Configure Cisco Unity Express 10.2 Using the GUI

First Published: 2020-04-01

Last Modified: 2020-04-01

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1

Welcome to Cisco Unity Express

Welcome to the online help pages for Cisco Unity Express. To search for help topics in this file, choose **Search** in the menu at the top of this page. For information on using help, choose **Using Help**.

For more information about Cisco Unity Express, see the Cisco Unity Express software and related documentation at the following URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps5520/tsd_products_support_series_home.html

Note The online help pages describe both user and administrator features of Cisco Unity Express. If you are a user, the GUI displays only a subset of all of the features and parameters described in the online help.

Tip When you use Cisco Unity Express, you can use the Back and Forward buttons on your browser to view information in another window, but if you make changes in that window and submit your changes, you will receive an error and your changes will **not** be saved. **Do not submit information after using your browser's navigation tools to move to another window**. Click the appropriate button or menu to reach the window in which you want to enter information.

CHAPTER 2

Change Your Password

Guidelines

- Passwords should be at least 3 and no more than 32 alphanumeric characters in length.
- Use a mixture of uppercase and lowercase letters and numbers.
- Spaces are not allowed.

Change an Expired Password

To change your password if you have reached the Expired Password prompt:

Step 1 Enter your old password. If it was not set by the system administrator, leave this field blank.

Step 2 Enter your new password.

Step 3 Enter your new password again for verification and click **Apply**.

Additional Change Password Procedures

Change your password by performing the following tasks:

Step 1 Choose **Configure** > **Users**.

Step 2 Click your name in the list of users.

Step 3 Ensure that **Password specified below** is selected in the Password options field.

Step 4 Enter your new password.

Step 5 Enter your new password again for verification and click **Apply**.

CHAPTER 3

Start the Initialization Wizard for Cisco Unified Communications Manager (CUCM)

This window appears the first time you log in to the system after installing the Cisco Unity Express software. Perform the following tasks:

- Call Agent Integration, on page 6—Use this option to change the call agent from Cisco Unified Communications Manager (CUCM) to Cisco Unified Communications Manager Express (CUCME).
- View Current Settings, on page 6—Use this option to display several system parameters that were defined when the Cisco Unified Communications Manager software was installed. Also displays the default Cisco Unity Express settings.
- Run the Initialization Wizard. See Overview, on page 7.

Note You cannot run the Initialization Wizard after choosing the following option.

- Skip Initialization Wizard and Log off—Use this option only if you are using the Cisco Unity Express command-line interface to configure the system parameters.
- Log Off (Run Initialization Wizard Later)

Call Agent Integration

This pull-down menu enables you to change the call agent. For example, you can change the call agent from Cisco Unified Communications Manager (CUCM) to Cisco Unified Communications Manager Express (CUCME).

Note Use this option with caution. Changing the call agent will permanently delete all non-local site related configuration and reboot the system automatically.

Step 1 Select the call agent from the pull-down menu.

You will receive a warning notifying you that changing the call agent will permanently delete all non-local site related configuration and reboot the system automatically.

Step 2 Click Ok to continue or Cancel to cancel the operation.

The system reloads. Once the system reload is complete, you will receive a notice that the system is not initialized, and that only Administrator logins are allowed.

Step 3 Log in to the administrative interface using your User Name and Password.

Current Settings

This window displays current system settings that were configured when the Cisco Unified Communications Manager application was installed. It also displays the Cisco Unity Express settings configured at the time of installation. You cannot change the system settings from this window. Run the Initialization Wizard to change the values.

- Language
- Mailbox Size
- Maximum Caller Message Size
- Message Expiry Time
- Voice Mail Number (CUCM)
- Voice Mail Number (SRST)
- Auto Attendant Access Number (CUCM)
- Auto Attendant Access Number (SRST)
- Voice Mail Operator Extension
- Auto Attendant Operator Extension
- Administration via Telephone Call-in number (CUCM)

- Administration via Telephone Call-in number (SRST)
- SIP MWI Notification Mechanism

Overview

When logging in to the system for the first time, use the Initialization Wizard to configure your system. The Initialization Wizard is a software tool that has a series of windows that help you configure Cisco Unity Express. The wizard starts automatically the first time you log in to the graphical user interface (GUI).

Some of the information shown on the wizard windows comes from system parameters that were configured during the installation of the Cisco Unified Communications Manager system and the Cisco Unity Express software.

Cisco Unified Communications Manager Login

Enter the required information in the fields:

- Primary Cisco Unified Communications Manager
- Secondary Cisco Unified Communications Manager (Optional)
- Tertiary Cisco Unified Communications Manager (Optional)
- Web User Name (Optional)
- Web Password (Optional)
- JTAPI User Name
- JTAPI Password

To go to the Import Cisco Unified Communications Manager Users, on page 7 window, click Next.

Import Cisco Unified Communications Manager Users

The Importing Cisco Unified Communications Manager Users window displays any users who were configured at the same time as the Cisco Unified Communications Manager software was installed. You can import any or all of those users into the Cisco Unity Express database. If no users are displayed, you can configure users after the initialization process is completed.

Note If you are importing Cisco Unified Communications Manager users, the usernames cannot contain spaces. If you import Cisco Unified Communications Manager user IDs that contain spaces, an error appears after your information is committed.

The Import Users window contains the following fields:

- User ID

- Extension number
- Primary Extension
- Mailbox—option to create a voice mailbox for the user
- Administrator

Step 1 If any users are listed, in the column to the left of the users' names, do one of the following:

- To import all the users in the list to the Cisco Unity Express database, click the box next to User ID. This places a check mark in the box next to each user ID.
- To import specific users to the Cisco Unity Express database, click the box next to each user ID that should be imported into the database. Users who are not in the Cisco Unity Express database will not have a voice mailbox.

Step 2 In the Primary Extension column, select a primary extension for the user. The primary extension is the main extension that callers dial to reach a user. If no primary extension is designated for a user, that user cannot receive voice-mail messages, but will be reachable by callers using the dial-by-name feature. In this field, None means that none of the displayed extensions for the user is the primary extension. You can designate a mailbox for this user now, but the user cannot access it until you configure the user's primary extension at a later time.

Step 3 In the Mailbox column, do one of the following:

- To create a mailbox for all users, click the box next to Mailbox. This places a check mark in each user's box in the column. Cisco Unity Express creates the mailbox when the initialization process is complete.

Note Clicking this box creates a mailbox for all users displayed in the list. If you selected specific users in Step 2, do not click this box.

- To create a mailbox for specific users, click the box in the Mailbox column for each user who should have a mailbox.

Step 4 In the Administrator column, do one of the following:

- To assign administrative privileges to all users, click the box next to Administrator. Note: If you selected specific users in Step 2, do not click this box.
- To assign administrative privileges to specific users, click the box in the Administrator column for each user who should have this permission.

Step 5 To go to the Configure System Defaults, on page 8 window, click Next.

Configure System Defaults

Use this procedure to configure system defaults when running the Initialization Wizard. The values shown in this window are Cisco Unity Express default values. These values affect all users and mailboxes in the voice-mail system. To change values for individual users, see Display or Modify a User Profile, on page 15.

The Defaults window displays following fields. If necessary, enter new values into the fields.

- System default Language

- Password and PIN Options:
- Password options
- Personal identification number (PIN)
- Mailbox Defaults:
- Mailbox Size
- Maximum Caller Message Size
- Message Expiry Time

To go to the Configure Call Handling, on page 9 window, click Next.

Configure Call Handling

Use this procedure to configure call handling when running the Initialization Wizard. You can change these values later by Configure Voice-Mail Call-Handling Parameters, on page 127.

Tip The Voice Mail number, Auto Attendant number, and Greeting Management number fields should not contain the same telephone number. However, the operator extensions can be the same for these systems.

The Voice Mail Call Handling window displays the following fields. If necessary, enter the Call in Numbers for Voice Mail, Auto Attendant and the Administration via telephone (AVT) system.

- Voice Mail Phone Number
- Voice-Mail Operator extension
- Auto attendant access number
- Auto attendant operator extension
- Administration via Telephone (AvT) number
- SIP MWI notification mechanism

To go to the Commit Your Information, on page 9 window, click Next.

Commit Your Information

The Commit window displays the values that you set up using the Initialization Wizard. Use the scroll bar to view additional parameters. At this point, none of these values has been saved to the Cisco Unity Express database.

Procedure

Step 1 If any value is not correct, click Back to return to the appropriate screen and change the value.

Step 2 If you want to save these values as the default startup system configuration, click the box to the left of "Finally, save to startup configuration....".

Step 3 If all the values are correct, click Finish to save the values and complete the initialization. The status window appears. The default values are stored in the Cisco Unity Express database, and users designated as administrators are added to the Administrator group.

Note If you are importing Cisco Unified Communications Manager users, the usernames cannot contain spaces. If you import Cisco Unified Communications Manager user IDs that contain spaces, an error appears after your information has been committed.

You can change default parameters later. See Related Topics.

Related Topics

Configure Domain Name Settings, on page 83
Add a New User, on page 13
Add a New Mailbox, on page 95

View the Status

The Initialization Wizard Status window appears after you have completed the Initialization Wizard and contains the fields shown in the following table. The field values show whether the information was updated or the action failed.

Click View/Hide details next to the fields to display information or error messages.

Field	Description
Auto-generated authentication information	If you chose to generate passwords and PINs for users automatically, they are displayed.
Defaults	Status of voice mailbox size, message length, message expiration time, password and PIN generation, and message-waiting indicator (MWI) on and off numbers.
User Creation	Status of creation of the selected Cisco Unified Communications Manager users in the Cisco Unity Express database.
MWI application creation	Status of initialization of the MWI policy.
Voice-mail application creation	Status of initialization of the voice-mail system and storage of the voice-mail system telephone number.
Administration via Telephone application creation	Status of initialization of the Administration via Telephone application and storage of the Administration via Telephone telephone number.
Auto Attendant application creation	Status of initialization of the auto attendant application and storage of the auto attendant telephone number.
JTAPI provider	Status of update of the corresponding JTAPI options and values entered in the Initialization Wizard fields.

Field	Description
CTI ports **Note** You must reload the system for importing users and CTI ports and for voice calls to work.	Status of the CTI ports. See **System** > **CTI Ports**.

Logout or Reload Cisco Unity Express.

CHAPTER 4

Configure Users for Cisco Unified Communications Manager (CUCM)

View List of Users

Use this procedure to view a list of users in the system.

Choose Configure > Users. The Configure Users window appears and contains the following fields:

- User ID—By default, the system displays users in alphabetical order by user ID. To sort from A to Z, click User ID.
- Display Name—To display the list of users in order by display name, click Display Name.
- Primary Extension—To display the list of users in order by primary extension, click Primary Extension.
- Use the dialog box to change the number of rows displayed per window.

Add a New User

Use this procedure to add a new user to the system.

Step 1 Choose Configure > Users. The Configure Users window appears:

Step 2 Click Add. The Add a New User window appears.

Step 3 Enter information into the following fields:

- User ID
- First Name and Last Name
- Nick Name
- Display Name
- Primary Extension
- Primary E.164 number
- Fax number
- Language
- Password options
- Password
- Confirm password—Enter the password again for confirmation.
- PIN options
- Personal identification number (PIN)
- Confirm PIN—Enter the PIN again for confirmation.
- Create mailbox—Click to create a voice mailbox for this new user. See Add a New Mailbox, on page 95 .

Step 4 Click Add to save your changes. The Add a New Mailbox window appears. Proceed to Add a New Mailbox, on page 95.

Note If you selected a random password or PIN, a message appears with the new password or PIN. Write these values in a secure place to give to the user. They are also displayed on the user profile page.

Import a User from CUCM

Use this procedure to select a user to import.

Note You must first configure the Cisco Unified Communications Manager Web Administrator Username.

Step 1 Choose **Configure** > **Users** > **Import**. The Import Cisco CUCM Users window appears.

Step 2 Click on **Find**. The Cisco CUCM User Search window appears.

Step 3 Specify User IDs in the field separated by a space, comma, or a new line.

Tip You can enter a maximum of 200 user IDs.

Step 4 Click Find. The Search Results window appears with the results listed. You have the option to View/Hide details of your search.

Display or Modify a User Profile

Use this procedure to display or modify a user profile.

Step 1 To view a user's profile, click Configure > Users. The Configure Users window appears.

Note If you do not see the user, click Find to search for the user (see Find a User, on page 16). You can also select All from the drop-down menu in the Rows Per Page field at the bottom of the Configure Users window.

Step 2 Click the user ID of the person whose profile you want to see. The user's profile window appears with the following fields shown:

- User ID
- First Name and Last name
- Nick Name
- Display Name
- Primary Extension
- Primary E.164 number
- Fax Number
- Language
- Password Login (enabled by default)
- Password options
- Password
- Confirm password—Enter the password again for confirmation.
- PIN login (enabled by default)
- PIN options
- Personal identification number (PIN)
- Confirm PIN—Enter the PIN again for confirmation.

Step 3 Click to enable notification for this user profile.

Additional User Profile Options

In this window, you can also click the following tabs:

- Groups—Change a user's groups. See Display or Modify Group Subscriptions, on page 16.
- Mailboxes—Display or modify a user's mailbox information. See Display or Modify a Mailbox, on page 97.

- Notification—Configure notification of received voice-mail messages to be sent to a user's phone, pager, or email. See Configure Notification Devices, on page 130.

Display or Modify Group Subscriptions

Use this procedure to modify the groups to which a user is assigned.

Step 1 Choose Configure > Users. The Configure Users window appears.

Step 2 Click the name of the user whose group subscription you want to view or modify. The User Profile window appears.

Step 3 Click the Groups tab. The following fields are displayed:

- Group ID
- Rights—member or owner
- Description
- Primary extension—primary extension of the general-delivery mailbox assigned to the group.

Step 4 To subscribe the user as the owner of another group, click Subscribe as owner. The Find window appears. Enter the group ID, description, or extension number in the Find window and click Find.

Or

Step 5 To subscribe the user as a member of another group, click Subscribe as member. The Find window appears. Enter the group ID, description, or extension number in the Find window and click Find.

Step 6 Click the box next to the group that this user should join and click Select Rows.

Step 7 (Optional) To unsubscribe the user from a group, click the box next to the Group Name and click Unsubscribe.

See Configure Groups, on page 19 for more information.

Find a User

Use this procedure to search for a user.

Step 1 Choose Configure > Users. The Configure Users window appears.

Step 2 Click Find. The following fields appear:

- User ID
- Name
- Extension

Note All fields are optional.

Step 3 Enter the search criteria in one or more fields and click Find. The User Configuration window displays the results of your search.

Delete a User

To delete a user from Cisco Unity Express, use this procedure. Deleting a user in the Cisco Unity Express GUI also deletes the user's mailbox. Deleting a user in the command-line interface leaves the user's mailbox orphaned.

Step 1 Choose Configure > Users.

Step 2 Click the box next to the user ID that you want to delete.

Step 3 Click Delete.

Step 4 Click Ok to confirm the deletion.

CHAPTER 5

Configure Groups

View List of Groups

Use this procedure to view a list of groups:

Choose Configure > Groups. The Configure Groups window appears and contains the following fields:

- Group ID—By default, the group list is sorted alphabetically by group ID. To sort from Z to A, click Group ID.
- Display Name—To sort by description in alphabetical order, click Display Name. To sort from Z to A, click Display Name again.
- Primary Extension for the group's general-delivery mailbox. To sort numerically by primary extension, click Primary Extension. To sort from high to low, click Primary Extension again.
- Privileges—Lists the various specified group privileges that have been assigned.
- Use the dialog box to change the number of rows displayed per window.

Add a New User Group

Use this procedure to create a new group to which users can belong.

Before you begin

Configuring one or more groups is optional. Many businesses find that having a mailbox for a group, called a general-delivery mailbox, is very convenient. Members of a group can retrieve voice messages left in the general-delivery mailbox. For example, a Customer Service mailbox could be configured to receive messages from customers, and anyone assigned to a Customer Service group could retrieve the messages. Members of the general-delivery mailbox can be individual users or other groups. Individual users also have their individual mailboxes, and groups that are members of another group have their own mailboxes.

Be sure to have the following information available:

- The Extension number to be assigned to the group. Ensure that this extension is active.
- The maximum number of seconds for voice messages that this mailbox can hold.
- The maximum length, in seconds, for any voice message that is stored in this mailbox.
- The length of time, in days, that messages can remain in this mailbox.

Step 1 To add a new user group, choose Configure > Groups. The Configure Groups window appears.

Step 2 Click Add. The Add a New Group window appears.

Step 3 Enter information into the fields shown below:

- Group ID
- Full Name
- Description—The word “group” is automatically added to the Group ID entry. You can add more text to this description.
- Primary Extension for the group’s general-delivery mailbox
- Primary E.164 number
- Fax number

Step 4 Click to create mailbox—Click to create a general-delivery mailbox for this new group. See Add a New Mailbox, on page 95.

Capabilities

Check the boxes for capabilities, or privileges, to assign to the group. See Privileges for detailed information.

Step 5 Click **Add**. The Add a New Mailbox window appears. Enter or select the following information:

- Owner
- Description—Description of the mailbox.
- Zero-out number (operator assistance)

- Mailbox Size
- Maximum Caller Message Size
- Message Expiry Time
- Play Tutorial
- Allow Login Without PIN
- Enabled—Indicates that the mailbox will be activated immediately. Unchecking this box deactivates the mailbox.
- Fax enabled
- Enable notification for this user or group

See Configure Mailboxes, on page 95 for more information.

Step 6 To save the information, click Add. The Configure Groups window reappears with the new Group ID in the table.

Subscribe Members to a Group

Use this procedure to add members to a group. When you add members to a group, each member has access to the voice messages that are stored in the group's mailbox.

Step 1 Choose **Configure** > **Groups**. The Configure Groups window appears.

Step 2 Click the name of the group to which you are adding new members. The Group Profile window appears. Current information about the group is displayed in the fields.

Step 3 Click **Owners/Members**. The window displays all members of the group.

Step 4 To add a new member, click **Subscribe Member**. The Find window appears.

Step 5 Enter the ID, name, or extension of the person or group that you want to add to this group. All fields are optional.

Step 6 **Click Find**. All users that meet the search criteria appear.

Step 7 Remaining in the Find window, do one of the following:

- Add one or more members to the group by checking the box next to each selected member's name and click **Select Rows**. The Group window appears with the new member added.
- Look for other people to add but clicking **Back to Find** without checking a box next to any name. The Find window appears. Return to Step 5, on page 21 and continue.

Step 8 To add more members to the group, repeat Step 4, on page 21 through Step 7, on page 21.

Subscribe Owners to a Group

Use this procedure to add owners to a group. Each owner of a group has control of the group's mailbox, but cannot access the group's messages unless he is a member of the group.

Step 1 Choose **Configure** > **Groups**. The Configure Groups window appears.

Step 2 Click the name of the group to which you are adding new owners. The Group Profile window appears. Current information about the group is displayed in the fields.

Step 3 Click **Owners/Members**. The window displays all members and owners of the group.

Step 4 To add a new owner, click **Subscribe Owner**. The Find window appears.

