



Release Notes for Cisco Unified CallManager 4.1(3) Plug-in, Release 3.0 (for Cisco Voice Provisioning Tool)

Published August 11, 2006

These release notes describe system requirements, installation and upgrade notes, caveats, documentation notes, and technical assistance information for Release 3.0 of the Cisco Unified CallManager 4.1(3) Plug-in for the Cisco Voice Provisioning Tool.

Contents

These release notes contain the following sections:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [New and Changed Information, page 3](#)
- [Installation Notes, page 5](#)
- [Caveats, page 6](#)
- [Documentation Updates, page 10](#)
- [Related Documentation, page 11](#)
- [Obtaining Documentation, page 12](#)
- [Documentation Feedback, page 12](#)
- [Cisco Product Security Overview, page 13](#)
- [Obtaining Technical Assistance, page 14](#)
- [Obtaining Additional Publications and Information, page 15](#)



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

© 2006 Cisco Systems, Inc. All rights reserved.

Introduction

The Cisco Voice Provisioning Tool (VPT), a web-based application, provides you a single interface from which to perform frequent move, add, and change operations on multiple servers within a Cisco IP Telephony deployment. The Cisco Unified CallManager 4.1(3) plug-in for VPT allows you to use VPT to perform user provisioning tasks on Cisco Unified CallManager 4.1(3)SR1 systems.

System Requirements

The following subsections describe the hardware and software requirements for the Cisco Unified CallManager 4.1(3) plug-in.

Hardware Supported

The plug-in is installed on the VPT server. For a list of hardware supported on the VPT server, see the *Cisco Voice Provisioning Tool Release Notes* at http://www.cisco.com/en/US/products/ps6524/prod_release_notes_list.html.

Software Compatibility

Release 3.0 of the Cisco Unified CallManager 4.1(3) plug-in can be installed on a server running Cisco Voice Provisioning Tool Release 1.0(1) or 1.0(2). It can be installed concurrently with any Cisco Unity or Cisco Unity Connection plug-in. When you run the installation for this plug-in release, VPT automatically upgrades any earlier release of the Cisco Unified CallManager 4.1(3) Release 1.0 plug-in if it is still installed on your system. See the “[Installation Notes](#)” section on page 5 for instructions for installing or upgrading to this release.

For each Cisco Unified CallManager cluster, you configure a product system in VPT to represent the publisher server; if only one Cisco Unified CallManager server acts as publisher and subscriber, you configure that server as the product system.

The following requirements must be met on the Cisco Unified CallManager server that will be used as a product system to interoperate with VPT by using this plug-in release:

- The Cisco Unified CallManager server must be running Cisco Unified CallManager version 4.1(3)SR3 plus ES68.
- The Cisco AVVID XML (AXL) web service must be available on the Cisco Unified CallManager server, and reachable from the VPT server. The AXL web service is enabled by default on Cisco Unified CallManager servers and does not have to be installed or configured.

Determining the Software Version

To determine the version of Cisco Voice Provisioning Tool software in use, browse to the VPT login window and click **About** in the upper right corner of the window. You can also access the About link from any window after you have logged in to the tool.

To determine the version of product plug-ins installed on a VPT server, open the VPT graphical user interface (GUI) as described in the *Cisco Voice Provisioning Tool System Management and Security Guide*, and choose **VPT Administration > Plug-Ins > Manage Plug-Ins**.

New and Changed Information

The following sections describe new and changed features and functionality that are pertinent to this release of the Cisco Unified CallManager 4.1(3) plug-in.

- [Additional Cisco IP Phone Types Supported](#)
- [Additional Device Profile Types Supported](#)
- [Changes to the Add New User and Manage Users Pages](#)
- [Changes to Settings for the Cisco 7920 IP Phone](#)
- [New Phone Configuration Fields](#)

Additional Cisco IP Phone Types Supported

Support for the following phone types in the Cisco IP Phone 7900 family was added in release 2.0:

- Cisco 7911
- Cisco 7941 and 7941G-GE
- Cisco 7961 and 7961G-GE
- Cisco 7971
- Cisco 7985

**Note**

To provision these phone types by using VPT, the Cisco Unified CallManager server must be running version 4.1(3)SR1.

No additional support was added for Release 3.0.

Additional Device Profile Types Supported

Support for the following device profile types for the Cisco IP Phone 7900 family was added in Release 2.0:

- Cisco 7911
- Cisco 7920
- Cisco 7941 and 7941G-GE
- Cisco 7961 and 7961G-GE
- Cisco 7971
- Cisco 7985

**Note**

To provision these device profile types by using VPT, the Cisco Unified CallManager server must be running version 4.1(3)SR1.

