User Settings

Settings for User Accounts and User Templates

You can specify different settings, such as password and transfer rules associated with a user template or a particular user account through Cisco Unity Connection Administration interface. For information on user accounts, see the Users chapter and for information on user templates, see the User Templates section.

User Template Basics

The Edit User Template Basics page allows you to specify the settings, such as alias and first name associated with a particular user template.

User Basics

The Edit User Basics page allows you specify the settings, such as alias and first name associated with a particular user account.

Consider the following points while changing the alias of a user:

- If you change the alias for a user, Unity Connection automatically creates an SMTP proxy address for the previous alias. This allows the other Unity Connection users to reply to the messages that were sent from the previous alias but the replies automatically reach to the new alias of the user.
- When Unity Connection is integrated with an LDAP directory, the Alias field cannot be changed for any user who is integrated with an LDAP user. However, if you are using Active Directory as the LDAP directory, you can change the value of the LDAP field that is mapped to the Alias field. The alias change is replicated to Unity Connection when the Unity Connection database is synchronized with the LDAP directory. This also causes Unity Connection to automatically create an SMTP proxy address for the previous alias.

Caution If you are using an LDAP directory other than Active Directory and you change the value of the LDAP field that is mapped to the Alias field, the user is converted to a non-LDAP-integrated user.

In the following configurations, you cannot edit fields, such as Alias (User ID in Cisco Unified Communications Manager Administration), and First Name:

- In Cisco Business Edition, when the Unity Connection user is integrated with the Cisco Unified CM Application User. You can only edit these fields in Cisco Unified CM Administration.
- In Unity Connection or in Cisco Business Edition, when Unity Connection user data is synchronized with data in an LDAP directory. You can only edit these fields in the LDAP directory.

Note If Unity Connection is configured to authenticate Unity Connection web application user names and passwords against the LDAP directory, you cannot change the Unity Connection web application password.

- In Unity Connection, if digital networking is configured, you cannot edit any fields for a user on servers other than the home server of the user. You must edit user settings on the server on which the user account was created.

  For information on moving mailboxes from one mailbox store to another, see the LDAP chapter.

Password Settings

Default phone PINs and web application passwords are applied to each user account that you create. The web application password and voicemail PIN settings for individual users determine:

- The authentication rule that governs the user account.
- The time of password or PIN lockout if the user password or PIN is locked by an administrator.
- The password changing settings of a user, whether user is allowed to change the password or the password must be changed during next sign in.
- The expiry of a password or PIN.
- The last time a password or PIN was changed.
- The number of failed sign-in attempts, the time of the last failed sign-in attempt, and the time period that the lockout is enforced.

Securing and Changing User Phone PINs

To help protect Unity Connection from unauthorized access and toll fraud, every user should be assigned a unique phone PIN. Additionally, each PIN should be six or more characters long and non-trivial.

Note To assign unique PINs to Unity Connection end user accounts (users with mailboxes) after they have been created, use the Bulk Password Edit tool along with a CSV file that contains unique strings for the PINs to apply PINs in bulk. The Bulk Password Edit tool is a Windows-based tool. Download the tool and view Help at http://www.ciscounitytools.com/applications/cxn/bulkpasswordedit/bulkpasswordedit.html.

PIN Synchronization between Unity Connection and Cisco Unified CM

PIN Synchronization feature in Unity connection allows the administrator to configure Unity Connection to maintain the common PIN for the users to access the Cisco Unity Connection Voicemail, Extension Mobility, Conference Now and Mobile Connect. Using this feature, when a user updates the voicemail PIN for Unity Connection, the PIN automatically gets synchronized with the corresponding user account on Cisco Unified CM and vice versa. PIN Synchronization is supported only with Cisco Unified CM 11.5(1) and later.

To enable this feature, check the **Enable End User PIN Synchronization for Primary AXL Server** check box on the Edit AXL Servers page of Cisco Unity Connection Administration.

For field information, see **Help > This Page**.