Step 5 Enter the ID, name, or extension of the person or group that you want to add as the owner of this group. All fields are optional.

Step 6 Click **Find**. All users that meet the search criteria appear.

Step 7 Remaining in the Find window, do one of the following:

- Add one or more owners to the group by clicking the box next to each selected owner's name and click **Select Rows**. The Group window appears with the new owner added.
- Look for other people to add by clicking **Back to Find** without clicking a box next to any name. The Find window appears. Return to Step 5, on page 22 and continue.

Step 8 To add more owners to the group, repeat Step 4, on page 22 through Step 7, on page 22.

Unsubscribe Members and Owners from a Group

Use this procedure to unsubscribe members and owners from a group. You must be an owner of a group to delete members and owners.

Step 1 Choose **Configure** > **Groups**. The Configure Groups window appears.

Step 2 Click the name of the group that you want to manage. The Group Profile window appears. Current information about the group is displayed in the fields.

Step 3 Click **Owners/Members**. The window displays all members and owners of the group.

Step 4 Click the box next to the name of each member or owner you want to delete.

Step 5 Click **Unsubscribe** to delete these members or owners. The Group Members window reappears with the members or owners removed.

Display or Modify Group Parameters

Use this procedure to display or modify group parameters.

Step 1 Choose **Configure** > **Groups**. The Configure Groups window appears.

Step 2 Click the name of the group that you want to view or modify. The Group Profile window for this group appears with the following fields:

- Group ID

- Full Name
- Description—The word “group” is automatically added to the Group ID entry. You can add more text to this description.
- Primary Extension for the group’s general-delivery mailbox
- Primary E.164 number
- Fax number
- Enable notification for this group (see Configure Message Notification, on page 129)

The available Privileges fields are displayed.

Step 3 To edit these fields, enter the new information and click **Save**.

View Owners and Members of a Group

Use this procedure to view owners and members of a group.

Step 1 Choose **Configure** > **Groups**. The Configure Groups window appears.

Step 2 Click the group name that you want to view. The Group Profile window for this group appears.

Step 3 Click the **Owners/Members** tab to see the users who are owners or members of this group. The Owners/Members window appears with the fields listed in the table. Click any column heading to sort by that subject.

View Group Membership in Another Group

Use this procedure to view the current group's membership in another group.

Step 1 Choose **Configure** > **Groups**. The Configure Groups window appears.

Step 2 Click the group name that you want to display. The Group Profile window for that group appears.

Step 3 To display the groups to which the group is subscribed, or the groups that this group owns, click the **Owner/Member of Groups** tab. The Owner/Member of Groups window appears with the fields listed in the table. Click on any column heading to sort by that subject.

Modify Group Ownership and Membership in Other Groups

A group has its own set of members, but a group can also be assigned as a member or an owner of one or more other groups. If a group is assigned as an owner of another group, any individual member of the owner group has privileges as an owner of the owned group. For example, if the Administrator group is added as an owner of the Technical Support group, any individual member of the Administrator group can add, modify, or delete members of the Technical Support group. Additionally, individual users that do not belong to another group can be added as owners of the Technical Support group.

Use this procedure to modify a group's ownership and membership in other groups.

Step 1 Choose **Configure** > **Groups**. The Configure Groups window appears.

Step 2 Click the name of the group whose membership you want to modify. The Group Profile window for this group appears.

Step 3 Click **Owner/Member of Groups**. The Owner/Member of Groups window appears.

Step 4 To designate your group as an owner of another group, click **Subscribe as owner**. To subscribe your group as a member of another group, click **Subscribe as member**. The Find window appears.

Step 5 In the Find window, enter the group ID, description, or extension of the groups that you want to find.

Step 6 Click **Find**. All groups that meet the search criteria appear.

Step 7 To select one or more groups, click the box next to each group's name and click **Select Rows**. The new groups are added to the list of groups in the Owner/Member of Groups window.

Delete a Group

Use this procedure to delete a group from Cisco Unity Express. Deleting a group will delete the group's mailbox. However, members of the group (individual members or other groups) will not be deleted from Cisco Unity Express.

Step 1 Choose **Configure** > **Groups**. The Configure Groups window appears.

Step 2 Select the box next to the name of the group that you want to delete and click **Delete**.

Step 3 At the prompt, click **Ok** to delete the group.

Find a Group

Use this procedure to search for a group.

Step 1 Choose **Configure** > **Groups**. The Configure Groups window appears.

Step 2 Click **Find**. The following fields appear in the Find Groups window:

- Group ID
- Description
- Extension—Extension for the group's general-delivery mailbox.

Note All fields are optional.

Step 3 Enter the search criteria in one or more fields and click **Find**. The Find Groups window closes and the Configure Groups window displays the results of your search.

CHAPTER 6

Set User Defaults

When you create a user, the defaults that you set in the Configure User window take effect. Use these procedures to specify the default global password and PIN policy settings for all users. This default set of parameters is applied when a new user is created.

Configure Password and PIN Options

If you chose to generate passwords and PINs for users automatically, they are configured in the following steps.

Procedure

Step 1 Choose **Configure** > **User Defaults**.

The system displays the Configure User Defaults page.

Step 2 Choose the default language from the drop-down list.

Step 3 Configure password and PIN options by performing the following tasks in the Password and Pin columns.

a) Although there is space to set a PIN, the Cisco Unified SIP Proxy system does not use PINs. If you set values here, they will not be used. (Optional) Select whether the auto-generation policy will be **random** or**blank**.
b) (Optional) Check **Enable expiry (days)** to set an expiration date for the password. The range is 3 to 365.
c) Set the history depth. The range is 1 to 10.
d) Select the minimum length of the password and PIN. The range for the PIN is 3 to 16. The minimum length of the password ranges from 8 through 64 characters. There is no limit on the maximum length of the password. A valid password should have at least one uppercase letter, one lowercase letter, one number, and a symbol.

Note The change in the minimum password length range is applicable when a new user is created or the password of an existing user is updated. It does not apply to passwords that are already in use.

Step 4 Click **Apply**.

Configure Account Lockout Policy

The account lockout policy determines how the system acts when a user tries to log in and fails.

Step 1 Choose **Configure**> **User Defaults**.

The system displays the Configure User Defaults page.

Step 2 Choose one of the following lockout policy types for the Password and PIN fields:

- Although there is space to set a PIN, the Cisco Unified SIP Proxy system does not use PINs. If you set values here, they will not be used. Disable lockout—The user can continue to try to login with no consequences for failing.
- Permanent—The user is permanently locked out after a certain number of failed login attempts. Enter the maximum number of failed attempts. The range is 1 to 200.
- Temporary—The user is temporarily locked out of the system. Enter values for the following:
  - Number of allowable attempts. The range is 1 to 200.
  - Temporary lockout duration. Pick any number in minutes.
  - Maximum number of failed attempts. The range is 1 to 200.

Step 3 Click **Apply** to save your settings.

CHAPTER 7

Configure Supervisors

View List of Supervisors

Use this procedure to > view a list of configured Supervisors.

Step 1 Choose **Configure** > **Supervisors**.

The Configure Supervisors window appears with a list of configured Supervisors that shows their user IDs.

Step 2 To configure Supervisors, you can either:

- Edit the list of primary and secondary reports for a Supervisor by clicking on the link for user ID.
- To add a new Supervisor, click **Designate.**
- To delete a Supervisor, click **Undesignate.**

Add Supervisors

Use this procedure to add a new Supervisor.

Step 1 Enter the user ID of the user that you want to be a Supervisor or click the search icon to the right of the field and click **Find** to display a list of users.

Step 2 Click **Designate** to save your settings.

Edit Supervisors

Use this procedure to edit the configuration of an existing Supervisor.

Step 1 Choose the tab for **Primary reports** or **Secondary reports**.

Step 2 Click **Add Employee**.

Step 3 Enter the user ID of the user that you want to add or click the search icon to the right of the field and click **Find** to display a list of users.

Step 4 Click **Add Employee** to save your changes.

Step 5 Repeat Steps 3, 4, and 5 as many times as necessary to add all of reports that you want.

Step 6 If needed, change the display name or the user ID of the user that you want to be a Supervisor or click the search icon to the right of the field and click **Find** to display a list of users.

Step 7 Click **Designate** to save your settings.

CHAPTER 8

Configure Privileges

Overview

Cisco Unity Express software provides several predefined privileges that you can assign to groups. You can also create your own privileges and modify the predefined privileges.

When you assign a privilege to a group, any member of the group is granted the privilege rights. An administrator group is created automatically by the software initialization process from the imported subscribers designated as administrators. You can assign subscribers to an existing group using CLI commands or the GUI option Configure > Users.

When you create or modify privileges, you add or delete the operations allowed by that privilege. Operations define the CLI commands and GUI functions that are allowed. Most operations include only one CLI command and GUI function. In addition to adding operations to a privilege, you can also configure a privilege to have another privilege nested inside of it. A privilege configured with a nested privilege includes all operations configured for the nested privilege.

Table 1: Privileges, on page 32 describes the predefined privileges provided with the Cisco Unity Express software and the operations associated with them. Table 2: Operations, on page 33 describes all available operations that you can add to privileges.

Note You cannot modify the superuser privilege. The superuser privilege includes all the operations.

To configure privileges, see Create a New Privilege, on page 36.

To display a list of privileges, use the **show privileges** command in Cisco Unity Express EXEC mode. To display detailed information about a specific privilege, use the **show privilege detail** command.

Note Users do not need privileges to access their own data. The user's data is primarily associated with the voice mail application and includes the user's:

- Language (configured for the user's voice mailbox)
- Password
- PIN
- Membership to groups owned by the user
- Ownership of groups owned by the user
- Notification profile
- Cascade settings
- Personal voice mail zero out number
- Voice mail greeting type
- Voice mail play tutorial flag
- Public distribution lists owned by the user
- Private distribution lists

Table 1: Privileges

Privilege	Description	Default Operations
superuser	Grants unrestricted system access.	all
Manageprompts	Allows subscribers access to the AvT prompt management but not to any other administrative functions.	prompt.modify system.debug
broadcast	Allows subscribers to send broadcast messages across the network.	broadcast.local broadcast.remote system.debug
local-broadcast	Allows subscribers to send broadcast messages only to subscribers on the local network.	broadcast.local system.debug
manage-passwords	Allows subscribers to create, modify, and delete user passwords and PINs.	user.pin user.password system. debug
ManagePublicList	Allows subscribers to create and modify public distribution lists.	voicemail.lists. public system.debug
manage-users	Allows subscribers to create, modify, and delete users.	user.configuration user.pin user.password user.mailbox user.notification user.remote, group.configuration system.debug
ViewHistorical Reports	Allows subscribers to view historical reports.	report.historical
ViewPrivateList	Allows subscribers to view another subscriber's private distribution lists. The subscriber cannot modify or delete the private lists.	voicemail.lists.private.view

Privilege	Description	Default Operations
ViewRealTime Reports	Allows subscribers to view real-time reports.	report.realtime
vm-imap	Allows subscribers to access the IMAP feature.	voicemail.imap.user

Table 2: Operations

Operation	Description
broadcast.local	Create and send broadcast messages to local locations. Delete or reschedule broadcast messages.
broadcast.remote	Create and send broadcast messages to remote locations.
call.control	Configure settings for Cisco Unified CME (SIP) and Cisco Unified Communications Manager (JTAPI).
database.enterprise	Configure Enterprise database settings.
group.configuration	Create, modify, and delete groups.
network.location	Create, modify, and delete network locations, network location caching, and NDR/DDR configuration.
prompt.modify	Create, modify, and delete system prompts for AA scripts. Also includes upload/download of prompts on the CLI.
report.historical.manage	Configure and generate historical reports. Collect data from Cisco Unity Express using the **copy** command.
report.historical.view	View historical reports.
report.realtime	Run and view real-time reports.
report.voicemail	Run and view voice mail reports.
restriction.tables	Create, modify, and delete restriction tables.
script.modify	Create, modify, and delete system AA scripts. Also include upload and download of scripts on the CLI and Editor Express.
security.aaa	Configure and modify AAA service settings.
security.access	Configure system level security regarding encryption of data, including defining crypto keys. **Note** Also includes permission to reload the system.

Operation	Description
security.password	Configure settings for the system password and policy, such as: • Expiry • Lockout (temporary and permanent) • History • Length
security.pin	Configure settings for the system PIN and policy, such as: • Expiry • Lockout (temporary and permanent) • History • Length
services.configuration	Configure system services: DNS, NTP/clock, SMTP, Fax Gateway, Cisco UMG, hostname, domain, interfaces (counters) and system default language. **Note** Also includes permission to reload the system.
services.manage	System level services commands not related to configuration like clearing DNS cache and ping
site.configuration	Create, modify, or delete sites for use with Cisco UMG.
software.install	Install, upgrade, or inspect system software or add-ons such as languages and licenses. **Note** Also includes permission to reload the system.
spokenname.modify	Create, modify, and delete spoken names for remote locations, remote users, and public distribution lists. Copy spoken names.
system.application	Configure system applications, such as voice mail, auto-attendant, Prompt Management, and so on.
system.backup	Configure backup.
system.calendar	Create, modify, and delete system schedules and holidays.
system.configuration	Configure system settings such as the clock, hostname, domain name, default language, and interfaces (counters).
system.debug	Collect and configure trace and debug data. Includes copying data like core and log files.
system.documents	Manage tiff, general, and template documents.
system.numbers	Create, modify, and delete call-in numbers for voice mail, AA, AvT, and IVR. This includes SIP, JTAPI, and HTTP triggers.

Operation	Description
system.sessions	Terminate others voice mail sessions (VVE, SIP, or JTAPI). Unlock locked mailboxes.
system.view	View system settings and configuration.
user.configuration	Create, modify, and delete users and groups, including the configuration of: • First and Last Name • Nickname • Display Name • Language
user.mailbox	Create, modify, and delete a user or group voice mailbox.
user.notification	Set or change others notification/cascade profiles.
user.password	Create, set, or remove others passwords.
user.pin	Create, set, or remove others pins.
user.remote	Create, modify, and delete remote users.
voicemail.configuration	Configure system-level voice-mail features: • Mailboxes • Fax • Notification/cascade • Non-subscriber options • Broadcast • TUI config • Live-record • Live-reply • IMAP • VVE
voicemail.imap.user	Manage personal voice mail via IMAP client.
voicemail.mwi	Reset/Refresh phone message waiting indicators. Configure SIP MWI delivery.
voicemail.lists.public	Create, modify, and delete public voice mail distribution lists.
voicemail.lists.private.view	(GUI Only) View others private voice mail lists.
webapp.modify	Deploy web applications on Cisco Unity Express.

Operation	Description
webapp.control	Start, stop, or restart web applications.

Create a New Privilege

Use this procedure to create a new privilege and or specify which operations are included in it.

Step 1 Choose Configure > Privileges. The Privileges Configuration window appears.
Step 2 Click Add.
Step 3 Enter a name and description for the privilege.
Step 4 Select the operations that you want to add to the privilege.
Step 5 Click **Add**.
Step 6 Click **Ok** to save your changes.

Customize an Existing Privilege

Use this procedure to change or display which operations are included a privilege.

Step 1 Choose Configure Privileges. The Privileges Configuration window appears.
Step 2 Select the privilege that you want to customize.

You might have to change the number of rows per page or select a different page to see the privilege that you want to change.

Step 3 Select the operations that you want to add to the privilege or deselect the operations that you want to remove.

Note Some operations are mandatory and cannot be removed.

Step 4 Click **Apply.**
Step 5 Click **Ok** to save your changes.

Delete a Privilege

Use this procedure to delete a privilege.

Step 1 Choose Configure Privileges. The Privileges Configuration window appears.
Step 2 Select the privilege that you want to delete.
Step 3 Click **Delete**.

Step 4 Click **Ok** to save your changes.

CHAPTER 9

Configure Authentication, Authorization, and Accounting

Configure the AAA Authentication Server

The two procedures for configuring AAA authentication consist of:

- Configure connection parameters for the AAA authentication server
- Configure whether the authentication servers or local authentication database will be queried first

Note To help protect the cryptographic information of the RADIUS server, you must view the running configuration to see this information.

About the Authentication Order

The AAA policy specifies the failover functionality that you can optionally configure for the authentication server. You can use these two types of failover functionality separately or in combination:

- Authentication failover
- Unreachable failover

About Authentication Failover

The authentication failover feature enables you to optionally use a remote RADIUS server for user login authentication, in addition to the local database. The procedure in this section configures the order in which authentication is resolved. You can configure authentication to use:

- The local database only

- The remote server only
- The local database first, then the remote server
- The remote server first, then the local database

When using both local and remote authentication, you can also configure whether you want the user attributes that are retrieved from a remote RADIUS AAA server to be merged with the attributes found in the local user database for the same username.

The authentication failover feature has the following limitations:

- Authentication with a RADIUS server is available only when accessing the GUI or CLI interface and requires only a user ID and password. Authentication for the TUI, VVE, AvT, and IMAP interfaces can use only the local database. Therefore, to gain access, users of the TUI, VVE, AvT, and IMAP interfaces must be configured locally. The auto-attendant interface does not require authentication because it is user independent.
- Login information is not synchronized between the local system and the remote server. Therefore:
    - Any security features such, as password expiration, must be configured separately for Cisco Unity Express and the RADIUS server.
    - Cisco Unity Express users are not prompted when security events, such as password expiration or account lockout, occur on the RADIUS server.
    - RADIUS server users are not prompted when security events, such as password expiration or account lockout, occur on Cisco Unity Express.

Unreachable Failover

The Unreachable Failover feature is used only with RADIUS servers. This feature enables you to configure up to two addresses that can be used to access RADIUS servers.

As Cisco Unity Express attempts to authenticate a user with the RADIUS servers, the system sends messages to users to notify them when a RADIUS server either cannot be reached or fails to authenticate the user.

Example of Authentication Sequence

In this example, authentication is performed by the remote server first, then by the local database. Also, two addresses are configured for the remote RADIUS server.

This sequence of events could occur during authentication for this example:

1. Cisco Unity Express tries to contact the first remote RADIUS server.
2. If the first RADIUS server does not respond or does not accept the authentication credentials of the user, Cisco Unity Express tries to contact the second remote RADIUS server.
3. If the second RADIUS server does not respond or does not accept the authentication credentials of the user, the user receives the appropriate error message and Cisco Unity Express tries to contact the local database.
4. If the local database does not accept the authentication credentials of the user, the user receives an error message.

Configure Connection Parameters for the AAA Authentication Server

Step 1 Choose Configure > AAA > Authentication.

The system displays the AAA Authentication Server Configuration windowConfigure AAA Authentication page.

Step 2 Enter the following information in the appropriate fields for the primary server, and optionally, for the secondary server:

- Server IP address or DNS name
- Port number used
- Cryptographic shared secret and security credentials
- Authentication order Number of login retries
- Length of login timeout

Step 3 Hostname Port Password Click **Apply**.

Step 4 Click **OK** to save your changes.

Specify the Policy that Controls the Behavior of Authentication and Authorization

Use this procedure to configure the information used to log into the authentication server.

Step 1 Choose Configure > AAA > Authorization.