No additional support was added for Release 3.0.

Changes to the Add New User and Manage Users Pages

With Release 2.0 or later of the Cisco Unified CallManager 4.1(3) plug-in, after you associate a phone or device profile with a new user on the Add New User page, you can click the device name of the phone or profile to modify settings for the device, delete the device, or reset/restart the device.

Similarly, you can click the device name of an associated device on the Manage Users page for a single user to modify settings for the device, delete the device, or reset/restart the device.

This functionality eliminates the need to do a separate search for a phone or device profile to make changes to it after adding or modifying a user.

Changes to Settings for the Cisco 7920 IP Phone

Additional settings were added to the configuration capabilities for the 7920 phone type beginning with Release 2.0:

- The Extension Mobility Feature can be enabled/disabled.
- IP Phone Service subscriptions can be added or removed.
- In the Advanced Phone/Profile Configuration section, the following settings have been added:
 - User Locale
 - Network Locale
 - Privacy
- In the Advanced Phone/Profile Configuration section, the following sections have been added:
 - Cisco IP Phone – External Data Locations
 - Product Specific Configuration (See the [“Documentation Updates”](#) section on page 10 for descriptions of new fields in this section.)
- In the Advanced Phone/Profile Configuration section, under Multi-level Precedence and Preemption (MLPP) Information, the MLPP Indication and MLPP Preemption fields are editable.

New Phone Configuration Fields

The following new fields are available in Release 2.0 or later in the Advanced Phone/Profile Configuration section of the phone and phone template configuration pages for certain phone models:

- Logging Display
- Load Server
- Use of PhoneBook or IP Phone Services Softkey
- Initial Display of Cisco Unified CallManager Softkeys During a Call

See the [“Documentation Updates”](#) section on page 10 for a description of the new fields.

Installation Notes

Use the following task list to install or upgrade to the Cisco Unified CallManager 4.1(3) plug-in, Release 3.0.

1. In the following cases, upgrade the Cisco Unified CallManager 4.1(3) server(s) that you want to access from VPT to version 4.1(3)SR3:
 - You are using Cisco 7920 IP phones.
 - You want to use the Active Directory or Netscape Directory integrations.

Otherwise, install or upgrade the Cisco Unified CallManager 4.1(3) server(s) to version 4.1(3)SR1.

See the *Installing Cisco Unified CallManager Release 4.1(3)* or *Upgrading Cisco Unified CallManager Release 4.1(3)* guides, at

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html.

2. If you have installed Cisco Unified CallManager 4.1(3)SR3, 4.1(3)SR3a, or 4.1(3)SR3b, install ES68.
3. Install or upgrade the Cisco Unified CallManager 4.1(3) plug-in. See the “[To Install or Upgrade a Cisco Unified CallManager Plug-in](#)” procedure on page 5.
4. Add a product system for each Cisco Unified CallManager publisher server, if applicable (any existing Cisco Unified CallManager 4.1(3) product systems configured in VPT will be automatically updated to use the Release 3.0 plug-in after the upgrade). See the *Cisco Voice Provisioning Tool System Management and Security Guide* for instructions on adding a product system, at http://www.cisco.com/en/US/products/ps6524/prod_maintenance_guides_list.html.

To Install or Upgrade a Cisco Unified CallManager Plug-in

To install or upgrade plug-ins, your administrator account must belong to a role that has Plug-in Management Install and View permissions for the VPT application.



Note The Cisco Voice Provisioning Tool automatically detects whether you have Release 1.0 of the Cisco Unified CallManager 4.1(3) plug-in installed, and performs an installation or upgrade as appropriate.

-
- Step 1** If your system is running Cisco Voice Provisioning Tool release 1.0(1), update the JAVA_HOME and PATH environment variables prior to installing or upgrading the plug-in.
- a. On the VPT server, on the Windows Start menu, choose **Settings > Control Panel > System**.
 - b. Click the **Advanced** tab.
 - c. Click **Environment Variables**.
 - d. In the System Variables list, find and click the **JAVA_HOME** variable and click **Edit**.
 - e. If it is not already present in the variable value, add the full path to directory of the JDK that is installed with VPT. Make sure that a semicolon (;) separates the new entry from any other entries. For example, if the JDK was installed in C:\j2sdk1.4.2_03, add the following to the end of the variable value:


```
;C:\j2sdk1.4.2_03
```
 - f. Click **OK**.
 - g. In the System Variables list, find and click the **Path** variable and click **Edit**.

