and Software* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.
- *Cisco Unity Networking Options Requirements* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_device_support_tables_list.html.
- *Recommended Service Packs and Updates for Use with Cisco Unity and the Cisco Unity Bridge* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_device_support_tables_list.html.

Determining the Software Version

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

- [Cisco Unity Bridge, page 2](#)
- [Cisco Unity, page 2](#)
- [Cisco Unity Voice Connector for Microsoft Exchange, page 3](#)

Cisco Unity Bridge

To Determine the Cisco Unity Bridge Version in Use

-
- Step 1** On the Bridge server, open the Bridge Administrator.
- Step 2** Click **About**. The About Cisco Unity Bridge page indicates the Bridge version.
-

Cisco Unity

To Determine the Cisco Unity Version in Use by Using the Cisco Unity Administrator

-
- Step 1** In the Cisco Unity Administrator, go to the **System > Configuration > Software Versions** page. The Cisco Unity version is displayed in the Cisco Unity Build Number field.
-

To Determine the Cisco Unity Version in Use by Using the AvCsMgr.exe File (Cisco Unity 3.0(4) and Later)

-
- Step 1** Browse to the **CommServer** directory.
 - Step 2** Right-click **AvCsMgr.exe**, and click **Properties**.
 - Step 3** In the Properties window, click the **Version** tab.
 - Step 4** In the Item Name list, click **Product Version**. The Cisco Unity version is displayed in the Value window.
-

Cisco Unity Voice Connector for Microsoft Exchange

This section contains two procedures. Do the procedure for your version of Cisco Unity.

To Determine the Voice Connector Version in Use: Cisco Unity 4.0 and Later, Voice Connector 10.0 and Later

-
- Step 1** Log on to the Exchange server on which the Voice Connector is installed.
 - Step 2** In Windows Explorer or My Computer, browse to the directory **<ExchangeServerPath>\VoiceGateway\Bin**.
 - Step 3** Right-click **GwIvc.exe**, and click **Properties**.
 - Step 4** Click the **Version** tab in the Properties window.
 - Step 5** In the Item Name box, click **Product Version** to view the product version in the Value box.
-

To Determine the Voice Connector Version in Use: Cisco Unity 3.1(3) Through 3.1(6)

-
- Step 1** Log on to the Exchange server on which the Voice Connector is installed.
 - Step 2** In Windows Explorer or My Computer, browse to the directory **<ExchangeServerPath>\VoiceGateway\Bin\LocalizedFiles\ENU**.
 - Step 3** Right-click **SetupRes.dll**, and click **Properties**.
 - Step 4** In the Properties window, click the **Version** tab to view the File Version.
-

Downloading the Software for a Cisco Unity Bridge Installation or Upgrade

The software required to install or upgrade to Bridge version 3.1(1) is available for download from the Cisco Software Center website. Use a computer with a high-speed Internet connection.

To Download the Bridge Software and the Required Service Packs and Updates

-
- Step 1** Confirm that the computer you are using has up to 680 MB of hard-disk space for the required software, in addition to the space required for the download files. (The download file sizes appear on the download pages.)
- Step 2** Check the *Recommended Service Packs and Updates for Use with Cisco Unity and the Cisco Unity Bridge* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_device_support_tables_list.html to determine whether new Windows 2000 Server, Windows Server 2003, or Internet Explorer service packs were qualified for use after Cisco Unity Bridge 3.1(1) was released. If so, download the latest service packs from Microsoft.com. Also download or print the installation instructions.
- Step 3** *If you are installing Windows Server 2003 on the Bridge Server, and if you did not download a Windows Server 2003 service pack in Step 2:* Download Windows Server 2003 Service Pack 1 from the Microsoft website and burn it to a CD.
- Step 4** *Optional but recommended:* Download the Cisco Unity Server Updates wizard, which contains Microsoft updates, and Cisco Security Agent for Cisco Unity, which can be installed on Cisco Unity Bridge servers.
- a. Go to the Voice and Unified Communications Downloads page at <http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=278875240>.
 - b. In the tree control on the Downloads page, expand **Unified Communications Applications > Voice Mail and Unified Messaging > Cisco Unity**, and click the link for the latest version of Cisco Unity.
 - c. Click **Microsoft Updates for Cisco Unity/Unity Connection**.
 - d. Follow the on-screen prompts to complete the download. Make note of the MD5 value.
-  **Note** To access the software download page, you must be logged on to Cisco.com as a registered user.
-
- See the *Software Installed by the Cisco Unity Server Updates Wizard* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html for information on which Microsoft updates and which version of the Cisco Security Agent for Cisco Unity are installed by the latest version of the wizard.
- See the *Release Notes for Cisco Security Agent for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html for information on supported configurations.
- Step 5** Download the Cisco Unity Bridge software:
- a. Go to the Voice and Unified Communications Downloads page at <http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=278875240>.
 - b. In the tree control on the Downloads page, expand **Unified Communications Applications > Voice Mail and Unified Messaging > Cisco Unity**, and click **Cisco Unity Bridge Version 3.0**.
 - c. Click **3.1(1)**.
 - d. Follow the on-screen prompts to complete the download. Make note of the MD5 value.
 - e. Repeat Step a. through Step d. to download **CiscoUnityBridge3.1.1ServicePacks.exe**.