Before using PIN Synchronization feature, ensure the following:

- The alias of the user on Cisco Unity Connection must be same as the user ID on the Cisco Unified CM or the users should be integrated with Cisco Unified CM through AXL server or LDAP.
- Authentication Rules on Cisco Unity Connection must be same as the Credential Policies on Cisco Unified CM to reduce possible error conditions.

  For more information on authentication rules, see "Passwords, PINs, and Authentication Rule Management" chapter in the *Security Guide for Cisco Unity Connection Release 11.x* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/security/b_11xcucsecx.html. .

Note For successful synchronization of the PIN, make sure that publisher server of Cisco Unified CM is up and running.

Task List for Configuring PIN Synchronization in Unity Connection

Do the following to configure PIN Synchronization feature in Unity Connection:

- In Cisco Unity Connection Administration, go to **Telephony Integrations** > **Phone System** and select the Phone system associated with the user. On the Phone System Basics page go to **Edit** > **Cisco Unified Communication Manager AXL Servers**. On the Edit AXL server page, configure the primary AXL server with valid username and password. The feature is not applicable for secondary AXL server.

  For more information on how to configure the AXL server, see the "Configuring an AXL Server in Unity Connection" section in the "Telephony Integration" chapter.

- After configuring the AXL server, select Test under section AXL Servers to check that AXL server is up and running.
- On the same page, check the **Enable End User PIN Synchronization for Primary AXL Server** check box to enable the feature.
- Log in to the Cisco Unified OS Administration, go to **Security** > **Certificate Management**. On the Find and List Certificates page, select **Upload Certificate\Certificate** Chain. On the Upload Certificate\Certificate Chain page upload a valid certificate for the Cisco Unified CM to the Cisco Unity Connection tomcat-trust.

  To ignore the certificate validation errors for AXL server, check the **Ignore Certificate Errors** check box on the Edit AXL Server page.

  For more information on certificates, see “Security” chapter of *Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection Release 11.x* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/os_administration/b_11xcucosagx.html.

Configuring PIN Synchronization in Cisco Unified CM

Do the following to configure PIN Synchronization feature in Cisco Unified CM:

- To enable PIN Synchronization, first upload a valid certificate for the Cisco Unity Connection from the Cisco Unified OS Administration page to the Cisco Unified Communications Manager tomcat-trust.
- To create an Application user in Cisco Unified CM, go to **User Management** > **Application User** and select **Add New**. On the Application User Configuration page, enter the values of the required field and select **Save**.

  Note Make sure that the User ID and password entered on the Application User Configuration page must match the username and password of the Cisco Unity Connection system administrator.

- In Cisco Unified CM, go to **System** > **Application Servers** and select the application server that you set up for Cisco Unity Connection. On the Application Server Configuration page, in the **Available Application User** field, select the application user that is created with Cisco Unity Connection administrator credentials and move it to the **Selected Application User** field.

If Cisco Unity Connection server is not available on the Find and List Application Servers page, you need to create a new application server for Cisco Unity Connection. For more information on how to add a new application server, see the "Integrate Applications, Configure Application Servers " chapter in the *System Configuration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

- On the Application Server Configuration page, check the **Enable End User PIN Synchronization** check box and Select **Save**.

For more information to enable PIN Synchronization in Cisco Unified CM, see "PIN Synchronization" section in the "New and Changed Features" chapter in the *Release Notes for Cisco Unified Communications Manager and IM & Presence Service, Release 11.5(1)* at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/rel_notes/11_5_1/cucm_b_release-notes-cucm-imp-1151.html.

Password and PIN Security Considerations for Template Defaults

Following are the considerations when preparing user templates for voicemail or administrator users:

Users with Voice Mailbox Accounts

The web application passwords and voicemail PINs for voicemail users are either set by default Voicemail User Template during installation or the passwords set on the Change Password page for the user template that you select when the creating accounts.