- h. If it is not already present in the variable value, add the full path to the bin directory of the JDK that is installed with VPT. Make sure that a semicolon (;) separates the new entry from any other entries. For example, if the JDK was installed in C:\j2sdk1.4.2_03, add the following to the end of the variable value:

```
;C:\j2sdk1.4.2_03\bin
```

- i. Click **OK**.
- j. Close the System Properties and Control Panel windows.
- k. Restart the server for the changes to take effect.

Step 2 Open a browser and go to <http://www.cisco.com/cgi-bin/tablebuild.pl/VPT>.

The Cisco Voice Provisioning Tool software page opens.



Tip When you download the plug-in, the browser gives you the option of saving the file to disk or opening the file. Save the file to disk before you install or upgrade the plug-in.

Step 3 To download the Cisco Unified CallManager plug-in, click the Cisco Unified CallManager plug-in zip file, which uses the following format: ccm_<Cisco Unified CallManager supported version>_<plug-in version>.zip.

For example, click ccm_4_1_3_v3_0.zip.

Step 4 To install the plug-in after you download it, open the VPT graphical user interface (GUI), as described in the *Cisco Voice Provisioning Tool System Management and Security Guide*.

Step 5 After you log in to the GUI, choose **VPT Administration > Plug-Ins > Install New Plug-In**.

Step 6 On the Install New Plugin page, enter the name of the download, or browse to the file by clicking **Browse**.

Step 7 Click **Install**.



Note The Voice Provisioning Tool restarts after you confirm that you want to install or upgrade a plug-in.

Caveats

This section contains information on the following topics:

- [Using Bug Toolkit, page 7](#)
- [Saving Bug Toolkit Queries, page 8](#)
- [Open Caveats—Release 3.0, page 9](#)
- [Resolved Caveats—Release 3.0, page 9](#)

This section contains caveat information for the Cisco Unified CallManager 4.1(3) plug-in Release 3.0 for the Cisco Voice Provisioning Tool only. See the release notes of the applicable version for caveat information for the Cisco Voice Provisioning Tool or Cisco Unified CallManager.

- Release notes for the Cisco Voice Provisioning Tool are available at http://www.cisco.com/en/US/products/ps6524/prod_release_notes_list.html.

- Release notes for all versions of Cisco Unified CallManager are available at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_release_notes_list.html.

Using Bug Toolkit

To access Bug Toolkit, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password



Tip

For detailed online Help with Bug Toolkit, click Help on any Bug Toolkit page.

To Use Bug Toolkit

- Step 1** To access the Bug Toolkit, go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.
- Step 2** Log on with your Cisco.com user ID and password.
- Step 3** Click the **Launch Bug Toolkit** hyperlink.
- Step 4** To find information about a specific caveat, enter the ID number in the Enter Known Bug ID field.
- Step 5** To view all caveats for the Cisco Voice Provisioning Tool, go to the Search for Bugs in other Cisco Software and Hardware Products section, and enter **Cisco Voice Provisioning Tool** in the Product Name field. Alternatively, you can scroll through the product name list and click **Cisco Voice Provisioning Tool**.
- Step 6** Click **Next**. The search window displays.
- Step 7** Choose the filters to query for caveats. You can choose any or all of the available options:
- Choose the Cisco Voice Provisioning Tool version.
 - Choose the major version for the major releases (such as 1.0 and so on).
A major release contains significant new features, enhancements, architectural changes, and/or defect fixes.
 - Choose the revision for more specific information; for example, choosing major version 1.0 and revision version 1 queries for release 1.0(1) caveats.
A revision (maintenance) release primarily contains defect fixes to address specific problems, but it may also include new features and/or enhancements.
 - Choose the Features or Components to query; choose an option from the Available list and click **Add** to place your selection in the Limit Search To list.
 - To query for all Cisco Voice Provisioning Tool caveats for a specified release, choose **All Features** in the left pane.
 - To query only for phone provisioning defects, choose **Phone-Prov** and click **Add**.
 - To query only for user provisioning defects, choose **User-Prov** and click **Add**.
 - To query only for installation defects, choose **Install** and click **Add**.
 - To query only for bulk administration defects, choose **Bulk** and click **Add**.
 - To query only for security defects, choose **Security** and click **Add**.

- Enter keywords to search for a caveat title and description.



Note To make queries less specific, use the All wildcard for the major version/revision, features/components, and keyword options.

- Choose the Set Advanced Options, including the following items:
 - Bug Severity level—The default specifies 1-3.
 - Bug Status Group—To view resolved caveats, check the **Fixed** check box.
 - Release Note Enclosure—The default specifies Valid Release Note Enclosure.