The system displays the Configure AAA Authorization Server Configuration window page.

Step 2 Select or deselect whether you want to merge the attributes of the remote AAA server with the attributes in the local database.

Step 3 Click **Apply**.

Step 4 Click **OK** to save your changes.

Configure the AAA Accounting Server

Overview

You can configure up to two AAA accounting servers. Automatic failover functionality is provided if you have two accounting servers configured. If the first server is unreachable, the accounting information is sent to the second server. If both accounting servers are unreachable, accounting records are cached until a server becomes available. If a server cannot be reached before the cache is full, the oldest accounting packets are dropped to make room for the new packets.

Because the configuration of the AAA accounting server is completely independent of the AAA authentication server, you can configure the AAA accounting server to be on the same or different machine from the AAA authentication server.

If you use a syslog server, it is not affected by the AAA configuration and continues to use the existing user interfaces. When the RADIUS server sends AAA accounting information to a syslog server, it is normalized into a single string before being recorded. If no syslog server is defined, the AAA accounting logs are recorded by the syslog server running locally on Cisco Unity Express.

Note Only RADIUS servers are supported.

AAA Accounting Event Logging

AAA accounting logs contain information that enables you to easily:

- Audit configuration changes.
- Maintain security.
- Accurately allocate resources.
- Determine who should be billed for the use of resources.

You can configure AAA accounting to log the following types of events:

- Logins—All forms of system access except IMAP, including access to the CLI, GUI, TUI, and VVE, when a login is required.
- Logouts—All forms of system access except IMAP, including access to the CLI, GUI, TUI, and VVE, when a login is required before logout.
- Failed logins—Failed login attempts for all forms of system access except IMAP, including access to the CLI, GUI, TUI, and VVE, when a login is required.
- Configuration mode commands—Any changes made to the Cisco Unity Express configuration using any interface except IMAP (CLI, GUI, TUI, and VVE).
- EXEC mode commands—Any commands entered in Cisco Unity Express EXEC mode using any interface except IMAP (CLI, GUI, TUI, and VVE).
- System startups—System startups, which include information about the system’s software version, installed licenses, installed packages, installed languages, and so on.
- System shutdowns—System shutdowns, which include information about the system’s software version, installed licenses, installed packages, installed languages, and so on.
- IMAP—Access to the IMAP system.

In addition to information specific to the type of action performed, the accounting logs also indicate the following:

- User that authored the action

- Time when the action was executed
- Time when the accounting record was sent to the server

Note Account logging is not performed during the system power-up playback of the startup configuration. When the system boots up, the startup-config commands are not recorded.

Configure the AAA Accounting Server

Use this procedure to configure the information used to log into the accounting server.

Step 1 Choose Configure > AAA > Accounting.

The AAA Accounting Server Configuration window appears.

Step 2 Click **Accounting Enabled**.

Step 3 Enter the following information in the appropriate field for the primary server, and optionally, for the secondary server:

- Server IP address or DNS name
- Port number used
- Cryptographic shared secret and security credentials
- Number of login retries
- Length of login timeout

Step 4 Click **Apply**.

Step 5 Click **OK** to save your changes.

Configure Accounting Event Logging

Use this procedure to configure which event types to log for AAA accounting.

Step 1 Choose Configure > AAA > Accounting.

The system displays the Accounting Server Configuration window.

Step 2 Select the log events that you want to include in the log and deselect those you do not want to include.

Step 3 Click **Apply** to save your changes.

CHAPTER 10

Configure Network Locations

View List of Network Locations

Use this procedure to view a list of network locations.

Step 1 Choose **Configure** > **Network Locations**. The Configure Network Locations window appears.

Step 2 The local location ID is displayed first. One of the network locations must be entered in this field to enable networking. To display or modify the local location configuration, click **View Location Profile** next to the Local Location ID. If no Local Location ID is listed, see Add a Network Location, on page 45.

Step 3 A list of locations is displayed with the following fields:

- Location ID
- Location name
- Abbreviation—Alphanumeric abbreviation for the location that is spelled to a user (if there is no spoken name) when the user performs addressing functions in the telephone user interface.
- Domain Name—Email domain name or IP address for the location. This information is added when sending a VPIM message to the remote location (for example, “4843000@cisco.com”). A domain name or IP address must be configured or networking is disabled at this location.

Step 4 If no Local Location ID is listed, proceed to Display or Modify a Network Location, on page 47 to create a new one.

Add a Network Location

Use this procedure to add a network location.

Step 1 Choose **Configure** > **Network Locations**. The Configure Network Locations window appears.

Step 2 Click **Add**. The Add a New Location window appears

Step 3 Enter information into the following fields:

- Location ID
- Location name
- Abbreviation—Alphanumeric abbreviation for the location that is spelled to a user (if there is no spoken name) when the user performs addressing functions in the telephone user interface.
- Domain Name/IP Address—Email domain name or IP address for the location. This information is added when sending a Voice Profile for Internet Mail (VPIM) message to the remote location (for example, “4843000@cisco.com”). A domain name or IP address must be configured or networking is disabled at this location.
- Phone Prefix—Prefix that is added to an extension to create a VPIM address for a user at the location. A prefix is required only if an email domain services multiple locations, and extensions between the locations are not unique. Valid values: 1 to 15 digits.
- VPIM Broadcast ID—You must enter a VPIM broadcast ID to enable sending and receiving of broadcast messages. The default value, “vpim-broadcast,” can be used for remote locations that have unique domain names. If more than one of the remote locations has the same domain name, you must enter a unique ID for each of those locations. For remote locations that are networked to a Cisco Unity system, enter a numeric VPIM broadcast ID that is compatible with the Cisco Unity system. To send broadcast messages from Cisco Unity to Cisco Unity Express, the VPIM ID must match on both systems.
- Calling Number Rule Prefix Digits—Any digits are supplied to this command are prepended to the E.164 phone number derived using the calling-number-rule before dialing the digits for a live-reply to a network delivered voice-mail message.
- Minimum Extension Length (required)—Minimum number of digits for extensions at the remote location. Valid values are 2 to 15; default is 2.
- Maximum Extension Length (required)—Maximum number of digits for extensions at the remote location. Valid values are 2 to 15; default is 15.
- Voicemail Encoding—Configures the encoding method used to transfer voice-mail messages from this location. You can select one of the following:
    - **Dynamic**—Cisco Unity Express negotiates with the receiving location to determine the encoding method
    - **G711ulaw**—Cisco Unity Express always sends messages as G711ulaw .wav files. Set this only if the receiving system supports G711 ulaw encoding (such as Cisco Unity).
    - **G726**—Cisco Unity Express always sends messages as G726 (32K ADPCM). Use for low-bandwidth connections or when the system to which Cisco Unity Express is connecting does not support G711ulaw
- Send Spoken Name—Enables sending the spoken name of the voice-mail originator as part of the message that is sent to the remote location. If the spoken name is sent, it is played as the first part of the received message.
- Send vCard Information—Enables sending vCard information in VPIM messages. User information from the vCard is added to the remote user directory cache (called the least recently used [LRU] cache). The LRU cache is updated with user information (such as the user's first and last name) whenever new vCards are received. The cache is used to provide addressing confirmation.

- Enabled—Indicates networking is enabled for this location. Check the box to enable networking, or uncheck it to disable networking.
- Enable Secure Messages—Indicates secure messaging is enabled for this location.

Step 4 Click **Add**. The Network Locations window reappears with the new location added.

Display or Modify a Network Location

Use this procedures to display or modify network locations, including configuring the local location ID:

Configure the Local Location ID

Step 1 Choose **Configure** > **Network Locations**. The Configure Network Locations window appears.

Step 2 To configure the local location ID, enter the location ID number. You must designate one of your network locations as the local location and enter it in this field to enable networking.

Step 3 Click **Apply**.

Step 4 Click **Ok** at the information prompt.

Display or Modify Locations

Step 1 Choose **Configure** > **Network Locations**. The Configure Network Locations window appears.

Step 2 To display or modify the local location configuration, click **View Location Profile** next to the Local Location ID. To display or modify a remote location configuration, click its location ID in the list of locations.

Step 3 The Location Profile window appears with the following fields:

- Location ID
- Location name
- Abbreviation—Alphanumeric abbreviation for the location that is spelled to a user (if there is no spoken name) when the user performs addressing functions in the telephone user interface.
- Domain Name/IP Address—Email domain name or IP address for the location. This information is added when sending a Voice Profile for Internet Mail (VPIM) message to the remote location (for example, “4843000@cisco.com”). A domain name or IP address must be configured or networking is disabled at this location.
- Phone Prefix—Prefix that is added to an extension to create a VPIM address for a user at the location. A prefix is required only if an email domain services multiple locations, and extensions between the locations are not unique. Valid values: 1 to 15 digits.
- VPIM Broadcast ID—You must enter a VPIM broadcast ID to enable sending and receiving of broadcast messages. The default value, “vpim-broadcast,” can be used for remote locations that have unique domain names. If more than one of the remote locations has the same domain name, you must enter a unique ID for each of those locations. For

remote locations that are networked to a Cisco Unity system, enter a numeric VPIM broadcast ID that is compatible with the Cisco Unity system. To send broadcast messages from Cisco Unity to Cisco Unity Express, the VPIM ID must match on both systems.

- Calling Number Rule Prefix Digits—Any digits are supplied to this command will be prepended to the E.164 phone number derived using the calling-number-rule before dialing the digits for a live-reply to a network delivered voice-mail message.
- Minimum Extension Length—Minimum number of digits for extensions at the remote location. Valid values are 2 to 15; the default value is 2.
- Maximum Extension Length—Maximum number of digits for extensions at the remote location. Valid values are 2 to 15; the default value is 15.
- Voicemail encoding—Configures the encoding method used to transfer voice-mail messages from this location. You can select one of the following:
    - **Dynamic**—Cisco Unity Express negotiates with the receiving location to determine the encoding method
    - **G711ulaw**—Cisco Unity Express always sends messages as G711ulaw .wav files. Set this only if the receiving system supports G711 ulaw encoding (such as Cisco Unity).
    - **G726**—Cisco Unity Express always sends messages as G726 (32K ADPCM). Use for low-bandwidth connections or when the system to which Cisco Unity Express is connecting does not support G711ulaw
- Send Spoken Name—Enables sending the spoken name of the voice-mail originator as part of the message that is sent to the remote location. If the spoken name is sent, it is played as the first part of the received message.
- Send vCard Information—Enables sending vCard information in VPIM messages. User information from the vCard is added to the remote user directory cache (called the least recently used [LRU] cache). The LRU cache is updated with user information (such as the user's first and last name) whenever new vCards are received. The cache is used to provide addressing confirmation.
- Enabled—Indicates networking is enabled for this location. Check the box to enable networking, or uncheck it to disable networking.
- Enable Secure Messages—Indicates secure messaging is enabled for this location.

Step 4 After making any changes, click **Save**.

Step 5 Click **Ok** at the information prompt.

Delete a Network Location

Use this procedure to delete a network location from Cisco Unity Express.

Caution Deleting a location disables networking to and from that location. Deleting the location designated as the local location disables networking for the entire Cisco Unity Express system. If you delete the location designated as the local location, you must add a new network location and designate it as the local location to reenable networking.

Step 1 Choose **Configure** > **Network Locations**. The Configure Network Locations window appears.

Step 2 Click the box next to the location ID of the location that you want to delete and click Delete.

Step 3 At the prompt, click **Ok** to delete the location.

CHAPTER 11

Configure Remote Users

View List of Remote Users

Use this procedure to view a list of users at remote locations.

> **Note** You must have at least one remote network location configured before you can add, modify, or view a list of remote users. See Configure Network Locations, on page 45 for more information.

Choose Configure > Remote Users. The Configure Remote Users window appears and contains the following fields:

- User ID—By default, the system displays users in alphabetical order by user ID. To sort from A to Z, click User ID.
- Display Name—To display the list of users in order by display name, click Display Name.
- Location ID—To display the list of users in order by Location ID, click Location ID.
- Primary Extension—To display the list of users in order by primary extension, click Primary Extension.
- Use the dialog box to change the number of rows displayed per window.

Add a New Remote User

Use this procedure to add a new remote user to the system directory. Remote users are users whose voice mailboxes are located at a remote network location. Remote users who are added to the system directory can be reached using the dial-by-name feature, and senders receive address and spoken name confirmation when sending messages to remote users.

> **Note** The system administrator can record a spoken name for remote users using the Administration via Telephone (AvT) interface. Spoken name information is also retrieved from the Voice Profile for Internet Mail (VPIM) messages received by the system from the remote user and the system directory is updated accordingly.

The number of users supported depends on the Cisco Unity Express module being used. See the Cisco Unity Express Release Notes for detailed support information.

> **Note** You must add the remote user's location before adding the remote user to the system.

Step 1 Choose Configure > Remote Users. The Configure Remote Users window appears.

Step 2 Click Add. The Add a New Remote User window appears.

Step 3 Enter information into the following fields:

- User ID
- First Name and Last Name
- Display Name
- Primary Extension
- Location: Choose one of the following to identify the location:
  - Location ID
  - Abbreviation—Alphanumeric abbreviation for the location.

Step 4 To save the information, click Add.

Display or Modify a Remote User

Use this procedure to display or modify the profile of a remote user in the system directory. Remote users are users whose voice mailboxes are located at a remote network location. Remote users who are added to the system directory can be reached using the dial-by-name feature, and senders receive address and spoken name confirmation when sending messages to remote users.

> **Note** The system administrator can record a spoken name for remote users using the Administration via Telephone (AvT) interface. Spoken name information is also retrieved from the VPIM messages received by the system from the remote user and the system directory is updated accordingly.

The number of users supported depends on the Cisco Unity Express module being used. See the Cisco Unity Express Release Notes for further support information.

Step 1 Choose Configure > Remote Users. The Configure Remote Users window appears.

Step 2 Click the name of the remote user whose profile you want to view. The Remote User Profile Window appears with the following fields shown that you can change:

- First Name and Last Name
- Display Name
- Primary Extension
- Location: Choose one of the following to identify the location:
    - Location ID
    - Abbreviation—Alphanumeric abbreviation for the location.

Step 3 After making any changes, click Apply.

Step 4 Click Ok at the information prompt.

Delete a Remote User

Use this procedure to delete a remote user from the system directory.

Step 1 Choose Configure > Remote Users. The Configure Remote Users window appears.

Step 2 Check the box next to the user ID that you want to delete.

Step 3 Click Delete.

Step 4 Click Ok to confirm the deletion.

CHAPTER 12

Configure the Cisco Unified Communications Manager System

Use this procedure to modi fy the Java Telephony API (JTAPI) provider (on Cisco Unified Communications Manager) information in Cisco Unity Express.

Note Any changes to the JTAPI provider on Cisco Unified Communications Manager require a software reload of Cisco Unity Express. You must save your Cisco Unity Express configuration and reload for the changes to take effect.

Use this procedure to configu re the Cisco Unified Communications Manager (CUCM).

Step 1 Choose **Configure** > **Communications Manager**. The Configure CUCM window appears.

Step 2 Enter the information in the following fields:

- Primary Communications Manager—IP address or hostname of the primary Cisco Unified Communications Manager system.
- Secondary Communications Manager—IP address or hostname of the first alternate Cisco Communications Manager system.
- Tertiary Communications Manager—IP address or hostname of the second alternate Cisco Unified Communications Manager system.
- Web User Name—Username to log in to the Cisco Unified Communications Manager system.
- Web Password—Password to log in to the Cisco Unified Communications Manager system.
- JTAPI user ID and password

Step 3 Click **Apply** to save the information.

Step 4 Click **Verify** to test the connection between Cisco Unified Communications Manager and Cisco Unity Express.

Step 5 Click **Reload Unity Express** to reload the software after you make configuration changes.

CHAPTER 13

Configure Voice-Mail Prompts

Caution: This section is for advanced users.

View List of Prompts

Use this procedure to view a list of voice-mail prompts.

Step 1 Choose **System** > **Prompts**. The System Prompts window appears and displays the following fields:

- Prompt Name—Filename of the prompt. To sort the table by prompt name, click **Prompt Name**.
- Creation Date—Date on which the .wav file was created. To sort the table by creation date, click **Creation Date**.
- Size (Bytes)—Size, in bytes, of the prompt file. To sort the table by size in bytes, click **Size (Bytes)**.
- Length (Seconds)—Length, in seconds, of the prompt file. To sort the table by length in seconds, click **Length (Seconds)**.
- To increase the number of rows shown on the page, click **Rows by Page** and choose the number you want to show.

Step 2 From the Languages list, select the Language for the Cisco Unity Express prompts. The Prompts window refreshes and displays all of the prompts available for the language you selected.

Display or Modify a Prompt

Use this procedure to dis play or modify a voice-mail prompt.

Step 1 Choose **System** > **Prompts**. The System Prompts window appears.

Step 2 Click the name of the prompt you want to display or modify. The Prompt Profile window appears. You can edit the prompt filename only.

Step 3 After editing, click **Apply**.

Step 4 Click **Ok** to save your changes.

Upload a Prompt

Use this procedure to upload new voice-mail prompts.

Step 1 Choose **System** > **Prompts**. The System Prompts window appears.

Step 2 Click **Upload**. See also Configure Auto-Attendant Script Parameters, on page 116.

Step 3 Enter information in the following fields:

- Language
- Source File Name—path to the file you want to upload. Click the **Browse** button to help you find the directory with the file you want to upload.
- Destination File Name—Enter the same filename as shown in the Source Filename field or a new filename for the prompt. This file should be in .wav format.
- Click to overwrite the destination file, if it exists.

Step 4 Click **Upload** to save your changes.

Download a Prompt

Use this procedure to download a prompt.

Step 1 Choose **System** > **Prompts**. The System Prompts window appears.

Step 2 Check the box next to the prompt that you want to download.

Step 3 Click **Download**. The File Download window appears.

Step 4 In the File Download window, click **Open** and select an application on your computer, or click **Save** to save the file to your computer.

Step 5 In the Save As window, navigate to the folder where you want to save the file and click **Save**.

Delete a Prompt

Use this procedure to delete a prompt.

Step 1 Choose System > Prompts. The System Prompts window appears.

Step 2 Click the box next to the prompt that you want to delete.

Step 3 Click Delete.

Step 4 Click Ok to confirm the deletion.

Change Prompt Languages

Use this procedure to change the language of voice-mail prompts.

Step 1 Choose **System** > **Prompts**. The System Prompts window appears.

Step 2 From the Languages list, select the language for the Cisco Unity Express prompts. The Prompts window refreshes and displays all of the prompts available for the language you selected.

CHAPTER 14

Configure System Scripts Using Editor Express

View List of Scripts

Use this procedure to view a list of scripts. For more information on Cisco Unity Express scripts, see the Cisco Unity Express Maintain and Operate Guides at the following URL: http://www.cisco.com/en/US/products/sw/voicesw/ps5520/prod_maintenance_guides_list.html.

