



# Release Notes for Cisco Unity Connection 1.2(1) Plug-in, Release 1.0 (for Cisco Voice Provisioning Tool)

---

*Published August 11, 2006*

These release notes describe system requirements, installation notes, caveats, documentation notes, and technical assistance information for release 1.0 of the Cisco Unity Connection 1.2(1) Plug-in for the Cisco Voice Provisioning Tool.

## Contents

These release notes contain the following sections:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [Installation Notes, page 3](#)
- [Caveats, page 4](#)
- [Documentation Updates, page 7](#)
- [Related Documentation, page 21](#)
- [Obtaining Documentation, page 22](#)
- [Documentation Feedback, page 22](#)
- [Cisco Product Security Overview, page 23](#)
- [Obtaining Technical Assistance, page 24](#)
- [Obtaining Additional Publications and Information, page 25](#)



---

**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 Unity Connection 1.2(1) plug-in for VPT allows you to use VPT to perform user provisioning tasks on Cisco Unity Connection 1.2(1) systems. (You can use VPT to provision users with mailboxes but not administrators or technicians. To provision administrators or technicians, you must use Cisco Unity Connection Administration.)

## System Requirements

The following subsections describe the hardware and software requirements for the Cisco Unity Connection 1.2(1) 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](http://www.cisco.com/en/US/products/ps6524/prod_release_notes_list.html).

### Software Compatibility

The 1.0 release of the Cisco Unity Connection 1.2(1) plug-in can be installed on a server running Cisco Voice Provisioning Tool release 1.0(2).

The following requirements must be met on the Cisco Unity Connection server to interoperate with the Cisco Unity Connection 1.2(1) plug-in:

- Cisco Unity Connection version 1.2(1) must be running on any product systems that will be configured to use the plug-in.

### 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**.

# Installation Notes

## To Install the Cisco Unity Connection 1.2(1) Plug-in

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

**Step 1** Open a browser and go to <http://www.cisco.com/cgi-bin/tablebuild.pl/VPT>.

The Cisco Voice Provisioning Tool software page displays.



**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 the plug-in.

**Step 2** To download the Cisco Unity Connection plug-in, click the Cisco Unity Connection plug-in zip file, which uses the following format: cuc\_<Cisco Unity Connection supported version>\_<plug-in version>.zip.

For example, click cuc\_1\_2\_1\_v1\_0.zip.

**Step 3** 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 4** Log in to the GUI, then choose **VPT Administration > Plug-Ins > Install New Plug-In**.

**Step 5** On Install New Plugin page, enter the name of the download, or browse to the file by clicking **Browse**.

**Step 6** Click **Install**.

## To Remove a Cisco Unity Connection Plug-in



**Note** When the plug-in that you are removing is the only plug-in of a particular product type, all permissions related to that product type will be removed from any roles to which they were assigned. For a Cisco Unity Connection plug-in, the All UNITY Cisco Unity Connection product system name and any associated privileges will be removed from all roles in the system. When you install the Cisco Unity Connection 1.2(1) plug-in, you will need to manually restore the permissions to any customer-defined roles. However, the pre-defined SuperAdmin, Full Provisioning, and View-Only roles will be automatically updated with the default set of permissions for the product type.

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

**Step 1** Open the VPT graphical user interface (GUI), as described in the *Cisco Voice Provisioning Tool System Management and Security Guide*.

**Step 2** Log in to the GUI, then choose **VPT Administration > Plug-Ins > Manage Plug-Ins**.

**Step 3** On the Manage Plug-Ins page, check the check box to the left of the Cisco Unity Connection plug-in that you are removing.




---

**Note** You cannot remove a plug-in if product systems are configured to use that plug-in. You must remove all such product systems from the tool prior to uninstalling the plug-in.

---

**Step 4** Click **Uninstall**.

**Step 5** When you are prompted to remove the plug-in, click **OK** to continue.




---

**Note** The Cisco Voice Provisioning Tool restarts after you confirm that you want to remove a plug-in.

---

## Caveats

This section contains information on the following topics:

- [Using Bug Toolkit, page 4](#)
- [Saving Bug Toolkit Queries, page 6](#)
- [Open Caveats—Release 1.0, page 6](#)

This section contains caveat information for the Cisco Unity Connection 1.2(1) plug-in 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 Unity Connection.