- Step 6** When the downloads are complete, extract the files to separate directories:
- a. In Windows Explorer, double-click the file.
 - b. In WinZip, specify a directory to which the files will be extracted.
- Step 7** When you are done extracting the files, delete the downloaded .exe files to free disk space.

If you are installing the Bridge software for the first time, see the applicable *Cisco Unity Bridge Installation Guide, Release 3.1*. The Domino and Exchange versions of the guide are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

Upgrading to Cisco Unity Bridge 3.1(1)

For upgrades from earlier 3.x versions of Bridge, see the “Upgrading Bridge 3.x Software to the Shipping Version” chapter of the *Cisco Unity Bridge Networking Guide*. The Domino and Exchange versions of the guide are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.

New and Changed Requirements and Support—Release 3.1(1)

This section contains information on new and changed support in the Cisco Unity Bridge Release 3.1(1) time frame only. See the release notes of the applicable version for information about new and changed support with earlier versions of the Bridge. Release notes for all versions of the Bridge are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

Brooktrout Voice-Fax Cards

Brooktrout TR114 voice-fax card is no longer being manufactured by Cantata, the manufacturer of Brooktrout cards. Cisco is no longer shipping the TR114 cards. However, these cards are still supported for upgrades to Cisco Unity Bridge 3.1.

Brooktrout TR1034 voice-fax cards have been qualified for use with Bridge 3.1.

When installing multiple voice-fax cards in a single Bridge server or expansion chassis:

- You cannot mix TR1034 cards and TR114 cards.
- You cannot mix voice-fax cards intended for different countries. However, universal PCI and non-universal PCI voice-fax cards designed for the same country can be used in a single Bridge server.

Cisco Security Agent for Cisco Unity Bridge Version 2.0(3)

Cisco Security Agent for Cisco Unity Bridge version 2.0(3) is qualified for use with Cisco Unity Bridge 3.1(1). The application combines host intrusion detection and prevention, malicious mobile code protection, and operating system integrity assurance.

For requirements and other information on using Cisco Security Agent for Cisco Unity Bridge, see the *Release Notes for Cisco Security Agent for Cisco Unity Bridge, Release 2.0(3)* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

For information on the full Cisco Security Agent product, see the product website at <http://www.cisco.com/en/US/products/sw/secursw/ps5057/index.html>.

Required Versions of Cisco Unity with IBM Lotus Domino

Bridge version 3.1(1) is supported only with Cisco Unity 4.0(5) and later with Domino. In installations with multiple Cisco Unity servers, all the servers must be upgraded to Cisco Unity 4.0(5) or later.

Required Versions of Cisco Unity with Microsoft Exchange and the Voice Connector for Exchange

Bridge version 3.1(1) is supported only with Cisco Unity 4.0(3) and later with Exchange and Cisco Unity Voice Connector for Microsoft Exchange 2000 version 11.0(1) and later. In installations with multiple Cisco Unity servers, all the servers must be upgraded to Cisco Unity 4.0(3) or later.