You need to share the PINs and passwords with users so that they can sign in to the Unity Connection conversation and to the Cisco Personal Communications Assistant (Cisco PCA). To increase system security, users must change both PIN and password as soon as possible, and enforce the PIN and password complexity rules.

Users Without Voice Mailbox Accounts

A default web application password is applied to each administrative account that you create. If the administrator user is associated with the default Administrator User Template, then the web application password is a randomly generated string.

Therefore, if you base new administrative accounts on the default Administrator User Template, you must either enter a new default password for the user template to replace the randomly generated string or change the password for each newly created administrator account. To increase system security, the administrators must change the password as soon as possible and enforce password complexity rules.

Change Password

You can change the web application password and voicemail PIN settings for a user on the **Edit > Password Settings** page for the user or associated user template.

Note In Cisco Business Edition, you can change user voice mail PINs and web application passwords either from the User Management pages in Cisco Unified CM Administration.

Note If Unity Connection is integrated with an LDAP directory, the web application password and password settings (for example, password-complexity settings and whether the password expires) are controlled by the LDAP server.

Users can also use the Messaging Assistant to change the passwords and PINs.

Securing and Changing the Web Application (Cisco PCA) Password

You can change the and specify the web application password and voicemail PIN settings for users from Cisco Unity Connection Administration.

Note The Cisco PCA password is referred to as the Web Application password in Cisco Unity Connection Administration.

Each user must be assigned a unique password with the following properties:

- The password must contain at least three of the following four characters: an uppercase character, a lowercase character, a number, or a symbol.
- The password cannot contain the user alias or its reverse.
- The password cannot contain the primary extension or any alternate extensions.
- A character cannot be used more than three times consecutively (for example, !Cooool).

The characters cannot all be consecutive, in ascending or descending order (for example, abcdef or fedcba).

Following are the considerations when securing Cisco PCA passwords for users:

- Users can change the Cisco PCA password only using the Messaging Assistant.
- The Cisco PCA password is not related to the Unity Connection phone PIN and the two are not synchronized. The users do not change the Cisco PCA passwords when prompted to change the phone PIN during first time enrollment.

Users that can access voice messages using an IMAP client must change the Cisco PCA password when updating the password in IMAP client. Passwords are not synchronized between IMAP clients and Cisco PCA. If users have trouble receiving voice messages in an IMAP client after updating Cisco PCA password, see the "Troubleshooting IMAP Client Sign-In Problems in Cisco Unity Connection" section in the "Configuring an Email Account to Access Cisco Unity Connection Voice Messages" chapter of the *User Workstation Setup Guide for Cisco Unity Connection* Release 11.x, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/user_setup/guide/b_11xcucuwsx.html..

Roles

You can assign different roles (System Roles and Custom Roles) to a user from the Edit Roles page of a user or the associated user template. System Roles are the predefined roles provided by Unity Connection whereas Custom Roles are the roles that the administrator creates based on the requirements. For more information on different roles and privileges, see the Roles section of the "User Attributes" chapter..

Note While specifying the user account settings, you can assign multiple roles to a particular user through Edit Roles page. The role you assign to the user account defines the privileges and tasks that an administrator can perform.

Message Waiting Indicator

Unity Connection can set message waiting indicators (MWIs) at up to 10 extensions for a user when new voice messages arrive. When a user account is added, Unity Connection automatically enables the MWI at the primary extension for the user.

You can change MWI settings, add or delete MWI extensions in Cisco Unity Connection Administration on the Message Waiting Indicators page for a user.

In a SCCP integration with Cisco Unified CM or in a SIP trunk integration with Cisco Unified CM 7.1 and later, Unity Connection can also send message counts to supported Cisco IP phones.

Note You cannot specify MWI settings for user templates.

Transfer Rules

The transfer rules specify how Unity Connection handles calls transferred from an automated attendant to user phones. As per the call transfer settings, Unity Connection can either release the call to the phone system, or it can supervise the transfer.