- Release notes for the Cisco Voice Provisioning Tool are available at [http://www.cisco.com/en/US/products/ps6524/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/ps6524/prod_release_notes_list.html).
- Release notes for all versions of Cisco Unity Connection are available at [http://www.cisco.com/en/US/products/ps6509/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/ps6509/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](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 2 queries for release 1.0(2) 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 6](#).

---

## 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 4](#).
- 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 1.0

[Table 1](#) describes possible unexpected behaviors in the Cisco Unity Connection 1.2(1) plug-in for VPT.

**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 4](#).

**Table 1**      **Open Caveats for Cisco Unity Connection 1.2(1) Plug-in for VPT Release 1.0**

Caveat Number	Severity	Component	Description
<a href="#">CSCse21946</a>	3	user-prov	Inappropriate error message displayed for Warn Quota
<a href="#">CSCse36898</a>	3	user-prov	Multi Modify user failure error is not displayed on top of the page
<a href="#">CSCse45771</a>	3	user-prov	Unable to see all the digits in the extension
<a href="#">CSCse45822</a>	3	user-prov	Unable to add a user with a valid extension
<a href="#">CSCse48616</a>	3	user-prov	Incorrect error message when deleting a user while server is unreachable
<a href="#">CSCse48792</a>	3	user-prov	Voice Conversations not disabled when Voice recognition is not selected

## 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:

- [Adding a Cisco Unity Connection Product System, page 7](#)
- [Installing and Removing Plug-ins, page 13](#)
- [Cisco Unity Connection User Configuration Settings, page 13](#)
- [User Settings for Bulk Provisioning, page 13](#)

## Adding a Cisco Unity Connection Product System

Use the task list that follows to add a Cisco Unity Connection system to the Cisco Voice Provisioning Tool.

1. Set up the Cisco Unity Connection server. See the *Cisco Unity Connection Installation Guide*, at [http://www.cisco.com/en/US/products/ps6509/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html).
2. Set up an administrative account on the Cisco Unity Connection server to be used by VPT to authenticate with the product system. See the [“Setting Up a Provisioning Account on the Cisco Unity Connection Server” section on page 8](#)
3. Add the Cisco Unity Connection system to VPT as a new product system. See the [“Adding a New Cisco Unity Connection Product System to the Cisco Voice Provisioning Tool” section on page 8](#).
4. Configure SSL. See the [“Configuring SSL” section on page 9](#).
5. Test the product system connection. See the [“Testing the Product System Connection” section on page 12](#).

## Setting Up a Provisioning Account on the Cisco Unity Connection Server

You must configure the Cisco Voice Provisioning Tool by using an account that has full access rights to Cisco Unity Connection Administration.

You can use an existing Cisco Unity Connection user account that can log in to Cisco Unity Connection Administration and that belongs to a class of service that has permissions to add and delete users. However, we recommend that you set up a separate Connection user specifically for use with VPT and notify other administrators that the user should not be deleted. You can also give the new user a display name that indicates the purpose of the account and specifies that it should not be removed from the system. See the *Cisco Unity Connection User Moves, Adds, and Changes Guide* for details on setting up users. The guide is available at [http://www.cisco.com/en/US/products/ps6509/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html).

## Adding a New Cisco Unity Connection Product System to the Cisco Voice Provisioning Tool

For each Cisco Unity Connection server, you configure a product system in VPT. To add a Connection server as a new product system in VPT, do the following procedure.



### Note

To add a product system, your administrator account must belong to a role that has Product Systems Management Add permissions for the VPT application. If you do not see the VPT Administration > Product Systems > Add New Product System option in the VPT navigation menu, your account does not have the applicable permissions.

### To Add a New Cisco Unity Connection Product System

**Step 1** In the Cisco Voice Provisioning Tool, choose **VPT Administration > Product Systems > Add New Product System**.

The Add New Product System window displays.

**Step 2** On the Product System Type drop-down list, click **UNITY-Connection 1.2(1)**.



**Note** The options available when adding a new product system depend on the product system type that you choose in this step.

**Step 3** Enter the Product System Name.

**Step 4** Optionally, enter the URL for the Cisco Unity Connection Administration interface.

This allows administrators with sufficient permissions to click the Product SA URL link from the Manage Product Systems window to easily browse to this URL to carry out any additional configuration activities.

This URL is typically **https://<Connection Server Name or IP Address>/cuadmin**.

**Step 5** Optionally, enter a description for the product system.

**Step 6** Enter the Connection IP Address/Hostname.

**Step 7** In the Connection CUAL Port field, enter **443**.

**Step 8** Enter the Cisco Unity Connection Login ID and Password and confirm the password.

This information must match the provisioning account on the Connection server.