Step 8 Click **Next**.

The Bug Toolkit returns a list of caveats based on your query. You can modify your results by submitting another query and choosing different criteria. You can also save your query for future use, as described in the “[Saving Bug Toolkit Queries](#)” section on page 8.

Saving Bug Toolkit Queries

Bug Toolkit allows you to create and then save your queries to monitor a specific defect or network situation. You can edit a saved search at any time to change the alert conditions, the defects being watched, or the network profile.

To save your Bug Toolkit queries, do the following procedure.

To Save Bug Toolkit Queries

Step 1 Search for caveats, as described in the “[To Use Bug Toolkit](#)” procedure on page 7.

Step 2 In the search result window, click the **This Search Criteria** button.

Step 3 After the page displays, enter a name for the saved search in the Name of Saved Search field.

Step 4 Under My Bug Groups, click one of the following radio buttons to save your defects in a bug group:

- Click the **Existing Group** radio button and choose an existing group name from the drop-down list box.
- Click the **Create New Group Named** radio button and enter a group name to create a new group for this saved search.

This bug group contains the bugs that are identified by using the search criteria that you saved. Each time that a new bug meets the search criteria, the system adds it to the group that you chose.

Bug Toolkit makes your queries available through the My Stuff window, which allows you to view, create, and/or modify existing bug groups or saved searches. Choose the **My Stuff** link to see a list of your bug groups.

Step 5 Under Email Update Options, you can set e-mail notification preferences if you want to receive automatic updates of a bug status change. Bug Toolkit provides the following options:

- **Do Not Send Me Any Email Updates**—If you choose this setting, Bug Toolkit does not send e-mail notifications.
- **Send My Updates To**—Click this radio button if you want e-mail notifications to go to the user ID that you enter in this field. You can specify the following notification options:

- **Updates As They Occur**—Bug Toolkit provides updates that are based on status change.
- **Weekly Summaries**—Bug Toolkit provides weekly summary updates.
- **Apply These Email Update Options to All of My Saved Searches**—Check this check box to use these e-mail update options for all of your saved searches.

Step 6 To save your changes, click **Save**.

A window displays the bug group(s) that you have saved. From this window, you can click a bug group name to see the bugs and the saved searches; you can also edit the search criteria.

Open Caveats—Release 3.0

[Table 1](#) describes possible unexpected behaviors in Release 3.0 of the Cisco Unified CallManager 4.1(3) plug-in for VPT, sorted by component, then by caveat number.



Note

For more information about an individual defect, click the associated Caveat Number to access the online record for that defect, including workarounds.

Because defect status continually changes, be aware that the list in [Table 1](#) reflects a snapshot of the defects that were open at the time this report was compiled. For an updated view of open defects, access Bug Toolkit and follow the instructions as described in the [“To Use Bug Toolkit” procedure on page 7](#).

Table 1 *Open Caveats for Cisco Unified CallManager 4.1(3) Plug-in, Release 3.0*

Caveat Number	Severity	Component	Description
CSCsd08794	3	bulk	Bulk: Bulk value is not the same as GUI value.
CSCse97904	3	bulk	Bulk Exp Task may become uneditable if product systems removed
CSCsd01170	3	ccm-op	User Default Profile cannot be set to None
CSCsa72225	3	phone-prov	IP phone service parameters are not being encoded/decoded properly
CSCsb49130	3	phone-prov	MLPP Domain not getting saved for 7910/7920/7935/7936 phones
CSCse90108	3	phone-prov	ModifyPhone:Module1&2 Load Name not saved (if not selected module 1/2)
CSCse91206	3	phone-prov	Add Line> Error message when modifying second line

Resolved Caveats—Release 3.0

[Table 2](#) describes defects that were resolved in Release 3.0 of the Cisco Unified CallManager 4.1(3) plug-in for VPT. (Caveats are listed in order by severity, then by component, then by caveat number.)



Note

For more information about an individual defect, click the associated Caveat Number to access the online record for that defect, including workarounds.

Because defect status continually changes, be aware that the list in [Table 2](#) reflects a snapshot of the defects that were resolved at the time this report was compiled. For an updated view of resolved defects, access Bug Toolkit and follow the instructions as described in the [“To Use Bug Toolkit” procedure on page 7](#).