When Unity Connection is set to supervise transfers, it can provide additional call control with call holding and call screening for indirect calls:

- With call holding, when the phone is busy, Unity Connection can ask callers to hold. Unity Connection manages each caller in the queue according to the settings that you configure.

  The wait time in the call holding queue for the first caller in the queue defaults to 25 seconds. If the caller is still on hold after this amount of time, Unity Connection asks if the caller wants to continue holding, leave a message, or try another extension. If the caller does not press 1 to continue holding, or press 2 to leave a message, the caller is transferred back to the Opening Greeting. If call holding is not selected, callers are sent to whichever user greeting is enabled.

- With call screening, Unity Connection can ask for the name of the caller before connecting to a user. The user can then hear who is calling and, when a phone is shared by more than one user, who the call is for. The user can then accept or refuse the call.

  If the call is accepted, it is transferred to the user phone. If the call is refused, Unity Connection plays the applicable user greeting.

Note Transfer, screening, and holding settings do not apply when an outside caller or another user dials a user extension directly.

To control how Unity Connection handles indirect calls at different times of the day or for specified period of time, you can define Standard, Closed, and Alternate transfer rules. The Standard transfer rule is always enabled and cannot be turned off. You can determine whether to enable Closed and Alternate transfer rules or customize the time for which the transfer rules should be enabled.

Message Settings

You can specify message settings for a specific user on the Edit Message Settings page for the user or user template that you use to create users. The message settings determine the message recording length, secure access, and message action of the outside (unidentified) callers when leaving messages for a user. You can specify the following settings:

- The maximum recording length for messages left for a user by outside callers.
- The action of outside callers when leaving messages for a user. For example, mark messages urgent or private, or re-record the messages.
- The secure access for the messages left by outside callers are secure. For more information, see the "Securing User Messages in Cisco Unity Connection" chapter of the *Security Guide for Cisco Unity Connection* Release 11.x to learn how Unity Connection handles secure messages. The guide is available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/security/b_11xcucsecx.html.

The language of the Unity Connection prompts that callers hear when leaving messages for a user.

Message Actions

Message actions determine how Unity Connection handles different types of messages that it receives for a user. Unity Connection applies the configured action for all messages of a given type that are addressed to the user. For example, if the message action for voice messages is set to relay messages of this type to a user at an alternate SMTP address, Unity Connection relays all voice messages including VPIM messages, messages that are sent from an IMAP client, and messages that are recorded and sent by phone. By default, Unity Connection is configured to accept each type of message, meaning that it delivers the message to the user mailbox.

If you choose to relay voice messages to another address, you should consider the following:

- When messages are set to be relayed, users are no longer able to access relayed messages from the Unity Connection phone interface, Web Inbox, Messaging Inbox, or other clients, such as Phone View or Cisco Unified Personal Communicator. You can use the Accept and Relay the Message action to instruct Unity Connection to save a copy of the message in the local user mailbox (where it is accessible by user interfaces) and also relay a copy to another address.
- Unity Connection relays dispatch messages as regular messages.
- Unity Connection does not relay broadcast messages.
- You can configure whether Unity Connection relays private messages and secure messages on the System Settings > Advanced > Messaging page. Private messages are relayed as regular messages with the private flag and secure messages are relayed as regular messages.

- If user accounts are configured to relay voice messages to an alternate SMTP address, the voice messages cannot be transcribed. If users want transcriptions along with the relay feature, you can configure user accounts to Accept and Relay voice messages. This allows the copy of the message that is stored on the Unity Connection server to be transcribed.
- When you configure SMTP notification devices for users, transcription is sent to the user SMTP address. This means that users receive two emails at the SMTP addresses. The first one is the relayed copy of the message WAV file. The second is the notification that includes the transcription. If the users need to access the original recording, users can call in Unity Connection or use an IMAP client to access the user account.

Note SMTP Relay functionality has been primarily designed to configure corporate email address only. In order to avoid any loop in relaying the message, Primary SMTP address of Unity Connection should not be configured as Relay address.