Step 1 Choose **System** > **Scripts**. The window displays a list of non-system scripts, showing the following fields:

- Script Name—Filename of the script. To sort the table by script name, click **Script Name**.
- Type—AA or IVR.
- Creation Date—Date on which the script file was created. This information is read from the script file properties. To sort the table by creation date, click **Creation Date**.
- Last Modified Date—Date on which the script was last modified. This information is read from the script file properties. To sort the table by the date last modified, click **Last Modified Date**.
- Size (Bytes)—Size of the script. This information is read from the script file properties. To sort the table by size in bytes, click **Size (Bytes)**.

To increase the number of rows shown on the page, click **Rows per Page** and choose the number you want to show.

Step 2 Click on **Show system scripts** to display the system scripts.

Note System scripts are indicated with an asterisk and cannot be modified or deleted. Scripts that you create do not have an asterisk and can be edited. See #unique_91 for more information.

Step 3 Click on **Hide system scripts** to hide the system scripts.

Create a New Script with Editor Express

Configure Settings for a New Script

Use this procedure to configure settings for a new script.

Step 1 Choose **System** > **Scripts** > **New**. The Editor Express window opens with an untitled.aef (unsaved) script.

Step 2 Configure the new script settings by selecting any combination of the following options:

a) Click the box to allow dial-by-extension at any time during the main menu.
b) Click the box to allow menu options to overlap with the extension dial-plan.
c) Enter the desired extension length.
d) Click the box to allow external transfers.
e) If your system supports multiple languages, click the box to enable the Language selection menu. If selected, the language selection menu displays in the Call Flow window.
f) Click the box to enable an alternate main menu for business closed hours. If selected, the Business Closed Menu options display in the Call Flow window.

Step 3 Click **Save**. A pop-up window appears prompting you to enter a script name.

Step 4 Enter a script name and save the file (an .aef extension is automatically added if you save the file).

Step 5 Click **Ok** to save your settings or click **Cancel**.

Proceed to the next section for Configure the Call Flow for a Script, on page 62 .

Configure the Call Flow for a Script

Use this procedure to configure the call flow from the **Editor Express** window.

Step 1 Choose **System** > **Scripts** > **New or select an existing script by clicking the Edit button**. The Editor Express window opens.

Step 2 Click the box to play the alternate (emergency) greeting.

Step 3 Choose an audio prompt file from the drop-down menu for the following prompts:

- Welcome prompt
- Language Menu prompt

  Select the prompt from the drop-down menu and click Add/ Remove Choice >>>. In the Add Language Choice window, select the key and assign it to a language. Click Ok. Repeat for each key to be assigned a language. To remove the language from a key, select the key and select Clear choice and click Ok.

  Note The maximum number of languages allowed is three. Only installed languages are displayed.

- Holiday prompt
- Business schedule: select a Business Schedule name from the drop-down menu.

- Business open prompt
- Business closed prompt

Step 4 Configure the actions for the following menus:

- Main Menu
- Business Closed Menu

a. Select the prompt to be used for each menu.

b. Assign additional keys and menu actions by clicking **Add Action**. The **Add Menu Action** window appears.

c. Select the **Key** from the drop-down list to assign a **Key** to an **Action**. You can choose the numbers 0-9, the “*” symbol, or the “#” symbol.

d. Select the **action** from the drop-down list to assign an **action** to the **key**. You can choose from one of the following actions:

- Play message
- Dial-by-name
- Dial-by-extension
- Transfer to extension
- Transfer to mail box number
- Sub-menu. You can add another action from this level.
- Disconnect call

Click **Ok** to save your settings or **Cancel**. The action is added to the script. Configure the additional settings for each action. See Table 3: Main Menu Prompt and Goodbye Prompt Actions, on page 64 for more information.

Continue to add menu actions by clicking the Add Action button and repeating this step. To remove an action from the menu, click Delete.

Step 5 Configure the **Good-bye** prompt.

a) Select the Good bye prompt name from the drop-down menu.
b) Click **Add action**. The **Add Good-bye Action** window appears.
c) Select the **action** from the drop-down list. You can choose one of the following actions:

- Transfer to extension
- Transfer to mail box number

See Table 3: Main Menu Prompt and Goodbye Prompt Actions, on page 64 for more information.

d) Click **Ok** to save your settings or **Cancel**. The action is added.

Step 6 Click **Save to save your script**.

Table 3: Main Menu Prompt and Goodbye Prompt Actions, on page 64 lists the Main Menu prompt and Goodbye prompt actions.

Table 3: Main Menu Prompt and Goodbye Prompt Actions

Action	Supported for:	Instructions for Setting Action
Play Prompt	Main Menu prompt	**a.** Select the prompt audio file from the drop-down menu. then **a.** Select one of the following options: • Repeat Main Menu • Disconnect Call
Dial By Name	Main Menu prompt	Select the search style: • First - Last Name • Last - First Name
Dial By Extension	Main Menu prompt	None.
Transfer to Extension	Main Men> Main Menu prompt Goodbye prompt	Enter the mailbox number subscribers will be transferred to.
Sub-Menu	Main Menu prompt	**a.** Select the prompt audio file from the drop-down menu. **b.** Add actions for the sub-menu.
Disconnect Call	Main Menu prompt	None.

Upload a New Prompt

Use this procedure to upload a new prompt from the **Editor Express** window.

Step 1 Choose **System** > **Scripts** > **New**. The Editor Express window appears.

Step 2 Click **Upload Prompt**. The **Upload** window appears.

Step 3 In the **Upload** dialog box, perform the following tasks:

a) Choose the language.
b) Enter the source filename, or path to the file you want to upload. Click the **Browse** button to help you find the directory with the file you want to upload.
c) Enter the destination filename (required). Enter the same filename as shown in the Source Filename field or a new filename for the prompt.

d) Click the box to overwrite the destination file, if desired, if the file already exists.

Step 4 Click **Upload** to save your changes.

Show/Hide Settings

You can choose to show or hide the Call Flow window by clicking on **Show/Hide Settings**.

Close Editor Express

To close the Editor Express window, click Close.

Upload a New Script

Use this procedure to upload a new script.

Step 1 Choose **System** > **Scripts**. The System Scripts window appears.

Step 2 Click **Upload**. The **Upload** window appears.

Step 3 In the **Upload** dialog box, perform the following tasks:

a) Enter the source filename, or path to the file you want to upload. Click the **Browse** button to help you find the directory with the file you want to upload.

b) Enter the destination filename (required). Enter the same filename as shown in the **Source File**name field or a new filename for the script.

c) Click the box to overwrite the destination file, if the file already exists.

Step 4 Click**Upload** to save your changes.

Edit Scripts

Only scripts that are created with **Editor Express** may be edited using the Web GUI interface in the browser window. These scripts appear in the System Scripts table with an **Edit** button next to the script name. Scripts created with the windows Cisco Unity Express editor are only editable on the windows editor and do not have an **Edit** button next to the script name.

Use this procedure to edit scripts.

Step 1 Choose **System** > **Scripts**. The System Scripts window appears.

Step 2 In the Script Name field, edit an existing script (the **Edit** button is present) by clicking the **Edit** button. The **Editor Express** window appears.

Step 3 Follow the procedures to configure **Editor Express** in Create a New Script with Editor Express, on page 62.

Step 4 Click **Save** to save your settings.

Delete Scripts

Use this procedure to delete a script.

Step 1 Choose **System** > **Scripts**. The System Scripts window appears.
Step 2 Select at least one entry to delete from the **Script Name** table.
Step 3 Click **Delete**.
Step 4 Click **Ok** or **Cancel** to complete the task.

Download Scripts

Use this procedure to download new scripts.

Step 1 Choose **System** > **Scripts**. The System Scripts window appears.
Step 2 Select the script that you want to download from list and click **Download**. Your system download window appears. You can save the file to disk or download the file using the default application.

CHAPTER 15

Configure Business Hours Settings

Display or Modify a Business Hours Schedule

Use this procedure to display or modify a business hours schedule.

Step 1 Choose **System** > **Business Hours Settings**. The System Business Hours window appears.

Step 2 Choose the Business Hours schedule you want to view or modify from the drop-down list.

Step 3 Click the box for each half-hour increment to check or uncheck it. A gray box indicates that the business is closed during that time period. A checked box indicates that the business is open.

Step 4 Click **Apply** to save your changes.

Add a Business Hours Schedule

Use this procedure to create a Business hours schedule.

Step 1 Choose **System** > **Business Hours Settings**. The System Business Hours window appears.

Step 2 Choose the Business Hours schedule you want to modify from the drop-down list, or, if you do not have a business hours schedule, click **Add** to create one.

Step 3 Click the box for each half-hour increment to check or uncheck it. A gray box indicates that the business is closed during that time period. A checked box indicates that the business is open.

Step 4 Click **Apply** to save your changes.

Copy Business Hour Days

Copy the business hours schedule from one day to another day, or range of days. For example, if you have a business that is open Monday through Friday for the same hours, you can configure first the hours for Monday, and copy Monday's schedule to all weekdays.

Use this procedure to copy the business hours schedule for a day.

Step 1 Choose **System** > **Business Hours Settings**. The System Business Hours window appears.

Step 2 Configure the day you want to copy and choose it from the drop-down list at the bottom of the Business Hours Settings window.

Step 3 Choose either the day to which you want to copy the configured schedule, or one of the following from the drop-down list on the right:

- **All weekdays**—copies the schedule for the configured day to all weekdays.
- **Weekend**—copies the schedule for the configured day to all weekend days.

Tip For a business that is open regular business hours on Monday through Friday, configure Monday's hours and copy Monday's hours to all weekdays, then configure Saturday's hours, and copy to Sunday.

Step 4 Click **Copy Schedule**.

Step 5 Click **Apply** to save your changes.

Delete a Business Hours Schedule

Use this procedure to delete a Business hours schedule.

Step 1 Choose **System** > **Business Hours Settings**. The System Business Hours window appears.

Step 2 Choose the schedule that you want to delete from the Business Hours Schedule drop-down list.

Step 3 Click **Delete**.

Step 4 Click **Ok** at the information prompt.

CHAPTER 16

Configure Holiday Settings

View List of Holidays

Use this procedure to view a list of Holidays.

Step 1 Choose **System** > **Holiday Settings**. The holiday settings for the current year are displayed. If no holidays are configured, proceed to Add a Holiday, on page 69.

Step 2 Choose the year for which you want to display the list of holidays from the drop-down list, or choose All Holidays to display all years.

Step 3 The list of holidays shows the date and description of each holiday.

Add a Holiday

Add Fixed Holidays

Fixed holidays are holidays that occur on the same date every year, such as New Year's Day or Christmas. Fixed holidays are automatically added to future years. Use this procedure to add fixed holidays.

Step 1 Choose **System** > **Holiday Settings**.

Step 2 Select **Fixed Holidays** from the drop-down list. The Add a New Holiday screen displays.

Step 3 Select the date by clicking on the calendar icon.

Step 4 Enter the holiday description (for example, “New Year's Eve”). This field is optional.

Step 5 Click **Add**.

Add Regular Holidays

Regular holidays are holidays that occur on a different date each year. Use this procedure to add regular holidays.

Step 1 Choose **System** > **Holiday Settings**.

Step 2 Choose the year for which you want to add holiday settings from the drop-down list. The Add a New Holiday screen displays.

Note You can add holidays only for the current year and next year.

Step 3 Select the date by clicking on the calendar icon.

Step 4 Enter the holiday description (for example, “New Year's Eve”). This field is optional.

Step 5 Click **Add**.

Copy Holidays

To copy a holiday from one calendar year to another, configure holidays for the year and choose **Copy All to Next Year**.

Display or Modify a Holiday

Use this procedure to display or modify Holidays.

Step 1 Choose **System** > **Holiday Settings**. The holiday settings for the current year are displayed.

Step 2 Choose the year for which you want to display or modify holidays from the drop-down list, or choose **All Holidays** to display all years.

Step 3 Click the holiday to edit the description.

Step 4 Click **Save** to save the changes.

Step 5 Click **Ok** at the information prompt.

Tip To change the date of a holiday, you must delete it and add it under the new date.

Copying Holidays

To copy a holiday from one calendar year to another, configure holidays for the year and choose **Copy All to Next Year**.

Delete a Holiday

Use this procedure to delete a holiday.

Step 1 Choose **System** > **Holiday Settings**.

Step 2 Choose the year for which you want to delete holidays from the drop-down list, or choose **All Holidays** to display all years.

Step 3 Check the box next to the holiday or holidays and click **Delete**.

Step 4 Click **Ok** at the information prompt.

CHAPTER 17

Configure Call-In Numbers

View List of Call-in Numbers

Use this procedure to view a list of the numbers that callers dial to reach system applications, such as voice mail, the auto attendant, and the Administration via Telephone (AvT) system.

Step 1 Choose **System** > **Call-in Numbers**.

Step 2 The window shows the configured call-in numbers with the fields shown below:

- Call-in Number—Extension that the caller dials to access a system application. These numbers can also be entered when configuring the auto attendant (see Configure Voice-Mail Call-Handling Parameters, on page 127) or configuring call-handling voice-mail parameters (see Configure Voice-Mail Call-Handling Parameters, on page 127).

You can also use wildcard trigger patterns when configuring call-in numbers (see Use Wildcard Trigger Patterns, on page 75).

- Application—Application reached when the call-in number is dialed. Valid values are any custom applications you have created, and the system defaults:
  - voicemail—Default voice-mail application.
  - autoattendant—Default auto attendant application.
  - promptmgmt—Default Administration via Telephone (AvT) application
- Enabled—Shows whether the application is enabled.
- Maximum Sessions
- Language

Display or Modify Call-in Numbers

Use this procedure to display or modify the numbers that callers dial to reach system applications, such as voice mail, the auto attendant, and the Administration via Telephone (AvT) system.

Step 1 Choose System > Call-in Numbers.

Step 2 Click the call-in number that you want to modify or view. The Call-in Number Profile window displays the following fields:

Step 3 To modify, edit the following fields:

- Call-in Number—Extension that the caller dials to access a system application. These numbers can also be entered when configuring the auto attendant (see Configure Voice-Mail Call-Handling Parameters, on page 127) or configuring call-handling voice-mail parameters (see Configure Voice-Mail Call-Handling Parameters, on page 127).

You can also use wildcard trigger patterns when configuring call-in numbers (see Use Wildcard Trigger Patterns, on page 75).

- Application—Application reached when the call-in number is dialed. Valid values are any custom applications you have created, and the system defaults:
  - voicemail—Default voice-mail application.
  - autoattendant—Default auto attendant application.
  - promptmgmt—Default Administration via Telephone (AvT) application
- Enabled—Shows whether the application is enabled.
- Maximum Sessions
- Language

Step 4 **Click Apply**.

Step 5 Click **Ok** to save.

Add a Call-in Number

Use this procedure to add a call-in number, or a number that callers dial to reach system applications. These applications include voice mail, the auto attendant, and the Administration via Telephone (AvT) system.

Step 1 Choose System > Call-in Numbers.

Step 2 Click Add.

Step 3 Enter the data in the following fields:

- Application—Application reached when the call-in number is dialed. Valid values are any custom applications you have created, and the system defaults:

- voicemail—Default voice mail application.
- autoattendant—Default auto attendant application.
- promptmgmt—Default Administration via Telephone (AvT) application.

- Call-in Number—Extension that the caller dials to access a system application. These numbers can also be entered when configuring the auto attendant (see Configure a Voice Mail Auto Attendant, on page 115) or configuring call-handling voice-mail parameters (see Configure Voice-Mail Call-Handling Parameters, on page 127).

You can also use wildcard trigger patterns when configuring call-in numbers (see Use Wildcard Trigger Patterns, on page 75).

- Maximum Sessions
- Enabled—Shows whether the application is enabled.
- Language

Step 4 Click **Add**.

Step 5 Click **Ok** to save.

Use Wildcard Trigger Patterns

You can configure a trigger to specify a number *pattern* instead of a single number. Incoming calls targeted to a number that matches the pattern cause the associated script to be invoked. The script determines which number was dialed by inspecting the called number attribute associated with the call. Cisco Unity Express supports a limit of 32 characters in the trigger pattern.

Wildcard patterns are based on Cisco Unified Communications Manager route patterns. The rules for choosing between multiple wildcard patterns matching an incoming call are similar to those used by Cisco Unified Communications Manager. For each pattern that is a candidate match for the dial string, Cisco Unity Express calculates the number of other dial strings of the same length as the input dial string that would match each pattern, and then selects the pattern that has the fewest alternative dial string matches.

Table 4: Trigger Pattern Wildcards and Special Characters, on page 75 shows the trigger pattern wildcards and special characters supported in Cisco Unity Express.

Table 4: Trigger Pattern Wildcards and Special Characters

Character	Description	Examples
X	The X wildcard matches any single digit in the range 0 through 9.	The trigger pattern 9XXX matches all numbers in the range 9000 through 9999.
!	The exclamation point (!) wildcard matches one or more digits in the range 0 through 9.	The trigger pattern 91! matches all numbers in the range 910 through 91999999999999999999999999999999.
?	The question mark (?) wildcard matches zero or more occurrences of the preceding digit or wildcard value.	The trigger pattern 91X? matches all numbers in the range 91 through 91999999999999999999999999999999.

Character	Description	Examples
+	The plus sign (+) wildcard matches one or more occurrences of the preceding digit or wildcard value.	The trigger pattern 91X+ matches all numbers in the range 910 through 9199999999999999999999999999999.
[ ]	The square bracket ([ ]) characters enclose a range of values.	The trigger pattern 813510[012345] matches all numbers in the range 8135100 through 8135105.
-	The hyphen (-) character, used with the square brackets, denotes a range of values.	The trigger pattern 813510[0-5] matches all numbers in the range 8135100 through 8135105.
^	The circumflex (^) character, used with the square brackets, negates a range of values. Ensure that it is the first character following the opening bracket ([). Each trigger pattern can have only one ^ character.	The trigger pattern 813510[^0-5] matches all numbers in the range 8135106 through 8135109.

CHAPTER 18

Configure CTI Ports for Cisco Unified Communications Manager

Use this procedure to import a new set of computer telephony integration (CTI ports) configured on Cisco Unified Communications Manager for use by Cisco Unity Express (in addition to the CTI ports already in use), or to remove or change CTI ports that are already in use. Typically you have one port for each application configured, such as voice mail, automated attendant, and the Administration via Telephone (AvT) system.

Step 1 Choose **System** > **CTI Ports**. The System CTI Ports window appears containing a list of CTI ports configured on Cisco Unity Express displays.

Step 2 To use a CTI port for Cisco Unity Express, leave the box next to it checked. To remove it from use by Cisco Unity Express, uncheck the box next to it. If you make changes, click Apply to save; unchecked ports will be deleted.

Step 3 To import all the CTI ports that are configured on the Cisco Unified Communications Manager associated with the current Java Telephony API (JTAPI) user, click Expand to also show available ports on Cisco Unified Communications Manager. A list of all CTI ports displays. To use a port for Cisco Unity Express, check the box next to the port and click Apply.

Note The maximum number of CTI ports that can be used concurrently by Cisco Unity Express depends on your user license.

CHAPTER 19

Configure Language Settings

Use this procedure to configure your language settings.

Step 1 Choose **System** > **Language Settings**.

Step 2 Select the System Default Language from the drop-down list.

Step 3 Click **Apply** to save your settings.