**Step 9** Click **Save**.

---

## Configuring SSL

Do the following tasks to set up secure communication between the Cisco Unity Connection server and the VPT server:

1. If you do not already have access to a copy of the server certificate, export a copy by doing the applicable procedure:
  - [To Export a Certificate Issued Either by Microsoft Certificate Services or by a Certificate Authority \(CA\), page 9](#)
  - [To Export a Self-Signed Certificate, page 10](#)



**Note** Cisco Unity Connection automatically creates a self-signed certificate during installation. However, if you installed a certificate either that you issued using Microsoft Certificate Services or that you had issued by another Certificate Authority, we recommend that you do the [“To Export a Certificate Issued Either by Microsoft Certificate Services or by a Certificate Authority \(CA\)” procedure on page 9](#) because this type of certificate is more secure than a self-signed certificate.

---

2. Copy the certificate(s) to the VPT server. See the [“To Copy Certificates to the VPT Server” procedure on page 10](#).
3. Add the Connection certificate(s) to a keystore on the VPT server. See the [“To Add Certificates to a Keystore by Using Keytool” procedure on page 11](#).
4. If you have not already done so, configure the keystore properties in the Cisco Voice Provisioning Tool. See the [“To Configure Keystore Information in the Cisco Voice Provisioning Tool” procedure on page 12](#).

### To Export a Certificate Issued Either by Microsoft Certificate Services or by a Certificate Authority (CA)

---

- Step 1** On the CA server, on the Windows Start menu, choose **Programs > Administrative Tools > Certification Authority**.
- Step 2** In the left pane of the Certification Authority window, right-click the <Root Certification Authority name>, and click **Properties**.
- Step 3** Click **View Certificate**.
- Step 4** Click the **Details** tab.
- Step 5** In the Show list, choose **All** and click **Copy to File**.
- Step 6** On the Certificate Export wizard welcome window, click **Next**.
- Step 7** Click **Base-64 Encoded X.509 (.CER)** and click **Next**.
- Step 8** Specify a file name and a location and click **Next**.
- Step 9** Verify the settings and click **Finish**.
- Step 10** To close the Certificate Details dialog box, click **OK**.
- Step 11** To close the Properties dialog box for the Root Certification Authority, click **OK**.

**Step 12** Close the **Certification Authority** window.

---

#### To Export a Self-Signed Certificate

---

- Step 1** On the Connection server, in Windows Explorer, browse to the directory **C:\Program Files\Cisco Systems\Cisco Unity Connection\store\public**.
- Step 2** Double-click the file **cucert.crt**.
- Step 3** In the Certificate dialog box, click the **Details** tab.
- Step 4** Click **Copy to File**.
- Step 5** On the Welcome to the Certificate Export Wizard page, click **Next**.
- Step 6** On the Export File Format page, click **Base-64 Encoded X.509 (CER)**, and click **Next**.
- Step 7** On the File to Export page, specify a file name and a location and click **Next**.
- Step 8** On the Completing the Certificate Export Wizard page, click **Finish**.
- Step 9** Verify the settings, and click **Finish**.
- Step 10** To close the Certificate dialog box, click **OK**.
- 

#### To Copy Certificates to the VPT Server


---

- Step 1** Copy the certificate(s) to the VPT server by doing the applicable steps:
- Recommended—By using a floppy disk. Continue with [Step 2](#).
  - For secure networks—By using a network share. Skip to [Step 3](#).
- Step 2** If you are using a floppy disk to copy the certificate, do the following sub-steps:
- a. Insert an empty formatted floppy disk in the floppy drive of the Connection or CA server.
  - b. Browse to the directory that contains the certificate (.CER) file.
  - c. Copy the certificate file to the floppy disk.
  - d. Remove the floppy disk from the Connection or CA server.
  - e. Insert the floppy disk in the floppy drive of a VPT server.
  - f. Copy the certificate file on the floppy disk to a directory on the VPT server.
  - g. For security, delete the certificate file on the floppy disk.
- Step 3** If you are using a secure network share to copy the certificate, do the following sub-steps:
- a. On the Connection or CA server, browse to the directory that contains the certificate.
  - b. Select the certificate file, and press **Ctrl-C**.
  - c. Open a network share to the VPT server and log on.
  - d. Browse to or create a directory on the VPT server in which to store certificates.
  - e. To paste the certificate file, press **Ctrl-V**.
-

To configure VPT to communicate with a Connection system that is using SSL, you must use the keytool application, which is included as part of the Sun Microsystems Java Development Kit (JDK) when you install the Cisco Voice Provisioning Tool.

