Setting Up Features and Functionality That Are Controlled by Class of Service

In Cisco Unity Connection, some features are controlled by class of service (COS), including features for which you need user licenses. A COS is specified in each user template; thus, a user is assigned to the COS that is specified in the template upon which the user account is based. You can reassign a user to a different COS at any time.

Note When a COS includes access to a feature that requires individual licenses, you can assign groups of users to the COS only if enough licenses are available.

See the following sections for information and procedures for setting up features that are controlled by class of service:

- Personal Call Transfer Rules, page 4-1
- Text to Speech Access to Exchange E-Mail, page 4-4
- Voice Recognition Features, page 4-5
- IMAP Client Access to Voice Messages, page 4-6
- Private Distribution Lists, page 4-7

Personal Call Transfer Rules

Personal Call Transfer Rules let Connection users create call transfer rules that forward and screen incoming calls according to any or all of the following criteria:

- identity of caller
- time of day
- meeting schedule

Connection users can specify that calls are forwarded to voice mail, to another phone number, or to a series of destinations (which must include at least one phone number and which can include SMS and SMTP notification devices).

With Personal Call Transfer Rules enabled, users are able to transfer both direct and indirect calls. Call holding and screening options also apply to both direct and indirect calls. Call holding is applied only on calls to the primary extension if a personal call transfer rule is applied; the call screening option will be applied only if it is selected for the rule.

The Personal Call Transfer Rules web tool offers the following additional features to Connection users:

Personal contacts list	Connection users can set up a directory of personal contacts, which supplements the information in the Connection directory. Connection uses the personal contacts list to forward incoming calls, and also to place outgoing calls when the Connection user uses the user speech recognition conversation.
Caller groups	Connection users can organize callers into groups, so that they can apply one rule to multiple callers without having to recreate the rule multiple times. Caller groups can contain other Connection users, system contacts, or personal contacts.
Personal destinations	In addition to notification devices, Connection users can create a directory of contact phone numbers to which Connection can direct incoming calls, according to rules that users set up.
Destination groups	Connection users can create groups of personal destinations and notification devices. When transferring a call to a destination group, Connection forwards the call to each destination in the group in the order listed until the phone is answered, the caller hangs up, or the last destination in the group is reached. Connection users can specify the ordering of destinations in the series, and the number of rings that Connection waits for the phone to be answered at each destination.
Call transfer rule tester	The call transfer rule tester lets users and administrators see how Connection would forward an incoming call based on an actual rule.
Transfer All rule	The Transfer All rule is a single rule that forwards all calls to a specific destination for a specified time. This rule can be created and activated only by phone.
Forward all calls to Cisco Unity Connection	Connection users can forward all calls to Cisco Unity Connection in order to automatically apply personal call transfer rules to incoming calls, rather than having the call ring the primary extension.

To create Personal Call Transfer Rules, users with voice mailboxes must belong to a class of service with this feature enabled. For information on how to change this class of service setting, see the "Enabling and Disabling Personal Call Transfer Rules For Users" section on page 4-3.

Users can create Personal Call Transfer Rules by using the Cisco Unity Personal Call Transfer Rules web tool. This feature is supported only when the Cisco Unity Connection system is integrated with Cisco Unified CallManager or Cisco Unified CallManager Express.

Optionally, you can configure Connection so that users can base Personal Call Transfer Rules on Exchange calendar and contact data. For more information, see the "Creating Cisco Unity Connection External Service Accounts to Allow Access to Microsoft Exchange Calendars and Contacts" section on page 4-3.

Caution Depending on your license settings, personal call transfer rules may not be available.

It is important to note that if Connection users have Personal Call Transfer Rules, call screening, and call holding options enabled for their class of service, the call holding and call screening options in the Cisco Personal Communications Assistant appear in the Cisco Unity Personal Call Transfer Rules web tool, not the Cisco Unity Assistant. Similarly, in order for an administrator to modify the call transfer

options for a user, instead of going to the Transfer Options page in Cisco Unity Connection Administration, go to the Call Transfer Rules page, which will launch the Personal Call Transfer Rules web tool for the user.

Enabling and Disabling Personal Call Transfer Rules For Users

To enable or disable Personal Call Transfer Rules, modify the Personal Call Transfer Rules Feature COS setting.

To Enable or Disable Personal Call Transfer Rules for Users

Step 1 In Cisco Unity Connection Administration, expand **Class of Service**, then click **Class of Service**.

Step 2 On the Search Class of Service page, under Class of Service Search Results, click the applicable class of service.

Note If the applicable class of service does not appear in the search results table, set parameters in the search fields at the top of the page, and click **Find**.