CHAPTER 20

Configure Fax Settings

Note The Cisco IOS gateways must be configured to handle fax calls.

Use this procedure to configure your fax settings.

Step 1 Choose **System** > **Fax Settings**. The System Fax Settings window appears.

Step 2 Enter the hostname for the outgoing Cisco IOS fax gateway. Fax printing is allowed only when the outgoing gateway is input.

Step 3 Enter a “From” e-mail address to use as the default. Use the format localhost@localdomain.com.

Step 4 Select the fax number restriction table from the drop-down list.

Note If no restriction tables are configured in the drop-down list, see Configure Restriction Tables, on page 89.

Step 5 Enter the fax printing number. Enter numbers without spaces, dashes, or parenthesis.

Note If multiple Sites (multiple Cisco Unified CMEs) are configured, a table will be present with a list of configured sites and their fax numbers that you can configure and modify.

Step 6 Enter the hostname for the incoming Cisco IOS fax gateway and click Add. Up to ten faxes/Cisco IOS gateways can be added.

Note If you omit the incoming gateway input, the receiving fax is automatically disabled on the system.

Step 7 Click **Apply** to save your settings.

CHAPTER 21

Configure Domain Name Settings

Perform the following tasks from the System Domain Name Settings page:

- Specify a domain and hostname in which Cisco Unity Express Cisco Unified SIP Proxy is located. See Change a DNS Server, on page 83.
- Add Domain Name Settings (DNS) servers. See Add a DNS Server, on page 84.
- Delete DNS servers. See Remove a DNS Server, on page 84.

Note After changing the domain name, you must reload the Cisco Unity Express software.

Change a DNS Server

Use this procedure to change one or both of the DNS servers if their names or IP addresses have changed since running the InitializationSetup Wizard.

Before you begin

Gather the following information:

- The hostname of Cisco Unity Expressthe Cisco Unified SIP Proxy system.
- The domain name and IP address of the DNS server.

Step 1 Choose **System** > **Domain Name Settings**.

The system displays the Domain Name Settings page.

Step 2 Change theEnter a hostname or domainthe name of the server that stores the Cisco Unity Express application files.

Step 3 Enter the hostname of Cisco Unity Express.

Step 4 Enter the domain name of the server. Click **Apply**.

Add a DNS Server

Enter additional DNS servers as alternate server destinations, to be used if the system cannot access the primary domain name server.

Restriction

You can have a maximum of four DNS servers.

Step 1 Choose **System** > **Domain Name Settings**.

The system displays the Domain Name Settings page.

Step 2 Click **Add** under Domain Name Service (DNS) Servers.

The system displays the Add a DNS server page.

Step 3 Enter the IP address of the server.

Step 4 Click **Add**.

Remove a DNS Server

Use this procedure to delete a DNS server.

Procedure

Step 1 Choose **System** > **Domain Name Settings**.

The system displays the Domain Name Settings page.

Step 2 Check the checkbox next to the DNS server that you want to delete.

Step 3 Click **Delete**.

Step 4 At the prompt, click **OK**.

What To Do Next Save and then reload the configuration. SeeUsing the Administration Control PanelSaving the Cisco Unified Messaging Gateway Configuration and Reloading the Cisco Unified Messaging Gateway Configuration. Related Topics Back to the Configure Domain Name Settings menu page

CHAPTER 22

Configure the System Login Banner

Use this procedure to configure your system login banner.

Step 1 Choose **System** > **Login Banner**. The Login Banner window appears.

Step 2 Enter the text for the login banner.

Step 3 Click **Apply** to save your settings.

CHAPTER 23

Configure Network Time and Time Zone Settings

Use these procedures to ensure that voice messages and system processes are identified with the correct day and time.

Before You Begin

These parameters are required to ensure that voice messages and system processes are identified with the correct day and time:

- Current day and time
- Time zone for your company or branch
- Network time protocol (NTP) server address

Note Reload the Cisco Unity Express software after any NTP changes to ensure that the server information is updated.

Add an NTP Server

Use this procedure to add an NTP server.

Step 1 Choose **System** > **Network Time and Time Zone Settings**. The Network Time and Time Zone Settings window appears.

Step 2 Click **Add**. The Add a NTP Server window appears.

Step 3 Enter the hostname or IP address for the NTP server. To make it the primary NTP server, check the box next to “Preferred”.

Step 4 Click **Add**. The Network Time and Time Zone Settings screen appears with the new server listed in the table.

Delete an NTP Server

Use this procedure to delete an NTP server.

Step 1 Choose **System** > **Network Time and Time Zone Settings**. The Network Time and Time Zone Settings window appears.

Step 2 To delete an NTP server, click the box next to the server to be removed and click **Delete**.

Step 3 Click **Ok** at the prompt. The window appears without the server listed.

Change the Time Zone

Use this procedure to change the time zone.

Step 1 Choose **System** > **Network Time and Time Zone Settings**. The Network Time and Time Zone Settings window appears.

Step 2 Use the drop-down menu to select the correct country.

Step 3 Use the drop-down menu to select the correct time zone.

Step 4 To activate the changes, click **Apply**.

Step 5 Click **Ok** at the information prompt.

CHAPTER 24

Configure Restriction Tables

Configure Restriction Table Parameters

Use this procedure to configure restriction table parameters.

Step 1 Choose **System** > **Restriction Tables**.

Step 2 Choose the restriction table name from the drop-down list. If there is no name indicated in the list, proceed to Add a New Restriction Table, on page 89.

Step 3 Choose the minimum digits allowed. Range:1-30. Default:1.

Step 4 Choose the maximum digits allowed. Range: 1-30. Default: 30.

Step 5 Click **Apply** to save your settings.

Add a New Restriction Table

Use this procedure to a dd a new restriction table.

Step 1 Choose **System** > **Restriction Tables**

Step 2 Click **Add**.

Step 3 Choose a name for your new restriction table by entering the name in the field.

Step 4 Click **Add** to save your changes.

Add Call Patterns to a Restriction Table

If desired, add up to 10 dial strings in the Call Pattern list. For each dial string, you must configure a call pattern and specify whether numbers matching the pattern are allowed or disallowed. External and long distance access codes should be specified. Digits 0 to 9 and the following special characters are allowed:

- *—Match zero or more digits
- .—Match exactly one digit. Each "." serves as a placeholder for one digit.
- 91555* (Allowed)
- 9011* (Not allowed)

Use this procedure to add call patterns to a restriction table.

Step 1 Choose **System** > **Restriction Tables**.

Step 2 In the Call Pattern window, enter the call pattern in the field. Valid patterns can include digits 0 to 9, asterisk (*), and dot (.). The * indicates a match of zero or more digits. Each dot serves as a placeholder for 1 digit.

Step 3 Choose whether the call pattern is to be allowed in the restriction table by clicking **Yes** or **No**.

Step 4 Click **Add** to save your settings.

(Optional) To change the location of a dial string in the comparison sequence, click **Move Up** or **Move Down.** Notification numbers that the user configures are compared against dial strings in the order that the strings are listed in the Call Pattern box. See Restriction Table Examples, on page 91 for more information.

Step 5 Click Yes or No to allow or not allow the call pattern.

Edit Restriction Table Entries

Use this procedure to edit call pattern entries in a restriction table.

Step 1 Choose **System** > **Restriction Tables**.

Step 2 Select the call pattern from the drop-down list and click**Edit**.

Step 3 In the pop-up window, choose whether the call pattern is to be allowed by clicking **Yes** or **No**.

Step 4 Click **Apply** to save your settings.

Delete Restriction Table Entries

Use this procedure to delete call pa ttern entries in a restriction table.

Step 1 Choose **System** > **Restriction Tables**.
Step 2 Select the call pattern from the list and click the **Delete** button.
Step 3 Click **Apply** to save your settings.

Delete Restriction Tables

Use this procedure to delete a restriction table.

Note Deleting a restriction table will cause unrestricted outgoing calls to be allowed by any features using that restriction table.

Step 1 Choose **System** > **Restriction Tables**.
Step 2 Select the restriction table from the **Restriction Table Name** drop-down list and click **Delete**. A warning message appears asking if you wish to continue.
Step 3 Click **Yes** or **No** to complete the task.

Restriction Table Examples

To restrict international and long distance numbers:

Step 1 Enter 9011* in the Call Pattern field, select **No**, and click **Add**.
Step 2 Enter 91.......... in the Call pattern field, select **No**, and click **Add**.

Disallow a Specific Area Code

To disallow a specific area code, except for one phone number within the area code:

Step 1 Enter 9011* in the Call Pattern field, select **No**, and click **Add**.
Step 2 Enter 915551212 in the Call Pattern field, select **Yes**, and click **Add**.
Step 3 Enter 91555....... in the Call Pattern field, select No, and click Add.

The system would first check against the * string, which allows any digits. Therefore, the configuration of any notification number would be permitted, because the 91555* and 9011* strings would not be reached. Moving the * string down to the end of the list would permit any numbers except those that matched in the first two dial strings.

CHAPTER 25

Configure SMTP

Set up Cisco Unity Express to notify users of voice-mail events by phone, pager, or email. Cisco Unity Express contacts these devices to let users know that they have received a voice-mail message. This feature is not enabled by default, and is enabled on a system-wide basis. See Configure Message Notification, on page 129.

Notifications for email and text pager devices are sent using a Simple Mail Transfer Protocol (SMTP) server. You must configure the SMTP server for these notification types to work.

Import SMTP Settings

You can import SMTP settings from email clients.

Use this procedure to import SMTP settings from an email client.

Step 1 Choose **System** > **SMTP Settings**. The System SMTP Settings window appears.

Step 2 From the Import SMTP Settings drop-down menu, select the email client.

Step 3 Click Apply to save your settings.

Configure the SMTP Server

Click Apply to save your settings. Use this procedure to configure the SMTP server.

Step 1 Choose **System** > **SMTP Settings**. The System SMTP Settings window appears.

Step 2 Enter the hostname or IP address of the external SMTP server.

Step 3 Select the security mode from the drop-down menu. Select one of the following:

- None: No security setting is enabled.
- SSL: Specifies that SSL is enabled.

- STARTTLS: Specifies that STARTTLS is enabled.

Step 4 Enter the port number used to connect to the SMTP server.

Step 5 Enter the username and password for the server.

Step 6 Click Apply to save your settings.

Test the SMTP Connection

Use this procedure to test the SMTP connection to an email address.

Step 1 Choose **System** > **SMTP Settings**. The System SMTP Settings window appears.

Step 2 Enter the Test Email Address.

Step 3 Click Send Test Email.

CHAPTER 26

Configure Mailboxes

View List of Mailboxes

Use this procedure to view a list of mailboxes in the system.

Choose Voice Mail > Mailboxes. The Voice Mail Mailboxes window appears and contains the following fields:

- Mailbox Owner (User/Group ID)—By default, the system displays mailboxes in alphabetical order by owner. To display a list of owners from Z to A, click **Mailbox Owner**.
- Primary Extension—To display a list of mailboxes in order by primary owner extension, click **Primary Extension**.
- Mailbox type—To display a list of mailboxes by mailbox type, click **Mailbox Type**.
- Description—To display a list of mailboxes in order by description, click **Description**.
- Use the dialog box to change the number of rows displayed per window.

Add a New Mailbox

Use the following procedures to add one of the following types of mailboxes:

- Personal (User) Mailbox
- General-Delivery Mailbox

Personal (User) Mailbox

An individual user may be assigned to a telephone connected to your telephone network. You can assign a mailbox to an individual user.

General-Delivery Mailbox

One or more people in the company can access a general-delivery mailbox. A caller leaves a message in the mailbox, and members of the group can log into the mailbox and retrieve the message. Any member can delete a message from the general-delivery mailbox.

Note Before you can configure a general-delivery mailbox, you must create the group. See Configure Groups, on page 19.

Use this procedure to add a new personal or general-delivery mailbox.

Step 1 Choose **Voice Mail** > **Mailboxes**. The Voice Mail Mailboxes window appears.

Step 2 Click **Add**. The Add a New Mailbox window appears.

Step 3 Enter or select the following information:

- Owner

Tip Click on the magnifying glass icon to open the Find window to search for an owner.

- Description—Description of the mailbox
- Announcement Only (cannot take messages)
- Mailbox Size
- Maximum Caller Message Size
- Message Expiry Time
- Play Tutorial
- Allow Login Without PIN (this feature is enabled only for Personal mailboxes and is not selectable for a general delivery mailbox). If you are adding a personal mailbox, the following options are available from the drop-down menu:
  - No
  - Yes - from subscriber's number
  - Yes - from any phone number
- Enabled—Indicates that the mailbox will be activated immediately. Unchecking this box deactivates the mailbox
- Fax enabled
- Enable notification for this user or group

Step 4 To save the information, click **Add**.

Display or Modify a Mailbox

Mailbox attributes are organized by the following tabs:

General Tab

Use this procedure to display or modify the general parameters of a personal (user) or general-delivery mailbox.

Step 1 Choose **Voice Mail** > **Mailboxes.**

Step 2 In the Mailbox Owner (User/Group ID) field, click the user ID or group ID. The General tab for that user or group appears with the following fields:

- Description—Description of the mailbox
- Announcement Only (cannot take messages)
- Mailbox Size
- Maximum Caller Message Size
- Message Expiry Time
- Play Tutorial
- Greeting Type (general-delivery mailbox only)
- Allow Login Without PIN
    - No
    - Yes - From Subscriber's Number
    - Yes - From Any Phone Number
- Enabled—Indicates that the mailbox will be activated immediately. Unchecking this box deactivates the mailbox
- Fax enabled
- Secure Outgoing Messages. This setting applies only to this mailbox.
    - Default—The default Secure Outgoing Messages setting configured for the entire voicemail system. See Configure Voice Mail, on page 123.
    - Never—Subscribers do not have the option to mark outgoing messages as secure
    - Ask—Outgoing messages are only marked secure when subscribers mark them as secure.
    - Always—All outgoing messages are automatically marked secure
    - Private—All outgoing messages marked Private are always secure
- Secure Incoming Messages. This setting applies only to this mailbox.
    - All—All messages in this mailbox are marked secure.
    - None—All incoming messages to this mailbox are unsecure.

Step 3 To edit these fields, enter the new information and click**Apply**.

This window also contains informational fields that cannot be edited:

- Created or Last Accessed
- Total Time Used
- Total messages
- New messages
- Saved messages
- Deleted messages
- Mailbox Usage
- Broadcast messages
- Future messages
- Fax messages
- In use

Greetings Tab

Greetings fall into the following three categories:

- Standard greetings
- State-based greetings:

  This category includes the following types of greetings:

  - Busy
  - Closed
  - Internal

- Alternate greetings

  This category includes the following types of greetings:

  - Alternate
  - Meeting
  - Vacation
  - Extended absence

By default, the standard greeting is enabled but none of the alternate or state-based greetings are enabled. The standard greeting is always enabled but if one of the alternate greetings is enabled, it takes precedence over the standard and state-based greetings.

You can enable one or all of the state-based greetings. These greetings are played when no alternate greeting is enabled and the following conditions apply:

- When the system is busy, the busy greeting is played. When enabled, the busy greeting has precedence over the other state-based greetings.
- During non-business hours, the closed greeting is played.
- When the call is from an internal number, the internal greeting is played.

Use this procedure to display or modify the Greetings tab of a personal mailbox.

Step 1 Choose **Voice Mail** > **Mailboxes**. The Voice Mail Mailboxes window appears.

Step 2 Select the **Greetings** tab. The Greetings window appears.

Step 3 To configure one of the following types of greetings, click the link for the greeting:

- Standard
- Closed
- Internal
- Busy
- Alternate
- Meeting
- Vacation
- Extended Absence

Step 4 Choose whether the greeting is either:

- Disabled
- Enabled indefinitely
- Enabled until a specified date and time

Step 5 Choose one of the following sources of the greeting:

- System default
- Personal recording (Click **Upload** and browse to the location of the file.)
- Nothing (This is an empty greeting and can be selected if you want no greeting to be played.)

Note To replace the uploaded greeting, you should have playback and recording devices available on the system and should be in enabled state.

Step 6 Click **Ok** to save your configuration.

Caller Input Tab

Customize how the call flow precedes in response to keys pressed by the caller during a call. For each mailbox, the mailbox owner or system administrator can assign one of the following actions to the keys input by the caller:

- Ignore the input
- Skip the greeting
- Repeat the greeting
- Transfer the call to another number
- Connect to the operator
- Play good bye
- Proceed with subscriber sign-in

These actions can be assigned only to single digit input by the user, such as the numbers zero through nine (0 - 9), the asterisk (*), or the pound sign (#).

You can also optionally restrict the use of the caller input feature by configuring a caller call-flow restriction table.

Use this procedure to display or modify the Caller Input tab of a personal mailbox.

Step 1 Choose **Voice Mail** > **Mailboxes**. The Voice Mail Mailboxes window appears.

Step 2 Select the **Caller Input** tab. The Caller Input window appears.

Step 3 For each of the possible caller inputs, the numbers zero through nine (0 - 9), the asterisk (*), or the pound sign (#), select one of the following actions:

- Ignore the input
- Skip the greeting
- Repeat the greeting
- Transfer the call to another number
- Connect to the operator
- Play good bye
- Proceed with subscriber sign-in

Step 4 Click **Apply** to save your configuration.

Unlock a Mailbox

Occasionally, a mailbox beco mes locked, and the owner cannot access the stored messages. A “mailbox is currently in use” message is typically played when a user tries to access a mailbox that is locked.

Use this procedure to unlock a mailbox.

Step 1 Choose **Voice Mail** > **Mailboxes**. The Voice Mail Mailboxes window appears.

Step 2 Click the box next to the mailbox that you want to unlock.

Step 3 To unlock the mailbox, click **Unlock**.

Delete a Mailbox

Before deleting a mailbox, you must erase the messages stored in the mailbox. The mailbox is removed from the user or group profile of any user or group that uses the mailbox.

Use this procedure to del ete a mailbox.

Step 1 Choose **Voice Mail** > **Mailboxes**. The Voice Mail Mailboxes window appears.

Step 2 Click the box next to the mailbox that you want to delete.

Step 3 Click **Delete**.

Step 4 At the prompt, click **Ok**. The Voice Mail Mailboxes window reappears, and the mailbox is removed.

Find a Mailbox

Use this procedure to search for a mailbox.

Step 1 Choose **Voice Mail** > **Mailboxes**. The Voice Mail Mailboxes window appears.

Step 2 Click Find in the Mailboxes window. The following fields appear:

- Mailbox Owner ID
- Mailbox Type—Personal delivery (belongs to a user) or general delivery (belongs to a group).

Note All fields are optional.

Step 3 Enter the search criteria in one or more fields and click Find. The Voice Mail Mailboxes window reappears and displays the results of your search.

CHAPTER 27

Configure Distribution Lists

View List of Public Distribution Lists

A Distribution list is used to send a voice-m ail message to multiple users at the same time.

Note You cannot modify the default public distribution list, named "everyone," that contains all users in the system. You must be a member of the administrators group, an owner of a list, or a member of a group with Public list manager capability to perform this action.

Use this procedure to view a list of public distribution lists.

