

User and Administrator Access

This chapter contains the following sections:

- Cisco Unity Connection Does Not Respond to Touchtones, page 6-1
- Cisco Personal Communications Assistant Pages Are Incomplete or Blank, page 6-2
- Users Cannot Access Cisco Personal Communications Assistant Pages, page 6-2
- Users Cannot Access the Cisco Unity Assistant, Cisco Unity Inbox, or Cisco Unity Personal Call Transfer Rules from the Cisco PCA, page 6-3
- Users Cannot Save Changes on Pages in the Cisco Unity Assistant, Cisco Unity Inbox, or the Cisco Unity Personal Call Transfer Rules, page 6-4
- Voice Mail Users Cannot Be Located in a Directory Handler, page 6-4

Cisco Unity Connection Does Not Respond to Touchtones

When Cisco Unity Connection is integrated by SCCP to Cisco Unified CallManager, Cisco Unity Connection may not respond to touchtones.

In certain situations, DTMF digits are not recognized when processed through VoIP dial-peer gateways. To avoid this problem, certain gateways must be configured to enable DTMF relay. The DTMF relay feature is available in Cisco IOS software version 12.0(5) and later.

Cisco IOS software-based gateways that use H.245 out-of-band signaling must be configured to enable DTMF relay.

The Catalyst 6000 T1/PRI and FXS gateways enable DTMF relay by default and do not need additional configuration to enable this feature.

To Enable DTMF Relay

Step 1 On a VoIP dial-peer servicing Connection, use the following command:

dtmf-relay h245-alphanumeric

- **Step 2** Create a destination pattern that matches the Cisco Unified CallManager voice mail port numbers. For example, if the system has voice mail ports 1001 through 1016, enter the dial-peer destination pattern 10xx.
- **Step 3** Repeat Step 1 and Step 2 for all remaining VoIP dial-peers servicing Connection.

Cisco Personal Communications Assistant Pages Are Incomplete or Blank

An incomplete Cisco Personal Communications Assistant page may be empty or partially empty because of an error in the processing of the dynamic elements contained in the page. Such errors can be caused by one or more of the following:

- An error in the data collection processing for the requested page (server side)
- An error in the data rendering processing of the requested page (server side)
- An error in the processing of the dynamic scripting in the page (client side)

To correct the problem, you will need to reinstall the Cisco Unity Connection system. See the *Cisco Unity Connection Installation Guide* for procedures and information. The guide is available at http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html.

Before you attempt to reinstall Cisco Unity Connection, gather the data that you may need to provide to Cisco TAC in the event that reinstalling Connection does not resolve the problem. Do the following:

- To assist in diagnosing data processing errors on the server side, collect the log files for Cisco PCA that cover the time when the issue occurred. The file names for these files start with "ciscopca_" and can be found in the "%CU_HOME%\logs" folder.
- To assist in diagnosing errors in the processing of the dynamic scripting in the page on the client side, try to collect a screen capture of the browser that shows the issue, and a text file containing the source code for the incomplete or blank page (however, note that if the Cisco PCA uses an SSL connection, you may not be able to save the source code).

If you are confident the issue resides on the server side, collecting the client information will still help Cisco TAC to determine the exact issue and provide a solution or workaround faster.

If the problem is that the Media Master control bar does not show up correctly or at all, see the "Media Master" chapter.

Users Cannot Access Cisco Personal Communications Assistant Pages

Users use the Cisco PCA website to access the Cisco Unity Assistant, the Cisco Unity Inbox, and the Cisco Unity Personal Call Transfer Rules pages.

When a user cannot access the Cisco Personal Communications Assistant pages, consider the following possible causes. Additional troubleshooting information and procedures are available in the "Cisco Personal Communications Assistant" chapter.

URL Is Case-Sensitive

Users can access the Cisco PCA at the following URL: http://<Cisco Unity Connection server>/ciscopca. Note, however, that the URL is case-sensitive.

Incorrect Browser or Client Configuration

When a user cannot access any of the Cisco PCA pages, it may be that the user browser or client workstation is not configured properly. Make sure that the browser and client workstation are configured as specified in the *Cisco Unity Connection User Setup Guide*. (The guide is available at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.)