Caution

If the Bridge server is running version 2.x, do not upgrade to version 3.1(1) unless you also plan to upgrade all Cisco Unity servers and the Voice Connector to the required versions. If you upgrade the Bridge server without upgrading Cisco Unity and the Voice Connector, messaging between the Bridge and Cisco Unity will fail. See the “Upgrading from Bridge 2.x to the Shipping Version” chapter of the *Cisco Unity Bridge Networking Guide, Release 3.1 (With Microsoft Exchange)* for information on upgrading the Bridge Networking option, including the Bridge server. The guide is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.

Voice-Fax Cards Qualified for Use with the Cisco Unity Bridge

The Brooktrout TR1034 voice-fax card has been qualified for use with Cisco Unity Bridge 3.1(1).

For the most current list of all supported voice-fax cards—including voice-fax cards qualified since the release of Cisco Unity Bridge version 3.1(1)—see the “Supported Voice-Fax Cards” section in *Cisco Unity Bridge 3.1 System Requirements, and Supported Hardware and Software* on Cisco.com at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

Windows Server 2003 on the Cisco Unity Bridge Server

Windows Server 2003 is now supported on the Bridge server. If you install Windows Server 2003 on the Bridge server, you must also install Windows Server 2003 Service Pack 1.



Caution

If Brooktrout TR114 voice-fax cards are installed in the Bridge server or an expansion chassis, you must install Windows 2000 Server. Windows Server 2003 is not supported with Brooktrout TR114 voice-fax cards.

Information on how to install Windows Server 2003 on a new Bridge system using a retail Windows disk appears in the *Cisco Unity Bridge Installation Guide, Release 3.1*. The Domino and Exchange versions of the guide are available at

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

Information on how to install Windows Server 2003 on a new Bridge system using Cisco Unity Platform Configuration discs appears in all versions of the Cisco Unity installation guides for the Cisco Unity 5.x release at

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

Information on how to upgrade from Windows 2000 Server to Window Server 2003 appears in the “Upgrading from Windows 2000 Server to Windows Server 2003 on a Bridge Server” chapter of the *Cisco Unity Bridge Networking Guide*. The Domino and Exchange versions of the guide are available at

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

New and Changed Functionality—Release 3.1(1)

This section contains information on new and changed functionality for Cisco Unity Bridge Release 3.1(1) only. See the release notes of the applicable version for information about new and changed functionality in earlier versions of the Bridge. Release notes for all versions of the Bridge are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

Bridge Administrator Includes New Options for Log Files

You can now specify the number of days that call trace logs created by the Bridge service are to be retained (see the System Settings page) and the number of days that trace logs created by the Bridge Digital Networking service are to be retained (see the Digital Networking page).

Installation and Upgrade Notes

For detailed information on installing the Cisco Unity Bridge, see the *Cisco Unity Bridge Installation Guide, Release 3.1*. The Domino and Exchange versions of the guide are available at

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

For detailed information on configuring Bridge Networking, see the *Cisco Unity Bridge Networking Guide, Release 3.1*. The Domino and Exchange versions of the guide are available at

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

Verify Logon Account Access to the Bridge Administrator Before an Upgrade

Before upgrading the Bridge software to version 3.1(1), confirm that the account with which you log on to the Bridge server has permission to access the Bridge Administrator.



Caution

If the account is denied access to the Bridge Administrator, do not continue or the Bridge Setup program will fail. You must log off, then log back on by using another account that is allowed access to the Bridge Administrator.

If access is denied, it is possible that the account is not in the Access Control List of the <Bridge>\Starfish\Asp directory or does not have Full Control permissions to that directory. Access to the <Bridge>\Starfish\Asp directory may have been restricted when password protection was added to the Bridge Administrator. (For more information, see the “Adding Password Protection to the Bridge Administrator” section in the “Setting Up Cisco Unity and the Bridge for Networking” chapter of the *Cisco Unity Bridge Networking Guide, Release 3.1 (With Microsoft Exchange)* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.)

Windows Fax Service Must Be Disabled Prior to Installing or Upgrading Bridge Software

If the Windows fax service is running or enabled while you are attempting to install or upgrade the Bridge software to version 3.1(1), you will see an error indicating that you must stop and disable the service. You disable the Windows fax service to prevent it from interfering with Brooktrout software.

Limitations and Restrictions

See the “Notable Behavior” section in the “About Bridge Networking” chapter of the *Cisco Unity Bridge Networking Guide, Release 3.1*. The Domino and Exchange versions of the guide are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.