Choose **Voice Mail** > **Distribution Lists** >**Public Lists**. The Voice Mail Distribution Lists Public Lists window appears with the following fields:

- Name—List name.
- Number—Number of the distribution list. This number must be unique to the list of public distribution lists.

- Description (optional)
- Member count

Add a Public Distribution List

Depending on your configuration, Cisco Unity Express supports up to a maximum of 25 public distribution lists and 1,000 members or owners total across all of these public distribution lists. See the Cisco Unity Express Release Notes for detailed support information.

Note You must be a member of the administrators group or a member of a group with Public list manager capability to perform this action.

Use this procedure to add a public distribution list.

Step 1 Choose **Voice Mail** > **Distribution Lists** > **Public Lists**. The Public Lists window appears.

Step 2 **Click Add**. The Add a Public Distribution List window appears.

Step 3 Enter information into the following fields:

- Name—List name.
- Number—Number of the distribution list. This number must be unique to the list of public distribution lists and cannot be longer than fifteen digits.
- Description (optional)

Step 4 Click **Add**.

Step 5 Proceed to Add Members to a Distribution List, on page 104.

Add Members to a Distribution List

Use this procedure to add members to your distribution lists.

Note Only administrators can add members to their own private distribution lists or to public distribution lists that they own.

Step 1 Choose **Voice Mail** > **Distribution Lists** and choose either **Public Lists** or **My Private Lists**.

Step 2 Click the name of the list.

Step 3 Click the **Members** tab.

Step 4 Click **Add Member** and one of the following choices:

- Add by voice-mail mailbox number. Enter the exact voice-mail mailbox number and click **Find**.

Note If searching for a remote user or Blind address, enter the location ID and the extension with no delimiters. Wildcard searching is not supported.

- Search for a member by user ID, name, description, or number. Click the button next to the search criteria you want to use. A wildcard search is performed regardless of what is entered in the search criteria text field, so results are not exact matches.

Tip To return a large list of results (and add a large list of members at one time), leave the search criteria text field blank. Check the box at the top of the list results page to select all of the results displayed on that page. To display all search results on the same page, and check the boxes next to all of the search results, choose **All** from the Rows Per Page drop-down list.

Step 5 Select the rows you want to add as members and click **Select row(s)**.

Add a Non Subscriber to a Distribution List

Use this procedure to add a non-subscriber to a distribution list.

Step 1 Choose **Voice Mail** > **Distribution Lists** and choose either **Public Lists** or **My Private Lists**.

Step 2 Click a distribution list name in the Name field. The Public List window or Private List window for that distribution list name appears.

Step 3 Click the **Members** tab.

Step 4 Click **Add Non Subscriber** and enter the phone number in the field.

Step 5 Click Add Member. The new non subscriber phone number appears in the Members field of the Public or Private list window for the distribution list name. The Type is listed as Non Subscriber.

Delete Members of a Distribution List

Delete Members of a Public Distribution List

You must be a member of the administrators group or a member of a group with Public list manager capability to perform this action.

To delete members of a public distribution list:

Step 1 Choose **Voice Mail** > **Distribution Lists** >**Public Lists**. The Public Lists window appears.

Step 2 Click the name of the list from which you want to delete members. The Public List window for that name appears.

Step 3 Click the **Members** tab.

Step 4 Check the box next to the name of the members you want to delete and click **Remove**.

Delete Members of a Private Distribution List

You can only delete members of private distribution lists which you own.

To delete members of a private distribution list:

Step 1 Choose **Voice Mail** > **Distribution Lists** >**My Private Lists**. The My Private Lists window appears.

Step 2 Click the name of the list from which you want to delete members. The My Private Lists window for that name appears.

Step 3 Click the **Members** tab.

Step 4 Check the box next to the name of the members you want to delete and click **Remove**.

Add Owners to a Public Distribution List

Depending on your c onfiguration, Cisco Unity Express supports up to a maximum of 25 public distribution lists and 1,000 members or owners total across all of these public distribution lists. See the Cisco Unity Express Release Notes for detailed support information.

A list owner can be either an individual local user, or a group. If a list is owned by a group, all members of that group are owners of the list.

Note You must be a member of the administrators group or an owner of a list to be able to add owners to it.

Use this procedure to add owners to a public Distribution list.

Step 1 Choose **Voice Mail** > **Distribution Lists** >**Public Lists**. The Public Lists window appears.

Step 2 In the Name field, click the name of the list. The Public List window for that name appears.

Step 3 Click the **Owners** tab.

Step 4 Click **Add Owner** and either:

- Add by voice-mail mailbox number. Enter the exact voice-mail mailbox number and click **Find**.

Note Wildcard searching is not supported.

- Search for a owner by user ID, name, description, or number. Click the button next to the search criteria you want to use. A wildcard search is performed regardless of what is entered in the search criteria text field, so results are not exact matches.

Tip To return a large list of results (and add a large list of owners at one time), leave the search criteria text field blank. Check the box at the top of the list results page to select all of the results displayed on that page. To display all search results on the same page, and check the boxes next to all of the search results, choose **All** from the Rows Per Page drop-down list.

Step 5 Select the rows you want to add as owners and click **Select row(s)**.

Delete Owners of a Public Distribution List

Use this procedure to delete owners of a public Distribution list.

Note You must be a member of the administrators group or a member of a group with Public list manager capability to perform this action.

Step 1 Choose **Voice Mail** > **Distribution Lists** >**Public Lists**. The Public Lists window appears.

Step 2 In the Name field, click the name of the list from which you want to delete owners. The Public List window for that name appears.

Step 3 Click the **Owners** tab.

Step 4 Check the box next to the name of the owners you want to delete and click **Remove**.

Display or Modify a Public Distribution List

Use this procedure to display or modify a public Distribution list.

Note You must be a member of the administrators group, an owner of the list, or a member of a group with Public list manager capability to perform this action.

Depending on your configuration, Cisco Unity Express supports up to a maximum of 25 public distribution lists and 1000 members or owners total across all of these public distribution lists. See the Cisco Unity Express Release Notes for detailed support information.

Step 1 Choose **Voice Mail** > **Distribution Lists** >**Public Lists**. The Public Lists window appears.

Step 2 In the Name field, click the name of the list to display or modify it. The Public List window for that name appears.

Note You cannot modify the default public distribution list, named "everyone," that contains all users in the system.

Step 3 To add owners to a list, click the Owners tab. See Add Owners to a Public Distribution List, on page 106. To add members to a list, click the Members tab. See Add Members to a Distribution List, on page 104.

Delete a Public Distribution List

Use this procedure to delete a public Distribution list.

Note You must be a member of the administrators group, an owner of the list, or a member of a group with Public list manager capability to perform this action.

Step 1 Choose **Voice Mail** > **Distribution Lists** >**Public Lists**. The Public Lists window appears.

Step 2 Check the box next to the list(s) you want to delete.

Step 3 Click **Delete**.

Step 4 Click **Ok** to confirm.

View List of Private Distribution Lists

Use this procedure to view a list of private distribution lists. A Distribution list is used to send a voice-mail message to multiple users at the same time. Private distribution lists are configured and maintained by you. You can own up to five private lists.

Step 1 Choose **Voice Mail** > **Distribution Lists** >**My Private Lists**. The My Private Lists window appears.

Step 2 The My Private Lists window appears and displays the following fields:

- Name—List name.
- Number—Number of the distribution list. This number must be unique to the list of public distribution lists.
- Description (optional)
- Member count

Add a Private Distribution List

Use this procedure to add a private distribution list. Distribution lists are used to send a voice-mail message to multiple users at the same time.

Step 1 Choose **Voice Mail** > **Distribution Lists** >**My Private Lists**. The My Private Lists window appears.

Step 2 Click **Add**.

Step 3 Enter information into the following fields:

- Name—List name.
- Number—Number of the distribution list. This number must be unique to the list of public distribution lists.
- Description (optional)

Step 4 Click **Add**.

Step 5 Click the name of the list to add members to the distribution list.

Display or Modify a Private Distribution List

Cisco Unity Express support s a maximum of 5 private distribution lists for each user, and 50 members total across all of the private lists belonging to a single user. Private distribution lists are configured and maintained by you. See the Cisco Unity Express Release Notes for detailed support information.

Use this procedure to display or modify a private Distribution list.

Step 1 Choose **Voice Mail** > **Distribution Lists** >**My Private Lists**. The Voice Mail Distribution Lists My Private Lists window appears.

Step 2 Click the name of the list to display or modify it. The My Private Lists window for that name appears.

Step 3 To add members to the list, click the **Members** tab. See Add Members to a Distribution List, on page 104.

Delete a Private Distribution List

Use this procedure to d elete a private distribution list.

Note You can only delete private distribution lists which you own.

Step 1 Choose **Voice Mail** > **Distribution Lists** >**My Private Lists**. The My Private Lists window appears.

Step 2 Check the box next to the list(s) you want to delete.

Step 3 Click **Delete**.

Step 4 Click **Ok** to confirm.

View List of Other Users' Private Distribution Lists

Use this procedure to view a list of other users' private distribution lists. Distribution lists are used to send a voice-mail message to multiple users at the same time. Private distribution lists are configured and maintained by their owners.

Step 1 Choose **Voice Mail** > **Distribution Lists** >**Other Users' Private Lists**. The Others' Private Lists window appears.

Step 2 Enter the user ID of the user whose lists you want to view and click **Find**.

Note You must enter the exact user ID. Wildcard searching is not supported.

Step 3 The system displays the private distribution lists belonging to the user and shows the following fields:

- Name—List name.
- Number—Number of the distribution list. This number must be unique to the list of public distribution lists.
- Description (optional)
- Member count

Step 4 Click the name of the list to view the profile of the private distribution list.

View Other Users' Private List Profiles

Use this procedure to view other users' private distribution list profiles. Distribution lists are used to send a voice-mail message to multiple users at the same time. Private distribution lists are configured and maintained by their owners.

Note You can view other users' private distribution list profiles, but you cannot modify them or make changes to list members. You must be a member of the administrators group, an owner of a list, or a member of a group with Private list viewer capability to view other users' private distribution lists. If you try to view them and do not have the proper permissions, you receive a message, “You do not have permission to view other users' private lists.”

Step 1 Choose **Voice Mail** > **Distribution Lists** >**Other Users' Private Lists**. The Others' Private Lists window appears.

Step 2 Enter the user ID of the user whose lists you want to view and click Find.

Note You must enter the exact user ID. Wildcard searching is not supported.

Step 3 The system displays a list of the private distribution lists belonging to the user.

Step 4 Click the name of the list to view its profile. The Profile tab displays the following fields:

- Name—List name.

- Number—Number of the distribution list. This number must be unique to the list of public distribution lists.
- Description (optional)
- Member count

Step 5 Click the Members tab to display members of the private distribution list.

CHAPTER 28

Voice Mail Message Waiting Indicators for Cisco Unified Communications Manager (CUCM)

Refresh Message Waiting Indicator

The MWI is a light indicator on a Cisco IP phone to notify the phone user that a voice-mail message is pending.

Occasionally, the MWI setting for a telephone can be out of synchronization with the user's message status in the voice-mail database. For example, a user could have pending messages, but the MWI would not be turned on. You can refresh the MWI light so that the light reflects the current message status in the voice-mail database.

Use this procedure to refresh the message waiting indicator (MWI) for a single mailbox or for all mailboxes.

Step 1 Choose **Voice Mail** > **Message Waiting Indicators** > Refresh.

Step 2 To refresh one mailbox, check the box next to mailbox owner's user or group ID and click **Refresh Selected**. To refresh all mailboxes, click **Refresh All**.

Modify Message Waiting Indicator Settings

Use this procedure to modify message waiting indicator settings.

Step 1 Choose **Voice Mail** > **Message Waiting Indicators** > **Settings**. The SIP MWI notification mechanism window appears. Select one or all of the following:

- **Subscribe Notify**—Cisco Unified Communications Manager subscribes to Cisco Unity Express using SUBCRIBE/NOTIFY SIP messages for MWI notification for each of the ephone-dns registered to receive MWI notifications. See MWI Configuration Examples, on page 114.

- Check the box to include envelope information in the notifications.

- **Unsolicited Notify**—Cisco Unified Communications Manager is not required to send a subscription request for each ephone-dn to Cisco Unity Express for MWI notification. Cisco Unity Express sends NOTIFY SIP messages to Cisco Unified Communications Manager whenever there is a change in the MWI status for any ephone-dn.

Step 2 Click Apply to save your settings.

MWI Configuration Examples

Subscribe/Notify Notification Example

The following example shows the configuration required to support the subscribe/notify method of MWI notification.

```
telephony-service
    …
    …
mwi sip-server 1.100.9.6 transport udp port 5060
ephone-dn  35
number 2010
    …
mwi sip
```

CHAPTER 29

Configure a Voice Mail Auto Attendant

Add an Auto Attendant

An Auto attendant allows you to create and change greetings that callers hear when your telephone system answers incoming calls.

A standard welcome greeting and other system messages are provided as part of the auto attendant included with Cisco Unity Express. Use this procedure to add a custom auto attendant. You can record a different welcome greeting to use in place of the standard greeting.

Use the following procedure to add an auto attendant.

Before you begin

You need the following information:

- The name of the .wav file containing the prerecorded welcome greeting. This file must be stored on the system so that it can be located and saved in the auto attendant script. This file should be recorded using ITU-T mu law and be an 8Khz/8 bit mono file.

Note For more information on recording auto attendant greetings, see the Cisco Unity Express Maintain and Operate Guides.

- The number of times the auto attendant will replay instructions to a caller before the call is disconnected. This count begins when the caller moves past the main menu and hears instructions for a submenu. The main menu will play five times; then, if the caller makes no choice or makes incorrect choices, the call is transferred to the operator.

- The Auto attendant operator extension.
- The Auto attendant access number.
- The Maximum Sessions for your system.

Step 1 Choose **Voice Mail** > **Auto Attendant**. The Auto Attendant window appears.

Step 2 Click **Add**. Enter the necessary information into the fields.

Note You must enter a valid numeric string into the operExtn field to add an auto attendant.

Step 3 Click Add to save your settings.

Step 4 Proceed to Configure Auto-Attendant Script Parameters, on page 116—You can upload welcome prompts from this window for the auto attendant to use.

Configure Auto-Attendant Script Parameters

After you select an automated attendant, the Script Parameters window appears and shows the parameters in the automated attendant script that you have selected.

Field	Description
allowExternalTransfers	True or false. Permits the caller to transfer to an external number. To prevent toll fraud, set this option to "false."
busClosedPrompt	Name of the .wav file containing the message that the caller hears after the welcome prompt if the business is closed at that time.
businessSchedule	Name of the business schedule the system uses to determine the open and closed hours for the business.
busOpenPrompt	Name of the .wav file containing the message that the caller hears after the welcome prompt if the business is open at that time.
dialByExtnAnytime	True or false. Allows a caller to enter a extension number directly when the welcome or menu prompt is being played out. The call is then transferred to that extension.
dialByExtnAnytimeInputLength	How many digits to collect as a part of dialByExtnAnytime.
dialByFirstName	True or false. For dial-by-name, using the first-last-name (instead of the regular last-first-name order).
disconnectAfterMenu	True or false. If true, then the call is disconnected after the menu. If false, then the call is transferred to the operator extension after the menu.
holidayPrompt	Name of the .wav file containing the message that the caller hears after the welcome prompt if the current day is a holiday.

Field	Description
MaxRetry	Number of times that the auto attendant will replay submenu instructions to the caller before disconnecting the call.
operExtn	Auto attendant operator extension
welcomePrompt	Name of the .wav file containing the message that the caller hears when the auto attendant begins to play.

If you have written and uploaded custom auto attendant scripts to Cisco Unity Express, the fields displayed in this window may be different. For more information on Cisco Unity Express auto attendant scripts, including field definitions, see the Cisco Unity Express Maintain and Operate Guides.

Use this procedure to configure auto attendant script parameters.

Step 1 Choose **Voice Mail** > **Auto Attendant**. The Auto Attendant window appears.

Step 2 Click on the name of the auto attendant that you wish to configure. The Edit window appears.

Step 3 Enter the information into the following fields:

- Call-in number
- Script
- Language
- Maximum Sessions
- Click the box to enable.

Step 4 Click Apply to save your changes.

Step 5 Modify the welcome greeting script parameters by clicking Upload next to each parameter. The upload screen appears. Enter the following information in the Upload screen:

- Source Filename
- Destination Filename
- Click the box to overwrite if the destination file already exists.
- Click Upload. After uploading, the new file appears on the welcomePrompt list. See Configure Voice-Mail Call-Handling Parameters, on page 127.

Select an Auto Attendant

Use this procedure to select an auto attendant script to modify or view.

Step 1 Choose **Voice Mail** > **Auto Attendant**. The Auto Attendant window appears.

Step 2 Click on the name of the auto attendant that you wish to configure. The Auto Attendant Edit window appears.

Step 3 Select the filename of the auto attendant script that you want to view or modify. The script contains prerecorded messages for various auto attendant options that the caller hears.

Note The application name is displayed; you do not need to change this value.

Step 4 To upload a new script to use with the auto attendant, click **Upload**.

Step 5 From the Language drop-down list, select the language for the Cisco Unity Express prompts.

Step 6 To go to the Script Parameters window, click Next. See Configure Auto-Attendant Script Parameters, on page 116.

Upload Scripts

Use this procedure to upload voice-mail scripts.

Step 1 Choose **Voice Mail** > **Auto Attendant**. The Auto Attendant window appears.

Step 2 In the Name field, click on the name of the auto attendant that you wish to configure. The Auto Attendant Edit window appears.

Step 3 Click Upload at the Script entry field(s). The Upload window appears.

Step 4 Enter the source filename, or path to the file that you want to upload or click the **Browse** button to help you find the directory with the file you want to upload.

Step 5 Enter the destination filename. Enter the same filename as shown in the Source Filename field or a new filename for the script. If you use the same filename, the existing script will be overwritten.

Step 6 Check the box to overwrite if the destination filename already exists.

Step 7 Click **Upload**.

Configure Auto-Attendant Call Handling

Use this procedure to configure auto-attendant call handling. After you configure script parameters, the Call Handling window appears, containing the following fields:

- Call-in Number—Auto attendant access number
- Maximum Sessions
- Enabled—Enables the auto attendant. Click **Yes** to enable the auto attendant. Click **No** to disable the auto attendant. Callers will hear a message that the auto attendant system is unavailable.

Step 1 Choose **Voice Mail** > **Auto Attendant**. The Auto Attendant window appears.

Step 2 Click on the name of the auto attendant that you wish to configure. The Auto Attendant Edit window appears.

Step 3 Enter the data in the fields.

Note You can change these values later by configuring voice mail call handling. See Configure Voice-Mail Call-Handling Parameters, on page 127.

Step 4 To save the data, click **Apply**. The auto attendant window appears with the new or revised auto attendant entry listed.

View List of Auto Attendants

Use this procedure to view a list of configured automated attendants (auto attendants).

Choose **Voice Mail** > **Auto Attendant**. The Auto Attendant window appears and contains a list of auto attendants and the following fields for each auto attendant. The system auto attendant is denoted by an asterisk.