Table 2 Resolved Caveats for Cisco Unified CallManager 4.1(3) Plug-in, Release 3.0

Caveat Number	Severity	Component	Description
CSCsb40475	2	phone-prov	Missing data in CCM response due to invalid nil
CSCsb27274	2	user-prov	Users not found if CCM uses Netscape or Active Directory instead of DC
CSCsb52156	3	ccm-op	Shared Settings do not seem to save and propagate
CSCsa88634	3	phone-prov	Multimod-phone:Display On/Idle fields permit invalid entry of 0:00
CSCsb28156	3	phone-prov	Add Phone GUI: accentuated character garbled or ignored
CSCsb46764	3	phone-prov	VPT shows Audio Sources deleted from CCM Admin
CSCsb49130	3	phone-prov	MLPP Domain not getting saved for 7910, 7920, 7935, and 7936 phones
CSCsb49954	3	phone-prov	Use Current Device Settings option not shown if no user profiles exist
CSCsb07218	3	user-prov	CCM Users with no first name are not returned in search

Documentation Updates

This section lists new and additional information that is not included in the current Cisco Voice Provisioning Tool documentation. The new and additional information will be incorporated in a future documentation release.

This section covers the following document updates and omissions:

- [Advanced Phone Settings, page 10](#)
- [Installing, Upgrading, and Removing Plug-ins, page 11](#)

Advanced Phone Settings

The new settings in [Table 3](#) apply to the “Advanced Phone Configuration Settings” table in the “Phone Configuration Settings” chapter of the *Cisco Voice Provisioning Tool User and Phone Management Guide*.

Table 3 New Settings for the Advanced Phone Configuration Settings Table

Setting	Description
Logging Display	This parameter is used only by Cisco TAC for troubleshooting.
Load Server	The Load Server option is used to optimize installation time for phone firmware upgrades. You can set the Load Server to another TFTP server IP address or name (other than the TFTP Server 1 or TFTP Server 2) from which the phone firmware can be retrieved for upgrades on the phones. When the Load Server option is set, the phone contacts the designated server for the firmware upgrade. Note Even if a Load Server is configured, the phone continues to use TFTP Server 1 or TFTP Server 2 for obtaining configuration files.

Table 3 **New Settings for the Advanced Phone Configuration Settings Table (continued)**

Setting	Description
Use of PhoneBook or IP Phone Services Softkey	Set softkey to access Phone Book (PhBook) or IP Phone Services (Svc) when the phone is idle.
Initial Display of Cisco Unified CallManager Softkeys During a Call	Set the phone to display features in the Cisco Unified CallManager softkey template instead of the default softkeys for the Cisco Wireless IP Phone (MuteOn and EndCall).

Installing, Upgrading, and Removing Plug-ins

The *Cisco Voice Provisioning Tool Installation and Upgrade Guide* does not include information on upgrading, installing or removing plug-ins. For instructions on upgrading Cisco Unified CallManager plug-ins, see the “[Installation Notes](#)” section on page 5. For instructions on installing or removing plug-ins, see the *Cisco Voice Provisioning Tool Release Notes*.

Related Documentation

See the following documents for more information on the Cisco Voice Provisioning Tool and Cisco Unified CallManager:

- *Cisco Voice Provisioning Tool Documentation Guide*
This guide lists and describes the documents that make up the Cisco Voice Provisioning Tool documentation set. The guide is available at http://www.cisco.com/en/US/products/ps6524/products_documentation_roadmaps_list.html.
- *Cisco Voice Provisioning Tool Installation and Upgrade Guide, Release 1.0(2)*
This guide describes how to install and upgrade the Cisco Voice Provisioning Tool. The guide is available at http://www.cisco.com/en/US/products/ps6524/prod_installation_guides_list.html.
- *Cisco Voice Provisioning Tool System Management and Security Guide*
This guide provides descriptions of the Cisco Voice Provisioning Tool and its components, as well as step-by-step instructions for configuring and managing the tool itself. The guide is available at http://www.cisco.com/en/US/products/ps6524/prod_maintenance_guides_list.html.
- *Cisco Voice Provisioning Tool User and Phone Management Guide*
This guide provides information on provisioning users, phones, and device profiles for Cisco Unified CallManager and Cisco Unity. The guide is available at http://www.cisco.com/en/US/products/ps6524/prod_maintenance_guides_list.html.
- *Cisco Unified CallManager Documentation Guide*
Provides a list of Cisco Unified CallManager documents that are available with the release (for example, the 4.1(3) release). The document also provides a URL for each document so that you can locate the document on the web. The guide is available at http://www.cisco.com/en/US/products/sw/voicew/ps556/products_documentation_roadmaps_list.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://cisoiq.texterity.com/cisoiq/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/learning/index.html>

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, 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, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, 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. (0601R)

© 2006 Cisco Systems, Inc. All rights reserved.