Unsupported Software Is Installed on Client Workstation

Confirm that the user does not have an unsupported combination of software or an unsupported third-party application installed on the workstation. See the *Compatibility Matrix: Cisco Unity Connection and the Software on User Workstations*, available at http://www.cisco.com/en/US/products/ps6509/products_device_support_tables_list.html.

Cisco Unity Connection Uses SSL but the Certificate Has Not Been Distributed to the Trusted Root Store

If you installed an SSL certificate on the Cisco Unity Connection server to secure Cisco PCA access to Connection, you probably will also want to add the certificate to the Trusted Root Store on user workstations. If you do not install the certificate on user workstations, users can use Cisco PCA, but the web browser will display a message to alert the user that the authenticity of the site cannot be verified, and therefore its content cannot be trusted. Connection may also display this warning message if the URL used to connect to the Connection server is different from the hostname of the server at the time the Connection software was installed.

If you installed an SSL certificate to secure IMAP e-mail client access to Connection, you may need to add the certificate to the Trusted Root Store on user workstations. Some of the IMAP e-mail clients supported for use with Connection display SSL security messages, while others do not.

For situations where the client computer is running Windows Server 2003 and a user is using Internet Explorer 6.0 to access the Cisco Personal Communications Assistant, provide the user with the following "To Add the Cisco Unity Connection Server to the List of Trusted Sites for Internet Explorer 2003" procedure to add the Cisco Unity Connection server to the list of Trusted Sites. These additional configuration steps must be performed for these user workstations in order for the Cisco PCA to work correctly.

To Add the Cisco Unity Connection Server to the List of Trusted Sites for Internet Explorer 2003

Step 1	Open the Cisco Personal Communications Assistant Login page. It is not necessary to log in to the Cisco PCA.
Step 2	On the Internet Explorer File menu, click Add This Site To > Trusted Sites Zone.
Step 3	In the Trusted Sites dialog box, click Add.
Step 4	Click Close to close the Trusted Sites dialog box.

Step 5 Restart Internet Explorer.

Users Cannot Access the Cisco Unity Assistant, Cisco Unity Inbox, or Cisco Unity Personal Call Transfer Rules from the Cisco PCA

When users can access the Cisco PCA, but cannot access the Cisco Unity Assistant, the Cisco Unity Inbox, or the Cisco Unity Personal Call Transfer Rules, consider the following possible causes:

• In order to access the Cisco Unity Assistant, users must be given the proper class of service rights on the Class of Service > Edit Class of Service page or the Class of Service > New Class of Service page in Cisco Unity Connection Administration. The class of service must have the "Allow Users to Use the Cisco Unity Assistant" setting enabled.

- The Cisco Unity Inbox is a licensed feature, and can be accessed only if it is purchased. In addition, users must be given the proper class of service rights on the Class of Service > Edit Class of Service page or the Class of Service > New Class of Service page in Cisco Unity Connection Administration. The class of service must have the "Allow Users to Use the Cisco Unity Inbox" setting enabled.
- In order to access the Cisco Unity Personal Call Transfer Rules, users must be given the proper class of service rights on the Class of Service > Edit Class of Service page or the Class of Service > New Class of Service page in Cisco Unity Connection Administration. The class of service must have the "Allow Users to Use the Cisco Unity Personal Call Transfer Rules" setting enabled.

Users Cannot Save Changes on Pages in the Cisco Unity Assistant, Cisco Unity Inbox, or the Cisco Unity Personal Call Transfer Rules

When user browser settings are set to cache temporary Internet pages automatically, users can create a bookmark or Favorite to access a Cisco Unity Assistant, Cisco Unity Inbox, or Cisco Unity Personal Call Transfer Rules web page, but the page will be read-only. Explain to users that they should bookmark the Cisco PCA home page, rather than individual pages. (Users should not change their browser settings as a workaround; when the browser is not set to automatically check for newer versions of temporary Internet files, the Media Master control is not displayed correctly.)

Voice Mail Users Cannot Be Located in a Directory Handler

Callers may report that they are unable to locate one or more users in a directory handler.

For users to be located in a directory handler, they must have a recorded name, and must be configured to be listed in the directory.

Verify the List in Directory setting on the Edit User Basics page for the user in Cisco Unity Connection Administration.