- Name—Name of the auto attendant.
- Number—Auto attendant access number.
- Maximum Sessions
- Enabled—Whether the auto attendant is enabled.

Edit an Auto Attendant

Use this procedure to edit an auto attendant.

Step 1 Choose **Voice Mail** > **Auto Attendant**. The Auto Attendant window appears.

Step 2 In the Name field, click the name of the auto attendant that you want to modify. The Voice Mail Auto Attendant Edit window appears.

Step 3 Enter information that you want to change.

Note You cannot change the name of the auto attendant from this window. See Select an Auto Attendant, on page 117.

Step 4 Enter information you want to change in the Script Parameters window. You can upload welcome prompts from this window for the auto attendant to use. See Configure Auto-Attendant Script Parameters, on page 116.

Step 5 Enter information you want to change in the Call Handling window. See Configure Voice-Mail Call-Handling Parameters, on page 127.

Step 6 Click **Apply** to save your data.

Step 7 See Configure Auto-Attendant Script Parameters, on page 116.

Delete an Auto Attendant

Use this procedure to delete an auto attendant.

Step 1 Choose **Voice Mail** > **Auto Attendant**. The Auto Attendant window appears.

Step 2 Check the box next to the auto attendant that you want to delete.

Step 3 Click **Delete**.

Step 4 Click **Ok** to confirm the deletion.

CHAPTER 30

Set Voice Mailbox Defaults

When you create a mai lbox, the defaults that you set in the **Defaults Mailbox** window take effect. Use this procedure to specify the default maximum mailbox size, the maximum caller message size, and the message expiry time. This default set of parameters is applied when a new mailbox is created.

Step 1 Choose **Voice Mail** > **VM Defaults**. The Voice Mail VM Defaults window appears.

Step 2 Enter the information in the following fields:

- Mailbox Size, in seconds
- Maximum Caller Message Size, in seconds
- Message Expiry Time, in days

Step 3 To save your entries, click **Apply**.

CHAPTER 31

Configure Voice Mail

When you create a user, the defaults that you set in the **Defaults Voice Mail** window apply to that user. Now you can configure voice mail settings.

Use this procedure to configure the voice-mail application.

Step 1 Choose **Voice Mail** > **VM Configuration**. The Voice Mail VM Configuration window appears.

Step 2 Enter information in the following fields:

- Maximum voice message store, in minutes.
- Maximum subscriber recording size, in seconds.
- Maximum broadcast message size, in seconds.
- Broadcast message expiry time, in days.

Note The following selections are optional.

- Prompt language.
- Use Message Waiting Indication (MWI) extension for Broadcast messages:
  - **Yes**—When a broadcast message is received by the system, the message waiting indicator (MWI) light is turned on the users' phones.
  - **No**—When a broadcast message is received by the system, the MWI light is not turned on the users' phones.
- Play caller ID for external callers:
  - **Yes**—If a message from an external caller is received, and the ID of the external caller is available from the system, the telephone number of the caller is played in the envelope information when the voice-mail recipient listens to the message.
  - **No**—If a message from an external caller is received, the system plays an “unknown caller” prompt in the envelope information when the voice-mail recipient listens to the message.
- Enable remote user information cache:
  - **Yes**—Enables collection of vCard and spoken name information from remote voice-mail users to be added to the directory cache (called the least recently used [LRU] cache on the local system. The LRU cache is updated

with user information (such as the user's first and last name) whenever new messages are received. The cache is used to provide addressing confirmation.

  - **No**—Disables collection of vCard and spoken name information from remote voice-mail users for the LRU cache.

- Mandatory message expiry—Choosing **Yes** allows an administrator to force a user to delete messages upon expiry, therefore not allowing the user to choose to save the message again.
- Mailbox Selection. Choose from the following:
  - Last Redirecting Party
  - Original Called Party
- Outgoing e-mail “from” address.
- Non-subscriber **Delivery Restriction Table**. Choose no restriction table or select from a list of configured restriction tables.
- Caller Call Flow Restriction Table
- Business Hours Schedule for Greetings
- Click to enable **Live Reply**
- Live Reply Network Precedence—Choose from the following:
  - Disabled—Turn off live reply to network delivered voice-mail messages.
  - Calling Number Rule—Use the calling number rule to determine live reply number for a network delivered voice-mail.
  - E.164 number—Use the E.164 number in the voice-mail header when using live reply for a network delivered voice-mail.
  - E.164 number-Calling Number rule—Use the E.164 number in the voice-mail header if available otherwise use the calling number rule for live reply.
- Live Reply Calling Number Rule—Choose from the following:
  - Extension—Use extension in network voice-mail header for live reply.
  - Prefix-Extension—Use network location prefix then extension in network voice-mail header for live reply.
  - Location-Extension—Use network location id then extension in network voice-mail header for live reply.
  - Location-Prefix-Extension—Combine network location id, prefix, and voice-mail extension for live reply.
  - Prefix-Location-Extension—Combine network location prefix, id, and voice-mail extension for live reply.
- Live Reply Restriction Table. Choose no restriction table or select from a list of configured restriction tables.
- Live Record Pilot Number.
- Click to enable **Live Record Beep**.
- Enter the **Live Record Beep Duration**. Range is 50 to 1000 milliseconds.

- Enter the Live Record Beep Interval. Range is 1 to 30 seconds.
- Select the option for Secure Messages. This setting applies to all Cisco Unity Express subscribers who are logged into the voicemail application.
    - Never—Subscribers do not have the option to mark outgoing messages as secure.
    - Ask—Outgoing messages are only marked secure when subscribers mark them as secure.
    - Always—All outgoing messages are automatically marked secure.
    - Private—All outgoing messages marked Private are always secure. This is the default value.

Step 3 To save your changes, click **Apply**.

CHAPTER 32

Configure Voice-Mail Call-Handling Parameters

Use this procedure to configure call-handling parameters.

Step 1 Click **Voice Mail** > **Call Handling**. The Voice Mail Call Handling window appears.

Step 2 Enter the data in the following fields:

- Voice Mail Phone Number
- Voice Mail Language
- Maximum Sessions
- Voice Mail Operator Number
- Application Parameter Settings Script
- Administration via Telephone (AvT) call-in number
- Administration via Telephone (AvT) prompt language

Step 3 Click **Apply** to save your changes.

CHAPTER 33

Configure Message Notification

Set up Cisco Unity Express to notify users of voice-mail events by phone, pager, or email. Cisco Unity Express contacts these devices to let users know that they have received a voice-mail message. This feature is not enabled by default, and is enabled on a system-wide basis.

Note If this feature is enabled system-wide, configured for specific users, and then disabled system-wide, upon enabling it again, the specific user configurations are restored.

To configure notification by email and for text paging devices, you must also configure an SMTP server. See Configure SMTP, on page 93.

Notification Administration

Use these procedures to configure notification.

Step 1 Choose **Voice Mail** > **Message Notification** >**Notification Administration**. The Notification Configuration window appears.

Step 2 Check the box to enable system-wide notification and choose one of the following message notification types from the drop-down list:

- **Urgent Messages**—Notifications are only sent for voice-mail messages marked “urgent” by the sender.
- All Messages—Notifications are sent for all voice-mail messages.

Step 3 Check the box to enable system-wide notification for live recordings.

Step 4 Check the box to allow a user to log in to the voice mailbox to retrieve voice-mail messages after notification.

Step 5 Enter voicemail notification text:

- Enter the text that will precede the voicemail message notification. The maximum message length is 250 characters.

- Enter the signature text that will follow the voicemail message notification. The maximum message length is 250 characters.

Step 6 Check the box to send voice messages as .wav file attachments to email notification messages.

Step 7 Check the box to enable cascading notifications.

Step 8 Enter the number of seconds after which a call is considered failed. The range is 12 to 96.

Step 9 Choose a restriction table name from the drop-down menu. See Configure Restriction Tables, on page 89 .

Step 10 Click Apply to save your settings.

Enable Subscriber Notification

Use this procedure to enable or disable notification for selected subscribers.

Step 1 Choose **Voice Mail** > **Message Notification** >**Subscriber Notification Management**.

Step 2 If the subscribers for which you want to configure notification are not listed, click **Find** and enter the User or Group ID. Use * for wildcard searching.

Or

Step 3 If the subscribers are listed, check the box next to their user or group ID and click **Enable Notification** or **Disable Notification**. The User Profile window appears with the Notification Tab active.

Step 4 A list of notification devices is displayed. Click the box next to specific devices to enable them. To configure a notification device, see Configure Notification Devices, on page 130.

Note The check boxes are not enabled if notification has been disabled on a system-wide basis. See .Notification Administration, on page 129

Configure Notification Devices

Use this procedure to configure a specific notification device.

Step 1 Choose **Voice Mail** > **Message Notification** >**Subscriber Notification Management** and click the user's name in the list of users.

Step 2 In the Notification Device window, click the name of the device that you want to configure.

Step 3 Enter data into the following fields. The fields shown depend on the type of device that you have selected.

- Device phone number
- Extra digits (such as access codes)
- To: (Email address)—Enter the email address to which to send notifications.

- Text for pager/text for email—Enter the text to display on the pager or in the email when the notification is sent. **Note**: Special characters, including the "?," are not allowed.
- If the ability to send a copy of the voice-mail message as an email attachment is enabled system-wide (see Notification Administration, on page 129), you can check the box to allow this feature for the user.
- Notification preferences—Choose one of the following from the drop-down menu:
  - **Urgent Messages**—Notifications are only sent for voice-mail messages marked "urgent" by the sender.
  - All Messages—Notifications are sent for all voice-mail messages.**Note**: If you select "All," but the system-wide notification preference is "Urgent," you are not allowed to select "All" for an individual user. See Notification Administration, on page 129.
- Notification schedule—See Set Up the Notification Schedule, on page 131.

Step 4 Click **Apply** to save your data.

Set Up the Notification Schedule

When configuring a specific notification device, a calendar with the days of the week and the time, in half-hour increments, is shown.

Select Notification Manually

Use this procedure to manually select notification dates and times.

Step 1 Choose **Voice Mail** > **Message Notification** >**Subscriber Notification Management** and click the user's name in the list of users.

Step 2 Click on a name in the User/Group ID field. The User Profile window appears.

Step 3 Check the boxes under the day and time. A checked box indicates a time period when notifications will be sent to the user.

Step 4 Set Cascade options—Set your cascade settings to notify specified recipients after any specified time.

Step 5 Click **Apply** to save your changes.

Set Notifications for a Day

Use this procedure to quickly set notifications for an entire day.

Step 1 In the Quick Add box, select the day, start time, and end time.

Step 2 Click **Add**.

To copy a day's notification schedule, select the day to copy in the drop-down list, then click **Copy**.

Step 3 Click **Apply** to save your changes.

CHAPTER 34

Configure My Notification Devices

You can configure notify yourself of voice-mail events by phone, pager, or email. Cisco Unity Express contacts these devices to let you know that you have received a voice-mail message. This feature is not enabled by default, and must be enabled on a system-wide basis by the system administrator before you can configure notifications.

Cascading Settings

Cisco Unity Express supports Cascading Message Notification, which allows you to set up a series of notifications to a widening circle of recipients at various time intervals if your message is not immediately responded to.

In the Voice Mail > Message Notification > My Notification Devices window, set your cascade settings to notify specified recipients after a specified time. Range is 5 to 10080 minutes.

Use this procedure to configure notify yourself of voice-mail events by phone, pager, or email.

Step 1 Choose **Voice Mail** > **Message Notification** >**My Notification Devices**.

Step 2 In the Notification Device window, click the name of the device that you want to configure.

Step 3 Enter data into the following fields. The fields shown depend on the type of device that you have selected.

- Device phone number
- Extra digits (such as access codes)
- To: (Email address)—Enter the email address to which to send notifications.
- Text for pager/text for email—Enter the text to display on the pager or in the email when the notification is sent. **Note**: Special characters, including the “?,” are not allowed.
- If the ability to send a copy of the voice-mail message as an email attachment is enabled system-wide, you can check the box to enable this feature.
- Notification preferences—Choose one of the following from the drop-down menu:
  - **Urgent Messages**—Notifications are only sent for voice-mail messages marked “urgent” by the sender.
  - All Messages—Notifications are sent for all voice-mail messages.

Note If you select "All," but the system-wide notification preference is "Urgent," you are not allowed to select "All" for an individual user.

- Notification schedule—See Set Up the Notification Schedule, on page 131.

Step 4 Click **Apply** to save your data.

CHAPTER 35

Configure Integrated Messaging (IMAP)

Integrated messaging is a feature for Cisco Unity Express that allows users to manage voice-mail messages by using an Integrated Messaging Access Protocol (IMAP)-compatible email client. The following clients are supported:

- IBM Lotus Notes 10
- Microsoft Outlook 2016
- Thunderbird 60.7.1

Voice messages are received as email attachments in the form of .wav files. After it is enabled in #unique_193, IMAP works automatically on a system-wide basis when you open your email client to check incoming voice-mail.

Note Integrated messaging is available for personal mailboxes only.

Integrated Messaging Service Configuration

Use this procedure to configure system-wide integrated messaging.

Step 1 Choose **Voice Mail** > **Integrated Messaging** >**Service Configuration**.

Step 2 Check the box next to Enable Integrated Messaging.

Step 3 Enter the session idle timeout value, in minutes. When a user's integrated message session has been idle for this time period, the session is timed out and the user must restart. Range is 30 to 120.

Enter the maximum session allowed value, or the number of concurrent integrated message sessions that can run on the Cisco Unity Express system. The number of sessions supported depends on the Cisco Unity Express module being used. See the Cisco Unity Express Release Notes for detailed support information.

Step 4 Select the security mode from the drop-down menu:

- None: Only non-SSL connections are permitted.

- Secure Sockets Layer (SSL): Only SSL connections are permitted.
- Mixed: Both non-SSL and SSL connections are permitted.

Step 5 Click **Apply** to save your settings. You must restart Integrated Messaging Service for configuration changes to take effect.

View Integrated Messaging Sessions

Use this procedure to view IMAP sessions.

Step 1 Click **Apply** to save your settings. You must restart Integrated Messaging Service for configuration changes to take effect. Use this procedure to view IMAP sessions.

Step 2 Choose **Voice Mail** > **Integrated Messaging** >**Sessions**.

Note If IMAP sessions have been enabled on the system, the statistics will appear in this window. If no sessions are present, you will see the "There are no active IMAP sessions" message.

CHAPTER 36

Configure VoiceView Express

VoiceView Express allows voice-mail users to browse, listen to, and manage new and saved voice-mail messages using their Cisco IP Phone display and soft-keys available on the phone. Users can compose and send voice-mail messages to other users and manage their personal mailbox options using VoiceView Express.

Configure the VoiceView Express Service

Use this procedure to configure the VoiceView Express service.

Step 1 Choose **System** > **VoiceView Express** > **Service Configuration**. The VoiceView Express Service Configuration window appears.

Step 2 Click the check box to enable VoiceView Express (VVE).

Step 3 Enter the session idle timeout value. This is the interval after which an idle VoiceView Express session is automatically closed. The range is 5 to 30 minutes, and the default value is 5 minutes.

Step 4 (For CUCME configurations only): If you have multiple authentication servers on your network, you can enter a fallback authentication server to be used if the VoiceView Express authentication server is unable to authenticate. For example, if you have multiple phone services configured in CUCME that require authentication, you can specify one of those servers to use as the fallback server for VoiceView Express. Enter the URL of the fallback authentication server.

Step 5 Click **Apply** to save your changes.

Terminate VoiceView Express Sessions

Use this procedure to termina te VoiceView Express (VVE) sessions.

Step 1 Choose **System** > **VoiceView Express** > **Sessions**. The VoiceView Express Sessions window appears.

Step 2 The session window displays all active VoiceView Express sessions.

Step 3 To terminate a VoiceView Express session, check the box next to the session and click **Terminate**.

CHAPTER 37

Configure IVR

The Interactive Voice Response (IVR) option is a separately licensed option that integrates with Cisco Unity Express. IVR allows a telephone caller to select options from a voice menu and otherwise interact with the Cisco Unified Express system. The Cisco Unity Express IVR applications work with Cisco Unified Communications Manager Express or Cisco Unified Communications Manager. After the system plays a pre-recorded voice prompt, the caller presses a number on a telephone keypad to select an option.

If your system is configured with IVR, the GUI screen will have an IVR tab that you can select to configure IVR features.

Configure IVR Applications

Add IVR Applications

Use this procedure to add IVR applications.

Step 1 Choose **IVR** > **IVR Applications**. The IVR Applications window appears.

Step 2 Click **Add** to begin adding IVR applications. The **Add** window appears.

Step 3 Enter the application name in lower case.

Step 4 Select one of the following trigger types:

- **Call-in number**—A number to dial in to the application.
- **HTTP trigger—**Enter a new URI. A corresponding HTTP trigger is created.

Note Entering information in this next step automatically selects Script parameter choices in the Configure Script Parameters, on page 140 section.

Step 5 Select the script information from the drop-down list.

Step 6 (Optional) Add a new script by clicking **Upload**. The Upload dialog box appears where you can upload a script. You can also manage scripts using **System** > **Scripts**. See Configure System Scripts Using Editor Express, on page 61 for more information about scripts.

Step 7 Select the language.

Step 8 Enter the Maximum Sessions.

Step 9 Click to enable.

Step 10 Click Apply to save your changes.

Note You must enter a valid string in the operExtn field to save your changes.

Configure Script Parameters

Use this procedure to configure script parameters.

Note All the steps in this section are required.

Step 1 Choose **IVR** > **IVR Applications**. The IVR Applications window appears.

Step 2 Click **Add** to begin configuring IVR script parameters.

or

Step 3 Click on the name of an existing IVR application. The Edit window appears.

The list of script parameters, generated dynamically, depends on your installation. The following types of scripts may be available in your installation:

- busClosedPrompt
- holidayPrompt
- welcomePrompt
- disconnectAfterMenu
- dialByFirstName
- allowExternalTransfers
- MaxRetry
- dialByExtnAnytime
- busOpenPrompt
- businessSchedule
- dialByExtnAnytimeInputLength
- operExtn*:

Step 4 For each script parameter in your installation, select the appropriate script from the drop-down list.

Step 5 Click**Upload**. The **Upload** dialog box appears.

Step 6 In the **Upload** dialog box:

a) Enter the source filename, or path to the file you want to upload.

Tip Click the **Browse** button to help you find the directory with the file you want to upload.

b) Enter the destination filename. Enter the same filename as shown in the Source Filename field or a new filename for the script.

c) Click the box to overwrite the destination file, if the file already exists.

d) Click **Upload** to save your settings. You can also manage scripts using **System** > **Scripts**. SeeConfigure System Scripts Using Editor Express, on page 61.

Step 7 Click **Add** in the IVR Applications window to save your settings.

Delete a Script

Use this procedure to delete a script.

Step 1 Choose **IVR** > **IVR Applications**. The IVR Applications window appears.

Step 2 Check the box of the file to delete from list and click **Delete**.

Step 3 Click **Ok** or **Cancel** to complete the task.

Configure HTTP Triggers

Add HTTP Triggers

Use this procedure to add IVR HTTP triggers.