Note Unity Connection supports the relay function in message action only when you have configured an SMTP smart host on the **System Settings > SMTP Configuration > Smart Host** page.

Caller Input

The caller input settings define actions that Unity Connection takes in response to phone keypad keys pressed by callers during a user greeting. For each greeting that allows caller input, you can specify whether callers can skip the greeting, record a message, exit the greeting, transfer to numbers that are not associated with users or call handlers, or transfer to an alternate contact number, call handler, directory handler, or interview handler of your choice. You also use caller input settings to specify which keys users can press to interrupt a user greeting so that they can sign in to Unity Connection.

The caller input settings can be changed only by an administrator user. By default, for each user greeting, Unity Connection acts on certain keys and ignores others.

Table A-1 lists the default actions assigned to phone keypad keys.

Table 1: Table A-1 Default Actions Assigned to Phone Keypad Keys

When Callers Press This Key	Cisco Unity Connection Does This
#	Skips the greeting.
*	Prompts the caller to sign in
0	Sends the caller to the Operator call handler
1 through 9	Ignores the caller

Note Verify that the phone keypad key you select to lock is not the first digit of any of the extensions in your system. If it is, locking the key prevents callers from dialing an extension.

Mailbox

Unity Connection allows you to specify the maximum size, or quota, for every user mailbox. You can configure mailbox quotas that permits Unity Connection to:

- Issue a warning when a mailbox reaches a specified size.
- Prevent a user from sending messages when the mailbox reaches a larger size.
- Prevent a user from sending or receiving messages when the mailbox reaches the largest size that you want to allow.

To handle the varying needs of users in your organization, you can override the systemwide quotas for individual mailboxes and for user templates. For example, you may want to allow employees in the sales department to have larger mailboxes than other employees. If you create user accounts for all sales employees using the same template, you can either specify higher quotas for the user template or higher quotas for individual user accounts.

Caution Quotas are not enforced for messages left by outside callers if the Full Mailbox Check for Outside Caller Messages check box is not checked. This check box appears on the **System Settings > Advanced > Conversations** page. For more information, see the Help for that page.

Message Aging Policy

To ensure that the hard disk where voice messages are stored does not fill up, you can configure Unity Connection message aging rules to automatically move read messages to the Deleted Items folder after a specified number of days and to permanently delete messages in the Deleted Items folder after a specified number of days.

To help enforce a message retention policy, you can configure Unity Connection message aging rules to permanently delete secure messages that are older than a specified number of days based on whether or not users have touched the messages in some way.

Phone Menu

Unity Connection offers several versions of the phone conversation that users hear and use. The version you select determines whether Unity Connection responds only to phone keypad input or also uses voice recognition to interpret spoken commands:

- Touchtone Conversation- Users press keys to tell Unity Connection what they want to do. There are several touchtone conversations to choose from. Each one offers a unique keypad mapping for the message retrieval menus. For some, the keys assigned to options in the Main menu are also unique.
- Voice-Recognition Conversation- Users say voice commands to interact with Unity Connection. Even when assigned to the voice-recognition conversation, users can also press keys on the phone to tell Unity Connection what they want to do; in this case, the touchtone conversation setting is used to determine which keys are mapped to which options. This allows the touchtone conversation setting to serve as a backup if the voice-recognition services are unavailable, and also when users simply choose to use the keypad instead of voice commands to interact with Unity Connection.The user account or template must be assigned to a class of service that enables a license and the voice-recognition feature.

In case of a video call, Unity Connection plays the touchtone conversation only, even if the user is enabled for voice-recognition conversation (Use Voice Recognition Input Style). The user selects the applicable key to switch to voice-recognition conversation (Switch Between Using the Phone Keypad and Using Voice Commands) using custom keypad mapping.