Caveats

You can find the latest caveat information for Cisco Unity Bridge Release 3.1(1)—in addition to caveats of any severity for any release—by using Bug Toolkit, an online tool available for customers to query defects according to their own needs. Bug Toolkit is available at http://www.cisco.com/pcgi-bin/Support/Bugtool/launch_bugtool.pl.



Note

To access Bug Toolkit, you must be logged on to Cisco.com as a registered user.

This section contains caveat information for Cisco Unity Bridge Release 3.1(1) only. See the release notes of the applicable version for caveat information for earlier versions of the Bridge. Release notes for all versions of the Bridge are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

Open Caveats—Release 3.1(1)

Click a link in the Caveat Number column to view the latest information on the caveat in Bug Toolkit. (Caveats are listed in order by severity, then by component, then by caveat number.)

Table 1 Cisco Unity Bridge Release 3.1(1) Open Caveats

Caveat Number	Component	Severity	Description
CSCse30118	bridge	2	Bridge should better handle failure reading correspondents file at start
CSCee01101	bridge	3	Bridge fails to make calls if system time set back into the past

Table 1 *Cisco Unity Bridge Release 3.1(1) Open Caveats (continued)*

Caveat Number	Component	Severity	Description
CSCeg19346	bridge	3	Bridge: fallback from DST to Standard time hangs callout process
CSCsa71595	bridge	3	Bridge: Admin callouts stalled
CSCsb46026	bridge	3	Bridge-Cannot install Bridge Lic Install Wizard if folder path has space
CSCsc58690	bridge	3	Bridge-Space in multiple folders in install path causes ASP errors
CSCse19134	bridge	3	Bridge: Brooktrout TSP Event Viewer error on Win2003 with TR1034 board
CSCse30226	bridge	3	Need to account for unexpected value in InetRecvProtocol of VPIM.cfg

Resolved Caveats—Release 3.1(1)

Click the link in the Caveat Number column to view the latest information on the caveat in Bug Toolkit.

Table 2 *Cisco Unity Bridge Release 3.1(1) Resolved Caveats*

Caveat Number	Component	Severity	Description
CSCsa82488	bridge	3	Connectivity issues, causes bad message to bridge and spikes CPU to 100%

Documentation Updates

Changes

This section lists changes to the current Cisco Unity Bridge documentation. The changed information will be incorporated in a future documentation release, or as otherwise noted.

Cisco Unity Bridge Installation Guide: Installing Windows Server 2003 or Windows 2000 Server

The Domino and Exchange versions of *Cisco Unity Bridge Installation Guide, Release 3.1*, were published before Cisco Unity Bridge servers started shipping with Windows Server 2003 Cisco Unity Platform Configuration discs (PCDs). As a result, the “Installing Windows Server 2003 or Windows 2000 Server” section of the “Installing the Operating System” chapter of these guides does not contain a procedure for installing Windows Server 2003 using a PCD.

The procedure for the Cisco Unity Bridge is identical to the procedure that appears in the “Installing Windows Server 2003 by Using the Cisco Unity Platform Configuration Discs” section of the “Installing the Operating System” chapter in any of the Cisco Unity installation guides for release 5.x. If you have a Windows Server 2003 PCD, you can simply refer to the procedure in the Cisco Unity installation guides for release 5.x at

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

Cisco Unity Bridge Installation Guide: Installing the Latest Microsoft Updates Recommended for Use with the Bridge

The Domino and Exchange versions of *Cisco Unity Bridge Installation Guide, Release 3.1*, were published before the Cisco Unity Server Updates wizard was first released. To install Microsoft updates and, optionally, Cisco Security Agent for Cisco Unity, see the “Running the Server Updates Wizard” section in the applicable version of *Software Installed by the Cisco Unity Server Updates Wizard* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

Cisco Unity Documentation

For descriptions and URLs of Cisco Unity documentation on Cisco.com, refer to the *Cisco Unity Documentation Guide*. The document is shipped with Cisco Unity and is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_documentation_roadmap09186a00801179df.html.

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 at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

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

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation 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.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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



Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request 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 list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing 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.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations 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.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—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.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

<http://www.cisco.com/go/guide>

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- *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 at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

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

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- *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>

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learn2ng/index.html>

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

© 2009 Cisco Systems, Inc. All rights reserved.