The keytool application creates a keystore (by default, the keystore is stored as a file). You can store multiple certificates in a keystore; the keystore is created automatically when you add the first certificate by using the keytool application. For more information on the keytool command, refer to the Sun Microsystems Java Development Kit documentation.

### To Add Certificates to a Keystore by Using Keytool

- Step 1** On the VPT server, check to make sure that the PATH environment variable on the system includes the path to the bin directory of the JDK that is installed with VPT:
- On the Windows Start menu, choose **Settings > Control Panel > System**.
  - Click the **Advanced** tab.
  - Click **Environment Variables**.
  - In the System Variables list, find and click the **Path** variable and click **Edit**.
  - If it is not already present in the path, 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 path:  
**;C:\j2sdk1.4.2\_03\bin**
  - Click **OK**.
  - Close the System Properties and Control Panel windows.
- Step 2** Verify that the JDK tools are available by using the path specified in [Step 1](#):
- On the Windows Start menu, choose **Programs > Accessories > Command Prompt**.
  - In the command prompt window, enter **javac**. If the path is set correctly, usage information for the javac command displays.
- Step 3** In the command prompt window that opened in [Step 2](#), change to the directory where the Cisco Voice Provisioning Tool is installed. For example, enter:  
**cd C:\Program Files\Cisco Systems\Voice Provisioning Tool**  
and press **Enter**.
- Step 4** Enter  
**keytool -import -alias <Name of Server the Certificate was Obtained From> -storepass <Password> -File <Certificate File> -keystore <Keystore File>**  
and press **Enter**.
- We recommend that you use the name of the Connection server or certificate authority from which the certificate was obtained for the alias. For example, if a self-signed certificate file from server connection1 is stored in C:\certificates\connection1-cert.CER, you might enter: **keytool -import -alias connection1 -storepass pa\$\$w0rd! -File C:\certificates\connection1-cert.CER -keystore C:\VPTProdSysKeystore**
-  **Note** The -keystore parameter specifies a file that holds the keystore. If you do not specify a full path, the file is created in the directory in which you run the keytool command. You will need to know the full path to the keystore file to configure the VPT security settings in the next procedure.
- Step 5** When prompted to trust the certificate, enter **yes** and press **Enter**.

- Step 6** To verify that the import was successful, enter **keytool -list -keystore <Keystore File>** and press **Enter**.
- Step 7** Repeat [Step 4](#) through [Step 6](#) for each certificate.



**Note** Ensure all product system keys are stored in the same keystore for the Cisco Voice Provisioning Tool to access them. Make sure you use the correct syntax for the keystore value each time that you enter a new certificate.

- Step 8** Close the command prompt window.



**Note** To configure keystore settings, your administrator account must belong to a role that has VPT Configuration Modify permissions for the VPT application. If you do not see the VPT Administration > Configuration option in the VPT navigation menu, your account does not have the applicable permissions.

#### To Configure Keystore Information in the Cisco Voice Provisioning Tool

- Step 1** In the Cisco Voice Provisioning Tool, choose **VPT Administration > Configuration**. The Configuration window displays.
- Step 2** In the Security settings section, enter the full path of the keystore and the password that you specified in [Step 4](#) of the “[To Add Certificates to a Keystore by Using Keytool](#)” procedure on page 11.
- Step 3** Click **Save**.
- Step 4** For the changes to take effect, you must restart the Tomcat service. On the Windows Start menu, choose **Programs > Administrative Tools > Services**. In the right pane, locate **VPT Tomcat**, right-click it, and click **Restart**.

## Testing the Product System Connection

When the product system setup is complete, you should test it by using the check that the tool provides.



**Note** To test product system connections, your administrator account must belong to a role that has Product System Connection Test permissions for the product system. If you do not see the VPT Administration > Product Systems > Manage Product Systems option in the VPT navigation menu, your account does not have the applicable permissions.

#### To Test the Product System Connection

- Step 1** In the Cisco Voice Provisioning Tool, choose **VPT Administration > Product Systems > Manage Product Systems**. The Manage Product Systems window displays a list of configured product systems.

- Step 2** Click the Test button in the Test Connection column of the product system that you want to test. If the test is successful, you should see a PASSED result for all tests.