Step 3 On the Edit Class of Service page, under Features, do one of the following:

- To enable Personal Call Transfer Rules, check the **Allow Users to Use Personal Call Transfer Rules** check box.
- To disable Personal Call Transfer Rules, uncheck the **Allow Users to Use Personal Call Transfer Rules** check box.

Step 4 Click **Save**.

Creating Cisco Unity Connection External Service Accounts to Allow Access to Microsoft Exchange Calendars and Contacts

When users belong to a COS that has access to the Cisco Unity Personal Call Transfer Rules feature, you can configure Cisco Unity Connection to access Exchange calendar information for a user, and to enable users to import their Exchange contacts. This allows users to create Personal Call Transfer Rules based on their Exchange calendar and contacts.

To enable this feature, you create a Connection external service account for each user who you want to have access to Exchange data. The external service account specifies the Exchange server on which the mailbox for the user is stored.

Before doing the "To Create Connection External Service Accounts to Access Microsoft Exchange Calendars and Contacts" procedure, you first need to configure Connection and Microsoft Exchange as described in the *Cisco Unity Connection Installation Guide* (available at http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html).

Microsoft Exchange Calendar

Connection accesses the Exchange calendar of a user to determine whether or not the user is in a meeting.

If the user creates a rule to forward calls when he or she is in a meeting, Connection applies the rule if the Show Time As setting for the meeting is set to "Busy." Meetings marked "Out of Office," "Tentative," or "Free" are not considered by Connection when evaluating the rule.

Note Schedule information is updated every 30 minutes, so new meetings may not be considered by Connection immediately.

Microsoft Exchange Contacts

Connection users can import their Exchange contacts into their Connection personal contacts list. Connection imports names, phone numbers, and e-mail addresses of the contacts stored on the Exchange server.

To Create Connection External Service Accounts to Access Microsoft Exchange Calendars and Contacts

Step 1 In Cisco Unity Connection Administration, click **Users**.

Step 2 On the Search Users page, in the Search Results table, click the alias of the applicable user.

Note If the user does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and click **Find**.

Step 3 On the Edit User Basics page, on the Edit menu, click **External Service Accounts**.

Step 4 On the External Service Accounts page, click **Add New**.

Step 5 In the Account Login field, enter the Active Directory user logon name for the user.

Step 6 In the Service Type list, select **WebDav**.

Step 7 In the Remote Server list, select the name of the WebDav service.

Step 8 In the Server URL Suffix field, enter the Exchange account logon name for the user.

Step 9 Click **Save**.

Text to Speech Access to Exchange E-Mail

You can configure Exchange and Cisco Unity Connection so that users can use Text to Speech (TTS) to listen to Exchange e-mails over the phone. To enable this feature for users, you must have the appropriate license, and you must modify class of service settings.

Connection uses the IMAP protocol to access e-mail messages in Exchange so that messages can be played via TTS. By default, Exchange is not configured to allow IMAP access to messages.

When the Message Type menu is enabled, Connection announces the number of new e-mail messages after the user logs on. See the "Enabling the Message Type Menu" section on page 3-16 for instructions on enabling this menu.

Note that users can turn this feature on and off from the Cisco Unity Assistant.

To enable users to use the TTS feature to read their Exchange e-mail, do the following procedures in the order presented.

To Enable TTS in a Class of Service

Step 1 In Cisco Unity Connection Administration, expand **Class of Service**, then click **Class of Service**.

Step 2 On the Search Class of Service page, in the Search Results table, click the display name of the applicable class of service.

Note If the class of service does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and click **Find**.

Step 3 On the Edit Class of Service page, under Licensed Features, check the **Allow Users to Access Voice Recognition or Text to Speech for E-Mail** check box.

Step 4 Under Features, check the **Allow Users to Use Text to Speech to Read E-Mail** check box.

Step 5 Click **Save**.

Step 6 Repeat Step 2 through Step 5 for each class of service for which you want to enable TTS.

To Enable TTS for a Cisco Unity Connection User

Step 1 In Cisco Unity Connection Administration, click **Users**.

Step 2 On the Search Users page, in the Search Results table, click the alias of the applicable user.

Note If the user does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and click **Find**.

Step 3 On the Edit User Basics page, on the Edit menu, click **External Service Accounts**.

Step 4 Click **Add New**.

Step 5 On the New External Service Account page, in the Account Login field, enter the Active Directory account alias that is associated with the Exchange mailbox that you want this Cisco Unity Connection user to be able to access.

Step 6 In the Message Store Type field, click **IMAP**.

Step 7 In the Remote Server field, click the name of the external service that is associated with the Exchange server on which the Exchange mailbox of this user is homed.

Step 8 Click **Save**.

Step 9 Repeat Step 3 through Step 8 for each user for whom you want to enable TTS.