Phone View feature

The Phone View feature allows users to see search results on the LCD screens of their Cisco IP phones when they use the Find Message or the Display Message menu. When it is enabled, Unity Connection users can search for the following types of messages:

- All new voice messages.
- All voice messages
- Messages from a particular user
- Messages from all outside callers
- Messages from a particular outside caller

For more information, see the "Cisco Unity Connection Phone Menus and Voice Commands " chapter of the *User Guide for the Cisco Unity Connection Phone Interface* for Release 11.x, available at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/user/guide/phone/b_11xcucugphone.html..

Playback Message Settings

All of the settings on the Playback Message Settings page, with the exception of the For Draft Messages, Play field, are applicable both to Unity Connection messages and to messages stored externally, depending on whether users are enabled to access email in third party message stores, and are enabled to use the single inbox feature.

Send Message Settings

System broadcast messages are recorded announcements that are sent to everyone in an organization. Users can either send system broadcast messages to all users or update the system broadcast messages stored in user mailboxes.

Note By default, Unity Connection users are not enabled to send or update broadcast messages.

To send or update system broadcast messages, users log on to Broadcast Message Administrator which is a special conversation that permits the users to send or update broadcast messages. For more information, see the Messaging chapter.

Greeting

Users can enable or record up to seven greetings using Messaging Assistant or phone. The greeting settings in Cisco Unity Connection Administration for a user template or user account allow you to specify which

greetings are enabled, how long they are enabled, the greeting source, and the actions that Unity Connection takes during and after each greeting.

When a greeting is enabled, Unity Connection plays the greeting in the applicable situation until the specified date and time arrives, and then the greeting is automatically disabled. A greeting can also be enabled to play indefinitely, which is useful for busy or closed greetings, or when an alternate greeting is enabled by a user during a leave of absence.

Following are the types of greetings that a user can record:

- Audio Greeting: Allows you to record an audio message that must be played when a particular greeting is enabled. For example, you can record an audio message for the Busy greeting, which the callers hear when the call is busy.
- Video Greeting: Allows you to record a video message that must be displayed when a particular greeting is enabled. For example, you can record a video message for the Holiday greeting, which the callers hear when the recipient is on holiday. For more information on Video greetings, see Video chapter.

Changing the Audio or Video Format of Recordings

Unity Connection uses the same audio or video format (or codec) for recording a message that the playback device uses. For example, if users listen to messages primarily on a phone system extension, you should configure users to record messages in the same audio or video format that the phone system uses. If users listen to messages on Personal Digital Assistants (PDAs), however, you should configure users to record messages in the audio format that the PDAs use (such as GSM 6.10).

Consider the following when setting the audio or video format for recording messages:

- Setting the audio or video format for recordings affects all messages, greetings, and names systemwide for all users.
- The audio or video format that you select affects only recordings made by phone, either using TUI, Media Player or TRAP. The recordings made using the Media Player and a microphone are always stored in G.711 mu-law.
- Minimizing the number of different audio formats in used for recording and playback of recorded messages, greetings, and names reduces transcoding between audio or video formats.
- When a message, greeting, or name is recorded in a lower quality audio or video format and later transcoded to a higher quality audio or video format during playback, the sound quality is not improved. Usually, the sound quality of a recording suffers when the sampling rate is changed.
- Changing the audio or video format for recordings affects only messages, greetings, and names that are recorded after the setting is changed. Existing messages, greetings, and names that were recorded in a different audio format are not affected by the new setting.

To Change the Audio or Video Format of Recorded Messages Using Phone

Step 1 In Cisco Unity Connection Administration, expand **System Settings** and select **General Configuration**.

Step 2 On the **Edit General Configuration** page, in the Recording Format list, select the applicable setting and select **Save**.

Post Greeting Recording

Post greeting recordings are the recorded messages that are played after greetings but before callers are allowed to leave a message for a user. For example, you may want to enable a post greeting recording for a particular group of users to convey a confidentiality policy or to let callers know when they can expect a response to the message. You can also use the feature to remind callers to include contact information, invoice or policy numbers, and other such information when they leave messages.