## Installing and Removing Plug-ins

The *Cisco Voice Provisioning Tool Installation and Upgrade Guide* does not include information on installing or removing plug-ins. See the “Installation Notes” section on page 3 for instructions on adding or removing plug-ins.

## Cisco Unity Connection User Configuration Settings

Fields in the Cisco Unity Connection 1.2(1) plug-in have the same definitions as fields of the same name in Cisco Unity Connection. For field definitions, see the Cisco Unity Connection Administration Help.

## User Settings for Bulk Provisioning

The Cisco Unity Connection 1.2(1) plug-in extends the bulk-provisioning functionality of the Cisco Voice Provisioning Tool and allows you to add or modify a large number of users to a Cisco Unity Connection server. Before you perform any bulk operations, review the “Bulk Provisioning Overview” chapter of the *Cisco Voice Provisioning Tool User and Phone Management Guide*, at [http://www.cisco.com/en/US/products/ps6524/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6524/prod_maintenance_guides_list.html).

The user configuration settings that you can include in the CSV file for bulk provisioning tasks with Cisco Unity Connection 1.2(1) plug-in are identical to those available from the GUI. You can export one user record to get a CSV file that shows header names for all supported settings.

Some settings accept special values, as described below.

### **unity\_user\_country**

Only 2 letter country codes assigned in the ISO 3316-1 standard are acceptable.

### **unity\_user\_timeZone**

Only time zone codes specified in Table 2 are acceptable.

**Table 2** Valid Time Zone Codes for Bulk Import

Time Zone Code	Time Zone Name
300	(GMT+13:00) Nuku'alofa
290	(GMT+12:00) Auckland, Wellington
285	(GMT+12:00) Fiji, Kamchatka, Marshall Is.
280	(GMT+11:00) Magadan, Solomon Is., New Caledonia
275	(GMT+10:00) Guam, Port Moresby
265	(GMT+10:00) Hobart
270	(GMT+10:00) Vladivostok
255	(GMT+10:00) Canberra, Melbourne, Sydney

**Table 2** Valid Time Zone Codes for Bulk Import (continued)

Time Zone Code	Time Zone Name
260	(GMT+10:00) Brisbane
250	(GMT+09:30) Adelaide
245	(GMT+09:30) Darwin
240	(GMT+09:00) Yakutsk
230	(GMT+09:00) Seoul
235	(GMT+09:00) Osaka, Sapporo, Tokyo
225	(GMT+08:00) Perth
220	(GMT+08:00) Taipei
227	(GMT+08:00) Irkutsk, Ulaan Bataar
215	(GMT+08:00) Kuala Lumpur, Singapore
210	(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi
205	(GMT+07:00) Bangkok, Hanoi, Jakarta
207	(GMT+07:00) Krasnoyarsk
203	(GMT+06:30) Rangoon
200	(GMT+06:00) Sri Jayawardenepura
201	(GMT+06:00) Almaty, Novosibirsk
195	(GMT+06:00) Astana, Dhaka
193	(GMT+05:45) Kathmandu
190	(GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi
185	(GMT+05:00) Islamabad, Karachi, Tashkent
180	(GMT+05:00) Ekaterinburg
175	(GMT+04:30) Kabul
170	(GMT+04:00) Baku, Tbilisi, Yerevan
165	(GMT+04:00) Abu Dhabi, Muscat
160	(GMT+03:30) Tehran
155	(GMT+03:00) Nairobi
150	(GMT+03:00) Kuwait, Riyadh
145	(GMT+03:00) Moscow, St. Petersburg, Volgograd
158	(GMT+03:00) Baghdad
130	(GMT+02:00) Athens, Beirut, Istanbul, Minsk
115	(GMT+02:00) Bucharest
120	(GMT+02:00) Cairo
125	(GMT+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius
140	(GMT+02:00) Harare, Pretoria
135	(GMT+02:00) Jerusalem
100	(GMT+01:00) Sarajevo, Skopje, Warsaw, Zagreb