Voice Recognition Features

Access to voice recognition features allows users to interact with Cisco Unity Connection by speaking commands rather than by using touchtone keys on the phone. To enable this conversation for users, you must have the appropriate license and must modify class of service settings.

Note that once enabled for voice recognition, users can turn this feature on and off from the Cisco Unity Assistant.

To Enable the Voice Recognition Conversation

Step 1 In Cisco Unity Connection Administration, expand **Class of Service**, then click **Class of Service**.

Step 2 On the Search Class of Service page, in the Search Results table, click the display name of the applicable class of service.

Note If the class of service does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and click **Find**.

Step 3 On the Edit Class of Service page, under Licensed Features, check the **Allow Users to Access Voice Recognition or Text to Speech for E-Mail** check box.

Step 4 Under Features, check the **Allow Users to Use Voice Recognition** check box.

Step 5 Click **Save**.

To set the voice recognition conversation for a user, see the "To Set the Conversation Version" procedure on page 3-13.

IMAP Client Access to Voice Messages

Use the following procedure to enable IMAP client access to voice messages for users associated with a class of service.

Note that regardless of what you do here to enable IMAP client access, users will have full access to messages by using the Cisco Unity Connection phone conversation and, if applicable, the Cisco Unity Inbox.

Note Users are unable to send, forward, or reply to voice messages from their IMAP client application. Encrypted message bodies can never be accessed from an IMAP client.

See the *Cisco Unity Connection User Setup Guide* for steps on setting up IMAP client software on user workstations. The guide is available at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

To Enable IMAP Client Access to Voice Messages in Applicable Classes of Service

Step 1 In Cisco Unity Connection Administration, expand **Class of Service**, then click **Class of Service**.

Step 2 On the Search Class of Service page, in the Search Results table, click the display name of the applicable class of service.

Note If the class of service does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and click **Find**.

Step 3 On the Edit Class of Service page, under Licensed Features, check the **Allow Users to Access Voice Mail Using an IMAP Client** check box.

Step 4 Choose one of the following options:

- Allow Users to Access Message Bodies—Users have access to the entire voice mail.
- Allow Users to Access Message Bodies Except on Private Messages—Users have access to the entire voice mail, unless the message is marked private, in which case they will have access only to the message header.
- Allow Users to Access Message Headers Only—Users have access only to message headers.

Step 5 Click **Save**.

Step 6 Repeat Step 2 through Step 5 for each class of service for which you want to enable voice mail access from the IMAP client.

Private Distribution Lists

Private distribution lists, like system distribution lists, are used to send voice messages to more than one user at a time. You can set up private lists for a user in Cisco Unity Connection Administration, although the user is the only person who can send voice messages to the list.

Users can manage their private lists by using the Cisco Unity Assistant or the phone. Refer users to the "Changing Private List Settings" chapter of the *Cisco Unity Connection User Guide* for details. The guide is available at http://www.cisco.com/en/US/products/ps6509/products_user_guide_list.html.

On the Class of Service page, under Private Distribution Lists, you specify the maximum number of lists available to users and the maximum number of members that users can add to each list when they use the Connection conversation or the Cisco Unity Assistant to manage their lists.

Maximum Number of Lists Per User

On the class of service page, you can set the maximum number of lists allowed to each user who is associated with the COS, up to 99 private lists per user.

Note that although both the Cisco Unity Connection conversation and the Cisco Unity Assistant use this COS setting to determine when a user has reached the maximum number of lists, each application calculates differently the number of lists that a user owns:

- When a user uses the phone to create a new list by adding members, the Cisco Unity Connection conversation counts the number of private lists that have members, and then compares the total to the value in this setting to determine whether the user has reached the list limit. Lists with no members (empty lists) are not included in the total number of lists that a user owns, even if the lists have recorded names or text names.
- When a user uses the Cisco Unity Assistant to create a new list, the Cisco Unity Assistant counts the number of lists that have a recorded voice name, a text name, or members, and then compares the total to the value in this setting to determine whether the user has reached the list limit. Lists with no members are included in the total number as long as they have recorded names or text names.

This means that if a user belongs to a COS that allows 15 lists, and the user has 12 private lists with members and two lists with recorded names but no members, the user can potentially create more lists by phone than in the Cisco Unity Assistant before reaching the list limit:

- When the user uses the Cisco Unity Connection conversation, the user will reach the list limit either by adding members to the two empty lists and creating one new list, or by creating three new lists. If the user reaches the limit by creating three new lists, the user cannot add members to the two empty lists until two lists are deleted.
- When the user uses the Cisco Unity Assistant, the user will reach the list limit by creating one new list. Despite reaching the list limit, the user can add members to the two empty lists.

Maximum Number of Members Per List

On the class of service page, you also specify the maximum number of members that users can add to a private list, up to a maximum of 999 members.