For each post-greeting recording, you use the Media Player on the Edit Post Greeting Recording page of a user template or user to record what you want callers to hear. Post greeting recordings are configured on the Call Management > Custom Recordings page in Cisco Unity Connection Administration. For information on custom recordings, see the Custom Recordings section.

Notification Devices

Users can be configured to call a phone or a pager or send text, or SMS messages to notify users of new messages and calendar events. You can configure the parameters for the call or notification message, the events that trigger the notification, and the schedule on which the notification occurs by setting up notification devices.

You can setup the notification devices for users using the Edit Notification Devices page of a user or user template. For more information, see the Notifications chapter.

Note With Unity Connection 10.5 and later, you can also enter the URI number for the work, mobile, and home notification devices.

Unified Messaging Account

When configuring the single inbox for Unity Connection, check the Generate SMTP Proxy Address From Corporate Email Address check box. When you check this check box, Unity Connection automatically creates a new SMTP proxy address for the value in the Corporate Email Address field. An SMTP proxy address allows Unity Connection to map the sender to a user and to map the message recipients to users by comparing the SMTP addresses in the message header to its list of SMTP proxy addresses. Applicable SMTP proxy addresses are necessary when using Cisco ViewMail for Microsoft Outlook with the single inbox feature to send messages.

When integrated with Exchange, Unity Connection allows touchtone and voice-recognition conversation users to hear the emails read to them when they sign in to Unity Connection using phone. The Text-to- Speech (TTS) playback is available provided that the text portion of the message does not exceed 1 MB in size and the text format of the message is supported by Unity Connection. Supported formats include plain text, quoted-printable text, HTML, and XML.

To enable users to access email in Exchange, configure unified messaging and select the options applicable to text to speech. For more information, see *Unified Messaging Guide for Cisco Unity Connection for Release 11.x* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/unified_messaging/b_11xcucumgx.html.

Video Service Accounts

Unity Connection allows the users to record and play video greetings using a video endpoint. Unity Connection facilitates you to record and play all types of following greetings as video:

- Alternate
- Busy
- Internal
- Closed
- Standard
- Holiday

Note Error greetings are played only as audio greetings.

Alternate Extensions

In addition to the primary extension for each user, you can set up alternate extensions. Alternate extensions can be used for various reasons, such as handling multiple line appearances on user phones. Alternate extensions can also make calling Unity Connection from an alternate device, such as a mobile phone or a phone at another work site more convenient.

When you specify the phone number or URI for an alternative extension, Unity Connection handles all calls from that number in the same way that it handles calls from a primary extension (assuming that ANI or caller ID is passed along to Unity Connection from the phone system). This means that Unity Connection associates the alternate phone number with the user account and when a call comes from that number, Unity Connection prompts the user to enter a PIN and sign in.

If users set an alternate device to forward to Unity Connection, callers can hear the user greeting and leave messages for the user, just as they would when dialing the primary extension of the user. (Callers can also be transferred to the alternate extension for a user from the automated attendant.) Users need to set forwarding from the device itself, not in Unity Connection. Note that the phone number must be passed to Unity Connection for the system to recognize the device.

Users can also address messages to an alternate extension that is associated with another user.

Alternate extensions are grouped into two categories:

- Administrator-defined alternate extensions-Administrators can add up to 9 alternate extensions. Administrators can view and edit both administrator-defined and user-defined alternate extensions.
- User-defined alternate extensions-Users can add up to 10 alternate extensions if they belong to a class of service that allows them to manage user-defined alternate extensions. Users can view administrator-defined alternate extensions if they belong to a class of service that allows them to do so.

Class of service settings allow you to determine whether users can view or manage alternate extensions and whether they can use the Unity Connection Messaging Assistant to manage a set of own alternate extensions.

Users who belong to a class of service with the Allow Users to Manage Their User-Defined Alternate Extensions option enabled can automatically add alternate extensions.To learn more about this feature, see the System Settings chapter.