**Table 2** Valid Time Zone Codes for Bulk Import (continued)

Time Zone Code	Time Zone Name
113	(GMT+01:00) West Central Africa
110	(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
95	(GMT+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
105	(GMT+01:00) Brussels, Copenhagen, Madrid, Paris
90	(GMT) Casablanca, Monrovia
85	(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
83	(GMT-01:00) Cape Verde Is.
80	(GMT-01:00) Azores
75	(GMT-02:00) Mid-Atlantic
65	(GMT-03:00) Brasilia
70	(GMT-03:00) Buenos Aires, Georgetown
73	(GMT-03:00) Greenland
60	(GMT-03:30) Newfoundland
56	(GMT-04:00) Santiago
55	(GMT-04:00) Caracas, La Paz
50	(GMT-04:00) Atlantic Time (Canada)
45	(GMT-05:00) Bogota, Lima, Quito
35	(GMT-05:00) Eastern Time (US & Canada)
40	(GMT-05:00) Indiana (East)
25	(GMT-06:00) Saskatchewan
30	(GMT-06:00) Guadalajara, Mexico City, Monterrey
33	(GMT-06:00) Central America
20	(GMT-06:00) Central Time (US and Canada)
13	(GMT-07:00) Chihuahua, La Paz, Mazatlan
15	(GMT-07:00) Arizona
10	(GMT-07:00) Mountain Time (US and Canada)
4	(GMT-08:00) Pacific Time (US and Canada); Tijuana
3	(GMT-09:00) Alaska
2	(GMT-10:00) Hawaii
1	(GMT-11:00) Midway Island, Samoa
0	(GMT-12:00) International Date Line West

**unity\_user\_language**

Only language codes specified in [Table 3](#) are acceptable.

**Table 3** Valid Language Codes for Bulk Import

Language Code	Name	Description
10241	ArabicSyria	Arabic_Syria 10241
10249	EnglishBelize	English_Belize 10249
1025	ArabicSaudiArabia	Arabic_Saudi_Arabia 1025
10250	SpanishPeru	Spanish_Peru 10250
1026	Bulgarian	Bulgarian 1026
1027	Catalan	Catalan 1027
1028	ChineseTaiwan	Chinese_Taiwan 1028
1029	Czech	Czech 1029
1030	Danish	Danish 1030
1031	GermanStandard	German_Standard 1031
1032	Greek	Greek 1032
1033	EnglishUnitedStates	English_United_States 1033
1034	SpanishTraditionalSort	Spanish_Traditional_Sort 1034
1035	Finnish	Finnish 1035
1036	FrenchStandard	French_Standard 1036
1037	Hebrew	Hebrew 1037
1038	Hungarian	Hungarian 1038
1039	Icelandic	Icelandic 1039
1040	ItalianStandard	Italian_Standard 1040
1041	Japanese	Japanese 1041
1042	Korean	Korean 1042
1043	DutchStandard	Dutch_Standard 1043
1044	NorwegianBokmal	Norwegian_Bokmal 1044
1045	Polish	Polish 1045
1046	PortugueseBrazilian	Portuguese_Brazilian 1046
1047	RhaetoRomanic	Rhaeto-Romanic 1047
1048	Romanian	Romanian 1048
1049	Russian	Russian 1049
1050	Croatian	Croatian 1050
1051	Slovak	Slovak 1051
1052	Albanian	Albanian 1052
1053	Swedish	Swedish 1053
1054	Thai	Thai 1054
1055	Turkish	Turkish 1055
1056	Urdu	Urdu 1056
1057	Indonesian	Indonesian 1057

**Table 3** Valid Language Codes for Bulk Import (continued)

Language Code	Name	Description
1058	Ukrainian	Ukrainian 1058
1059	Belarusian	Belarusian 1059
1060	Slovenian	Slovenian 1060
1061	Estonian	Estonian 1061
1062	Latvian	Latvian 1062
1063	Lithuanian	Lithuanian 1063
1065	Farsi	Farsi 1065
1066	Vietnamese	Vietnamese 1066
1067	Armenian	Armenian 1067
1068	AzeriLatin	Azeri_Latin 1068
1069	Basque	Basque 1069
1070	Sorbian	Sorbian 1070
1071	Macedonian	Macedonian 1071
1072	Sutu	Sutu 1072
1073	Tsonga	Tsonga 1073
1074	Tswana	Tswana 1074
1076	Xhosa	Xhosa 1076
1077	Zulu	Zulu 1077
1078	Afrikaans	Afrikaans 1078
1079	Georgian	Georgian 1079
1080	Faeroese	Faeroese 1080
1081	Hindi	Hindi 1081
1082	Maltese	Maltese 1082
1084	GaelicScots	Gaelic (Scots) 1084
1085	Yiddish	Yiddish 1085
1086	MalayMalaysia	Malay_Malaysia 1086
1087	Kazakh	Kazakh 1087
1088	Kyrgyz	Kyrgyz 1088
1089	Swahili	Swahili 1089
1091	UzbekLatin	Uzbek_Latin 1091
1092	Tatar	Tatar 1092
1094	Punjabi	Punjabi 1094
1095	Gujarati	Gujarati 1095
1097	Tamil	Tamil 1097
1098	Telugu	Telugu 1098
1099	Kannada	Kannada 1099

