CHAPTER 11

User and Administrator Access

See the following sections for information on problems that can occur when users and administrators access Cisco Unity Connection:

Cisco Unity Connection Does Not Respond to Touchtones

When Cisco Unity Connection is integrated by SCCP to Cisco Unified Communications Manager, 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 Cisco Unity Connection, use the following command:

dtmf-relay h245-alphanumeric

Step 2 Create a destination pattern that matches the Cisco Unified CM 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.

Users Do Not Hear Login Prompt When Calling Cisco Unity Connection

When a user calls Cisco Unity Connection directly and unexpectedly hears the Opening Greeting or another prompt rather than the login prompt, the problem can be caused by either of the following:

- The call matched a direct call routing rule other than the Attempt Sign-In rule, and the rule directed the call to a destination other than the Attempt Sign-In conversation.
- The calling extension is not found in the search scope set by the call routing rule that sent the call to the Attempt Sign-In conversation.

Connection uses the search scope of the call when it reaches the Attempt Sign-In conversation to identify which user is attempting to log on. If the user extension is in a partition that is not a member of the search space that is assigned as the search scope of the call by the routing rule, Connection routes the call to the Opening Greeting.

To resolve this problem, in Cisco Unity Connection Administration, check the direct call routing rules to determine which rule is processing the call and to check the search scope that is set by the rule. You can also enable the Arbiter micro trace (levels 14, 15, and 16 call routing), the RoutingRules micro trace (level 11 rules creation/deletion/evaluation) and the CDE micro trace (level 4 search space). (For detailed instructions on turning on traces and collecting logs, see the "Diagnostic Traces" chapter.

See also the "Users Hear the Opening Greeting Instead of the Password Prompt When Attempting to Log On" section on page 16-7.

Users Cannot Access Cisco Personal Communications Assistant Pages

Users use the Cisco Personal Communications Assistant (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 PCA pages, consider the following possible causes.

- **The Cisco PCA 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.
- **The browser or client configuration is not configured properly**—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 *User Workstation Setup Guide for Cisco Unity Connection Release 7.x*. The guide is available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/user_setup/guide/7xcucusx.html .
- **Unsupported software is installed on the 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/docs/voice_ip_comm/connection/compatibility/matrix/cucclientmtx.html.

Additional troubleshooting information and procedures for the Cisco PCA are available in the "Cisco Personal Communications Assistant (PCA)" chapter.

Security Alert Displayed When Users Access Cisco Personal Communications Assistant Pages

If you use the self-signed certificate generated during installation to provide an SSL connection to the Cisco PCA, the web browser of the user displays a message to alert the user that the authenticity of the site cannot be verified, and therefore its content cannot be trusted. Similarly, if you use a self-signed SSL certificate to secure IMAP email client access to Connection, some email clients supported for use with Connection display SSL security messages.

Although users can still access Connection despite the alerts, consider one of the following options to manage or eliminate security alerts when users browse to Cisco PCA and/or access their messages from an IMAP email client:

- Add the SSL certificate to the Trusted Root Store on each user workstation. In this way, you can ensure that users never see the security alert. See the following "To Add the SSL Certificate to the Trusted Root Store on User Workstations" procedure.
- Tell users to choose the "Accept Permanently" (or similar) option when the browser or email client displays the alert and asks them how to proceed. After instructing the browser and/or email client to always accept the certificate, the user will not see the alert again.

Do the following procedure if you want users to never see the security alert.

To Add the SSL Certificate to the Trusted Root Store on User Workstations

Step 1 From the OS Administration application on the Cisco Unity Connection server, right-click to download the certificate and save it as a file.

Step 2 Copy the certificate to each user workstation, and then import it by using tools in the browser or IMAP client, as applicable.

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

Revised May 2009

When users can access the Cisco Personal Communications Assistant (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 that the user is assigned to 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 that the user is assigned to must have the "Allow Users to Use the Cisco Unity Inbox and RSS Feeds" 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 that the user is assigned to must have the "Allow Users to Use 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. However, the page is read-only. Explain to users that they should bookmark the Cisco PCA home page rather than individual pages. Also note that 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.