Using the Custom Keypad Mapping tool in Cisco Unity Connection Administration, you can provide users with the option to edit the alternate extensions from the Preferences menu in the phone interface. When a user selects the option to edit the alternate devices, Unity Connection allows you to list or delete the existing alternate extensions. If the user signs in from a phone number that is not the primary extension or an existing alternate extension or in the Excluded Extensions for Automatically Added Alternate Extensions restriction table, when they select the option to edit the alternate devices, Unity Connection offers to add the phone number as a new alternate extension. For more information on custom keypad mapping, see the Using the Custom Keypad Mapping Tool section.

Alternate Extension Custom Settings

There are several conversation settings that can be customized for alternate extensions. By default, each alternate extension uses the same settings that have been configured for the primary extension of the user. You can also edit advanced settings, such as conversation volume and message speed for alternate extensions (work phone or mobile phone) from which the user is calling. For example, a user calling from a mobile phone may want to use the voice-recognition input style and not be asked for a PIN. But a user calling from a work phone may want to use the touch tone input style and be required to enter a PIN.

Alternate Names

Alternate names are different versions of a name than what is listed in the corporate directory. Cisco Unity Connection considers these names when a caller uses voice recognition to place a call. For example, if a caller asks Unity Connection to dial "Mary Jameson," which was the maiden name of Mary Brown, Unity Connection can reference this information and connect the caller to the correct user.

In addition to recognizing alternate names when users and outside callers use voice recognition to place a call, Unity Connection recognizes alternate names when callers and users use voice recognition to address voice messages. Alternate names can be created for users, VPIM contacts, administrator-defined contacts, system distribution lists, private lists, and user-defined contacts.

While Unity Connection already recognizes hundreds of common shortened names (Bill in place of William, for example), you might want to add another version of an uncommon name, unusual nicknames, or maiden names. You could also use alternate names to add phonetic spellings of hard-to-pronounce names. For example, you could add "Goolay" as an alternate name for the last name "Goulet."

From the Cisco PCA, users can edit or change the alternate names and can also create alternate names for customers, suppliers, family members, and friends who are not included in the Unity Connection directory, or for private lists. This helps in making it easier for the users or outside callers to dial the contacts or address to the lists when using voice commands.

Note You cannot add or edit alternate names on a user template, nor can you use the Bulk Edit utility to add or edit alternate names for multiple user accounts.

Private Distribution Lists

Users can use the private distribution lists that are associated with the accounts to send voice messages to more than one user at a time. The users can set up and manage the private lists using the Messaging Assistant

or the phone. For more information on private distribution list, see the " Managing your Private List " chapter of the *User Guide for the Cisco Unity Connection Messaging Assistant Web Tool* (Release 12.x) at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/user/guide/assistant/b_12xcucugasst.html.

Note You cannot specify private lists on a user template or for multiple user accounts at once.

SMTP Proxy Addresses

Unity Connection uses SMTP proxy addresses to map the recipients of an incoming SMTP message sent from an IMAP client to the appropriate Unity Connection user or VPIM contact. If users use IMAP clients to send, reply to, or forward messages to VPIM contacts you should configure each VPIM contact with an SMTP address.

Note Unity Connection handles SMTP messages sent to the contacts that are not associated with a VPIM location according to the option selected for the **System Settings > General Configuration > When a Recipient Cannot Be Found** setting.

For example, when Robin Smith, whose email client is configured to access Unity Connection with the email address robin.smith@example.com, records a voice message in ViewMail for Outlook and sends it to chris.jones@example.com, Unity Connection searches the list of SMTP proxy addresses for robin.smith@example.com and chris.jones@example.com. If these addresses are defined as SMTP proxy addresses for the Unity Connection users Robin Smith and Chris Jones respectively, Unity Connection delivers the message as a voice message from Robin Smith to Chris Jones.

Note For more information on configuring Unity Connection so that users can use IMAP clients to send, forward, or reply to messages through the Unity Connection server, see the Integrated Messaging