**Table 3** Valid Language Codes for Bulk Import (continued)

Language Code	Name	Description
1102	Marathi	Marathi 1102
1103	Sanskrit	Sanskrit 1103
1104	Mongolian	Mongolian 1104
1110	Galician	Galician 1110
1111	Konkani	Konkani 1111
1114	Syriac	Syriac 1114
1125	Divehi	Divehi 1125
11265	ArabicJordan	Arabic_Jordan 11265
11273	EnglishTrinidad	English_Trinidad 11273
11274	SpanishArgentina	Spanish_Argentina 11274
12289	ArabicLebanon	Arabic_Lebanon 12289
12297	EnglishZimbabwe	English_Zimbabwe 12297
12298	SpanishEcuador	Spanish_Ecuador 12298
13313	ArabicKuwait	Arabic_Kuwait 13313
13321	EnglishPhilippines	English_Philippines 13321
13322	SpanishChile	Spanish_Chile 13322
14337	ArabicUAE	Arabic_UAE 14337
14346	SpanishUruguay	Spanish_Uruguay 14346
15361	ArabicBahrain	Arabic_Bahrain 15361
15370	SpanishParaguay	Spanish_Paraguay 15370
16385	ArabicQatar	Arabic_Qatar 16385
16394	SpanishBolivia	Spanish_Bolivia 16394
17418	SpanishElSalvador	Spanish_El_Salvador 17418
18442	SpanishHonduras	Spanish_Honduras 18442
19466	SpanishNicaragua	Spanish_Nicaragua 19466
2049	ArabicIraq	Arabic_Iraq 2049
20490	SpanishPuertoRico	Spanish_Puerto_Rico 20490
2052	ChinesePRC	Chinese_PRC 2052
2055	GermanSwiss	German_Swiss 2055
2057	EnglishUnitedKingdom	English_United_Kingdom 2057
2058	SpanishMexican	Spanish_Mexican 2058
2060	FrenchBelgian	French_Belgian 2060
2064	ItalianSwiss	Italian_Swiss 2064
2067	DutchBelgian	Dutch_Belgian 2067
2068	NoewegianNynorsk	Norwegian_Nynorsk 2068
2070	PortugeseStandard	Portuguese_Standard 2070

**Table 3** Valid Language Codes for Bulk Import (continued)

Language Code	Name	Description
2072	RomanianMoldavia	Romanian (Moldavia) 2072
2073	RussianMoldavia	Russian (Moldavia) 2073
2074	SerbianLatin	Serbian_Latin 2074
2077	SwedishFinland	Swedish_Finland 2077
2092	AzeriCyrillic	Azeri_Cyrillic 2092
2110	MalayBruneiDarussalam	Malay_Brunei_Darussalam 2110
2115	UzbekCyrillic	Uzbek_Cyrillic 2115
3073	ArabicEgypt	Arabic_Egypt 3073
3076	ChineseHongKong	Chinese_Hong_Kong 3076
3079	GermanAustrian	German_Austrian 3079
3081	EnglishAustralian	English_Australian 3081
3082	SpanishModernSort	Spanish_Modern_Sort 3082
3084	FrenchCandian	French_Canadian 3084
3098	SerbianCyrillic	Serbian_Cyrillic 3098
4097	ArabicLibya	Arabic_Libya 4097
4100	ChineseSingapore	Chinese_Singapore 4100
4103	GermanLuxembourg	German_Luxembourg 4103
4105	EnglishCandian	English_Canadian 4105
4106	SpanishGuatemala	Spanish_Guatemala 4106
4108	FrenchSwiss	French_Swiss 4108
5121	ArabicAlgeria	Arabic_Algeria 5121
5124	ChineseMacau	Chinese_Macau 5124
5127	GermanLiechtenstein	German_Liechtenstein 5127
5129	EnglishNewZealand	English_New_Zealand 5129
5130	SpanishCostaRica	Spanish_Costa_Rica 5130
5132	FrenchLuxembourg	French_Luxembourg 5132
6145	ArabicMorocco	Arabic_Morocco 6145
6153	EnglishIreland	English_Ireland 6153
6154	SpanishPanama	Spanish_Panama 6154
6156	FrenchMonaco	French_Monaco 6156
7169	ArabicTunisia	Arabic_Tunisia 7169
7177	EnglishSouthAfrica	English_South_Africa 7177
7178	SpanishDominicanRepublic	Spanish_Dominican_Republic 7178
8193	ArabicOman	Arabic_Oman 8193
8201	EnglishJamaica	English_Jamaica 8201
8202	SpanishVenezuela	Spanish_Venezuela 8202

**Table 3** Valid Language Codes for Bulk Import (continued)

Language Code	Name	Description
9217	ArabicYemen	Arabic_Yemen 9217
9225	EnglishCaribbean	English_Caribbean 9225
9226	SpanishColumbia	Spanish_Colombia 9226

## Examples

The following examples show how user configuration settings are used for bulk operation with the Cisco Unity Connection 1.2(1) plug-in. The column headers for CSV file are **bold** and the values are in plain font.

### Create a Simple User

This example shows how a user is added by using a CSV file:

```
vpt_productSystems, vpt_user_userID, vpt_user_firstName, vpt_user_lastName,
unity_user_template, unity_user_displayName, unity_user_initials, unity_user_title,
unity_user_employeeId, unity_user_extension
usa-cuc3, johndoe, John, Doe, Voice Mail User Template, John Doe, PM, SW Eng, 946355000,
5000
```

### Add User MWI

This example shows how a simple MWI can be added to a user:

```
vpt_productSystems, vpt_user_userID, unity_mwi_displayName, unity_mwi_enabled,
unity_mwi_extension, unity_mwi_phoneSystem
usa-cuc3, jdoe, MWI-2, true,
500002, usa-cuc-ccm1
```

### Update User MWI

This example shows how an MWI can be changed. The `unity_mwi_originalExtension` is used to specify which MWI we want to change. This is how we can change the `unity_mwi_extension`.

```
vpt_productSystems, vpt_user_userID, unity_mwi_originalExtension,
unity_mwi_displayName, unity_mwi_enabled, unity_mwi_extension, unity_mwi_phoneSystem
usa-cuc3, jdoe, 500002, MWI-2, false, 5002,
usa-cuc-ccm
```

### Delete User MWI

This example shows how an MWI can be deleted. The MWI to be deleted is indicated by `unity_mwi_originalExtension` and the “vpt\_clear” is set in the `unity_mwi_extension` column.

```
vpt_productSystems, vpt_user_userID, unity_mwi_originalExtension, unity_mwi_extension
usa-cuc3, jdoe, 5002, vpt_clear
```

### Add User Phone Number

This example shows how three phone numbers can be added to a user:

```
vpt_productSystems, vpt_user_userID, unity_phoneNumber_phoneType,
unity_phoneNumber_phoneNumber, unity_phoneNumber_displayName
usa-cuc3, jdoe, 2;3;4,2001;3001;4001, pn1;pn2;pn3
```

### Add and Update User Phone Number

Here is a more complex example which adds the following phone number:

Extension: 10011

Display Name: pn1

Phone Type: 1 (Work Phone)

This example updates the phone type, extension, and display name of the three others (pn[2-4]). Note that the `unity_phoneNumber_originalPhoneType` is used to specify which phone number we want to change and it starts by the separator “;” because the first phone number is to be added.

```
vpt_productSystems, vpt_user_userID, unity_phoneNumber_originalPhoneType,
unity_phoneNumber_phoneType, unity_phoneNumber_phoneNumber,
unity_phoneNumber_displayName
usa-cuc3, jdoe, ;2;3;4, 1,
10011;20011;30011;40011, pn1;pn2;pn3;pn4
```

### Delete User Phone Number

Here is an example showing how to delete two phone numbers:

```
vpt_productSystems, vpt_user_userID, unity_phoneNumber_originalPhoneType,
unity_phoneNumber_phoneType
usa-cuc3, jdoe, 2;4,vpt_clear;vpt_clear
```

## Related Documentation

See the following documents for more information on the Cisco Voice Provisioning Tool and Cisco Unity Connection:

- 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](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](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](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](http://www.cisco.com/en/US/products/ps6524/prod_maintenance_guides_list.html).
- Cisco Unity Connection Documentation Guide*

Provides a list of Cisco Unity Connection documents that are available with the release (for example, the 1.0(2) 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/ps6509/products\\_documentation\\_roadmaps\\_list.html](http://www.cisco.com/en/US/products/ps6509/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](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](mailto: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](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](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](mailto: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](mailto: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](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.