Step 1 Choose **IVR** > **HTTP Triggers**. The IVR HTTP Triggers window appears.

Step 2 Click **Add**. The Add an HTTP Trigger window appears.

Step 3 Choose an application from the drop-down list. The list of applications, generated dynamically, depends on your installation.

Step 4 Enter the URL. Use the format, http://:8080/

Step 5 Enter the Maximum Sessions.

Step 6 Choose**Yes** or **No** to indicate whether you would like this HTTP trigger to be enabled.

Step 7 Select the language.

Step 8 Click **Add** to save your settings.

Delete HTTP Triggers

Use this procedure to delete an HTTP trigger.

Step 1 Choose **IVR** > **HTTP Triggers**.
Step 2 Click in the box next to the trigger that you want to delete.
Step 3 Click **Delete** from the menu at the top of the screen.
Step 4 Click Ok to delete the file.

Edit HTTP Triggers

Use this procedure to edit an HTTP trigger.

Step 1 To edit an HTTP trigger, go to the **IVR** > **HTTP Triggers** window.
Step 2 Click the HTTP trigger name. The selected HTTP trigger profile window opens.
Step 3 Edit the **Application**, **Maximum Sessions**, and **Language** fields as needed.
Step 4 Click **Yes** or **No** whether you want this HTTP trigger to be configured.
Step 5 Click **Apply** to save your settings.

View HTTP Triggers

Use this procedure to view a list of configured HTTP triggers.

Choose **IVR** > **HTTP Triggers**. The IVR HTTP Triggers window appears and contains a list of HTTP triggers and the following fields for each HTTP trigger.

- Name—Name of the application suffix.
- Application—Name of the application.
- Enabled—Whether the auto attendant is enabled.
- Maximum Sessions
- Language

Configure VoiceXML Applications

Add VoiceXML Applications

Use these procedures to add VoiceXML applications.

Step 1 Choose **IVR** > **VXML Applications**. If no VXML applications are configured, you must configure a new file.

Step 2 Click **Deploy** to add a new VXML application file. The Upload window appears.

Note The following steps are required.

Step 3 In the **Upload** window, enter the source filename.

Tip You can search for a file on your hard drive by clicking the **Browse** button.

Step 4 Enter the name for your source file.

Step 5 Click **Upload** to save your settings.

Delete VoiceXML Applications

Use this procedure to delete VXML applications.

Step 1 Choose **IVR** > **VXML Applications.**

Step 2 Click the box to select the application to delete.

Step 3 Click **Delete**. The system asks if you are sure that you want to delete the application.

Step 4 Click **Ok** or **Cancel** to complete the task.

Start VoiceXML Applications

Use this procedure to start VXML applications.

Step 1 Choose **IVR** > **VXML Applications**.

Step 2 Click the box to select the application you want to start.

Step 3 Click **Start**. The status of the selected application appears in the Status field.

Stop VoiceXML Applications

Use this procedure to stop VXML applications.

Step 1 Choose **IVR** > **VXML Applications**.

Step 2 Click the box to select the application that you want to stop.

Step 3 Click **Stop**. The status of the selected application appears in the Status field.

Restart VoiceXML Applications

Use this procedure to restart VXML applications.

Step 1 Choose **IVR** > **VXML Applications**.

Step 2 Click the box to select the application to restart.

Step 3 Click **Restart**. The status of the selected application appears in the Status field.

Configure the Enterprise Database Subsystem

Add a Database (DB) Profile

Use this procedure to add a database profile.

Step 1 Choose **IVR** > **Enterprise Database Subsystem**. If no database profiles are found, you must add a new profile.

Step 2 Click **Add** to add a new profile. The **Add DB Profile** window appears.

Step 3 In the **Add DB Profile** window, enter the name of the profile.

Step 4 Enter the profile description.

Step 5 Enter the hostname. You can enter any valid hostname or IP address.

Step 6 Enter the port number.

Step 7 Enter the database type. Choose one of the following from the drop-down menu:

- IBM DB2
- Microsoft SQL or MSDE (default)
- Oracle
- Sybase

Step 8 Enter the database name.

Step 9 Enter your username.

Step 10 Enter your password.

Step 11 Enter the number of maximum connections.

Step 12 Click **Add** to save your changes. The **Enabled** box is checked default.

Add and Delete Optional Database Driver Parameters

Use this optional procedure to add or delete database driver parameters.

Step 1 Choose **IVR** > **Enterprise Database Subsystem**.

Step 2 Click **Add**. The **Add DB Profile** window appears.

Step 3 In the **Add DB Profile** window, enter the **name** of the database driver parameter in the **Name** field.

Step 4 Enter the **value** of the database driver parameter in the **Value** field.

Step 5 Click **Add More** if you would like to add more driver parameters. Additional blank fields appear. Repeat Step 3, on page 145 and Step 4, on page 145.

Step 6 Delete driver parameters by checking the box next to the parameter in the list and clicking **Delete**.

Step 7 Click **Add** to save your changes.

Configure the IVR E-Mail Subsystem

Use this procedure to configure your IVR e-mail subsystem.

Step 1 Choose **IVR** > **E-mail Subsystem**.

Step 2 Enter the default "From" e-mail address. Default is localhost@localdomain.com. When Cisco Unity Express sends an e-mail it uses that e-mail as its own e-mail ID. Use any standard e-mail address.

Step 3 Click **Apply** to save your settings.

Manage IVR Documents

You can manage the following IVR document types from the **IVR Document Management** window:

- Templates—Plain text documents that have a ".txt" extension.
- TIFF Images—Image files typically used for fax that have a ".tif" or ".tiff" extension.
- Generic Files—Any document in any format, even plain text and TIFF files (for example, PDF, GIF, and BMP).

Configure IVR Templates

Use this procedure to configure IVR templates.

Step 1 Choose **IVR** > **Document Management** > **Templates**. If no documents are found, you must upload a new document.

Step 2 Click **Upload**. The **Upload** dialog box appears.

Step 3 In the **Upload** dialog box:

a) Select the language.
b) Enter the source filename, or path to the file you want to upload.

Tip Click the **Browse** button to help you find the directory with the file you want to upload.

a) Enter the destination filename. Enter the same filename as shown in the Source File name field or a new filename for the template.
b) Click the box to overwrite the destination file, if the file already exists.
c) Click **Upload** to save your settings.

Step 4 Click **Ok** to save your changes.

Configure IVR TIFF Images

Use this procedure to configure IVR TIFF images.

Step 1 Choose **IVR** > **Document Management** > **TIFF Images**. If no documents are found, you must upload a new document.

Step 2 Click **Upload**. The Upload dialog box appears.

Step 3 In the Upload dialog box, perform the following tasks:

a) Select the language from the drop-down list.
b) Enter the source filename, or path to the file you want to upload.

Tip Click the **Browse** button to help you find the directory with the file you want to upload.

a) Enter the destination filename. Enter the same filename as shown in the Source Filename field or a new filename for the image.
b) Click the box to overwrite the destination file, if the file already exists.
c) Click **Upload** to save your settings.

Step 4 Click **Ok** to save your changes.

Configure IVR Generic Files

Use this procedure to configure IVR generic files.

Step 1 Choose **IVR** > **Document Management** > **Generic Files**. If no documents are found, you must upload a new document.

Step 2 Click **Upload**. The Upload dialog box appears.

Step 3 In the Upload dialog box, perform the following tasks:

a) Select the language from the drop-down list.
b) Enter the source filename, or path to the file you want to upload.

Tip Click the **Browse** button to help you find the directory with the file you want to upload.

c) Enter the destination filename. Enter the same filename as shown in the Source Filename field or a new filename for the file.
d) Click the box to overwrite the destination file, if the file already exists.
e) Click **Upload** to save your settings.

Step 4 Click **Ok** to save your changes.

CHAPTER 38

Configure Backup and Restore

When a Scheduled Backup occurs, it automatically takes the system to the offline mode, and brings it back online after backup is done. To manually perform a backup, you must manually take the system offline.

In offline mode, the system continues to accept and process incoming calls and fax messages and also continues to support access to messages through the IMAP, TUI and VVE interfaces.

However, in offline mode, CLI configuration commands are not available, the GUI only displays the backup progress bar, and the user login for the GUI is disabled. The following interfaces are also disabled:

- **Settings** > **Options** in the TUI
- Everything in AvT
- **My Options** in VVE

Configure the Backup Server

Before you begin the backup process from the **Administration Backup/RestoreStart Backup** window, you must first set the parameters in this window.

Use this procedure to configure the backup server.

Step 1 Choose **Administration** > **Backup/Restore** >**Configuration**.

Step 2 Enter the information shown in the following fields:

- Server URL—The URL of the server on the network where backup files are stored. The format should be *ftp://server/directory/* where server is the IP address or hostname of the server.

- User ID—The account name or user ID on the backup server. You must have an account on the system to which you are backing up your data. Do not use an anonymous user ID.
- Password—The password for the account name or user ID on the backup server.
- Confirm Password—The password entered again.
- Maximum Revisions—The maximum number of revisions of the backup data that you want to keep on the server. The maximum number is 50. The default value is 5.

Step 3 Click **Apply** to save the information.

View Scheduled Backups

To view your scheduled backups, choose **Administration** > **Backup/Restore** >**Scheduled Backups**.

The Scheduled Backups window appears. From this window, you can see the following information about the backups:

- Name
- Description
- Schedule
- Next Run
- Categories of backup, or type of data to save

From this window, you can perform the following actions:

- To add a new scheduled backup, click **Schedule Backup**.
- To modify an existing scheduled backup, click the link for the schedule name.
- To disable all existing scheduled backups, click **Bulk Disable**. See Disable a Scheduled Backup, on page 154.

Add a Scheduled Backup

You must do the following before starting a backup:

- Configure the server used to back up the data. See Configure the Backup Server, on page 149.
- Save your configuration.

You can configure scheduled backups to occur once or recurring jobs that repeat:

- Every N days at a specific time
- Every N weeks on specific day and time
- Every N months on a specific day of the month and time

- Every N years on specific day and time

Use this procedure to add a new scheduled backup.

Step 1 Choose **Administration** > **Backup/Restore** >**Scheduled Backups**.

The Scheduled Backup tab appears.

Step 2 Enter a name for the scheduled backup.

Step 3 Enter a description of the scheduled backup; for example, “backupdata6-2-04.”

Step 4 Select the categories of backup, or type of data that you want to save:

- **Configuration**—Saves the configurations of the system and applications.
- **Data**—Saves your voice-mail messages.
- Historical Reporting Data—See Configure Historical Reporting, on page 167 for more information.

Step 5 Select whether the scheduled backup will occur:

- Once
- Daily
- Weekly
- Monthly
- Yearly

Step 6 Select whether the scheduled backup will start:

- Once
- On a specific date and time

Step 7 To save the scheduled backup, click **Apply**.

Step 8 To configure users who will be notified of the scheduled backup status, click the Notification tab. See Configure Backup Schedule Notification, on page 151.

Configure Backup Schedule Notification

When configuring a scheduled backup, you can configure the system to notify selected users about the backup status.

Add a Backup Schedule Notification

Use this procedure to add a backup schedule notification.

Step 1 Choose **Administration** > **Backup/Restore** >**Scheduled Backups**.

The Scheduled Backup tab appears.

Step 2 Click Schedule Backup to create a new scheduled backup, or select an existing scheduled backup.

Step 3 Click the Notification tab.

Step 4 Click Insert.

a) Select the Condition from the pull-down menu:

- **Success**—Notify the target only if the scheduled backup is completed successfully.
- **Failure**—Notify the target only if the scheduled backup fails.
- **Both**—Notify the target when a scheduled backup either succeeds or fails.

b) Select the Device for notification:

- **E-mail**—Notify by email
- **Text Page**—Notify by text page
- Voice Mail—Notify by voicemail

c) Enter the Username or E-mail address to be notified.

Step 5 Click **Insert**.

Delete a Backup Schedule Notification

Use this procedure to delete a backup schedule notification.

Step 1 Choose **Administration** > **Backup/Restore** >**Scheduled Backups**.

The Scheduled Backup tab appears.

Step 2 Click the Notification tab.

Step 3 Select the notification to be deleted.

Step 4 Click Delete.

Modify a Scheduled Backup

To modify a scheduled backup, choose **Administration** > **Backup/Restore** >**Scheduled Backups** and click the name of a scheduled backup.

The Modify Scheduled Backup window appears. From this window, you can modify the following fields:

- Description

- Categories or type of data to backup:
  - **Configuration**—Saves the configurations of the system and applications.
  - **Data**—Saves your voice-mail messages.
  - Historical Reporting Data—See Configure Historical Reporting, on page 167 for more information.
- Whether the scheduled backup will occur:
  - Once
  - Daily
  - Weekly
  - Monthly
  - Yearly
- Whether the scheduled backup will start:
  - Once
  - On a specific date and time

To save your changes, click **Apply**.

Manually Start a Backup

You must do the following before starting a backup:

- Configure the server used to back up the data. See Configure the Backup Server, on page 149.
- Save your configuration.

To manually perform a backup, you must take manually the system offline. In offline mode, the system continues to accept and process incoming calls and fax messages and also continues to support access to messages through the IMAP, TUI and VVE interfaces. However, in offline mode, CLI configuration commands are not available, the GUI only displays the backup progress bar, and the user login for the GUI is disabled. The following interfaces are also disabled:

- **Settings** > **Options** in the TUI
- Everything in AvT
- **My Options** in VVE

Use this procedure to begin the data backup process.

Step 1 Click **Administration** > **Backup/Restore** >**Start Backup**. The Start Backup window appears and the system automatically generates a backup ID. The backup ID number increases by 1 every time you back up the server.

Step 2 Enter a description of the backup file; for example, “backupdata6-2-04.”

Step 3 Select the categories of backup, or type of data that you want to save:

- **Configuration**—Saves the configurations of the system and applications.
- **Data**—Saves your voice-mail messages.
- **Historical Reporting Data**—Saves your historical reporting information.

Warning It is recommended that you save your Cisco Unity Express configuration. The backup will put the system in offline mode.

Step 4 To execute the backup, click **Start Backup**.

Disable a Scheduled Backup

To disable a scheduled backup, choose **Administration** > **Backup/Restore** >**Scheduled Backups**. The Scheduled Backups window appears.

- To disable an existing scheduled backup, click the name of a scheduled backup. The Modify Scheduled Backup window appears. Click the Disabled checkbox and click Apply.
- To disable all existing scheduled backups, click **Bulk Disable**. Select whether all scheduled backups should be always enabled, or select a date range for when the disabling of the scheduled backup will begin and end. Click Apply. All existing scheduled backups are disabled.

  Click on the Back To List button to return to the scheduled backup list without disabling all the scheduled backups.

Start a Restore

After you have backed up your voice-mail and configuration data to the server, you can restore it for every new installation or upgrade. Use this procedure to restore previous data or a previous configuration on your system.

Note If you restore a previously existing configuration, you cannot run the Initialization Wizard again. You will log in using the same administrative privileges that existed in the restored configuration.

Use this procedure to start a restore.

Step 1 Choose **Administration** > **Backup/Restore** >**Start Restore**. The window appears containing the following fields:

- Backup ID and Description—The backup ID and description of previous backups.
- Categories—The type of data that you want to restore. Choose:
  - **Configuration**—Saves the configurations of the system and applications.
  - **Data**—Saves your voice-mail messages.
  - **Historical Reporting Data**—Saves your historical reporting information.

Step 2 Select the row containing the configuration that you want to restore.

Note If you have backed up both the configuration and the data, you can restore both the categories, or select one to restore.

Step 3 Click **Start Restore**.

CHAPTER 39

Use the Administration Control Panel for Cisco Unified Communications Manager (CUCM)

Switch the Call Agent to Cisco Unified Communications Manager Express

Use this procedure to switch the call agent to Cisco Unified Communications Manager Express.

Step 1 Choose **Administration** > **Control Panel**.

Step 2 Under the Call Agent Integration: CUCM label, click Switch to CUCME.

A warning box appears indicating:

“Warning: This operation will a. permanently delete all non-local site related configuration b. reboot the system automatically Do you wish to continue?

Step 3 Click Ok to switch to Cisco Unified Communications Manager Express or click Cancel.

To save or reload Cisco Unity Express, see Save or Reload Cisco Unity Express, on page 157.

Save or Reload Cisco Unity Express

Note Tis operation takes a few moments to complete.

Use this procedure to save or reload Cisco Unity Express.

Step 1 Choose **Administration** > **Control Panel**.

Step 2 Click **Save Configuration**.

Step 3 Click Ok at the prompt.

Step 4 Click **Reload Cisco Unity Express**. A dialog box appears warning you that reloading the system will terminate all end user sessions and that any unsaved configuration data will be lost.

Step 5 Click **Ok** or **Cancel** to complete the task.

To switch the call agent to Cisco Unified Communications Manager Express, see Switch the Call Agent to Cisco Unified Communications Manager Express, on page 157.

CHAPTER 40

Cisco Smart Licensing

From Cisco Unity Express Release 9.0.5 onwards, only Cisco Smart Software Licensing is supported. In Cisco Smart Software Licensing, the purchased licenses are not tied to the hardware and Product Activation Key (PAK). Licenses can be configured by communication to the Cisco Smart Software Manager (CSSM) or Smart Software Manager satellite. You must purchase the licenses specific to Cisco Unity Express Virtual 10.1.

Configure Smart Licensing

Use this procedure to configure Smart Licensing:

Step 1 Launch Cisco Unity Express GUI, and choose Administration > Smart License > Configuration. The Configuration page appears.

Step 2 To set up Transport mode, select one of the three modes under Transport Settings section.

- Direct—Select this option to send data directly to Cisco Smart Software Manager (CSSM).
- Transport Gateway—Select this option to use a Cisco Call Home transport gateway or a premise-installed Smart Software Manager satellite. Specify the URL for the respective Smart Software Manager satellite or CSSM.
- HTTP/HTTPS Proxy—Select this option to use an intermediate HTTP/HTTPS proxy to send data. Enter the proxy server address and port number in **IP Address** and **Port** fields respectively.

Click Apply to update the Smart Licensing transport mode.

Step 3 To generate a token ID, log in to your Smart Account in CSSM or your Smart Software Manager satellite. Navigate to the virtual account containing the licenses to be used by this product instance. Generate a product instance Registration Token, and copy or save the token ID.

Step 4 To register your product instance, enter or paste your Token into the Product Instance Registration Token field under Smart Software Licensing Product Registration section. Then, click Register.

Step 5 To re-register the product instance, enter or paste your Token into the Product Instance Registration Token field, select the Reregister this product instance if already registered check box, and then click Register.

Step 6 To unregister the product instance, click Deregister.

Step 7 To renew the ID certificate, click Renew Registration. By default, registration is automatically renewed every six months.

Step 8 To renew authorization with CSSM or Smart Software Manager satellite, and enable the product instance to remain compliant, click Renew Authorization. By default, authorization periods are renewed every 30 days.

View Smart License Summary

You can view the status of Smart License Registration, Authorization, and Usage from Cisco Unity Express GUI at: Administration > Smart License > License Summary.

Smart Software Licensing Status

Parameter	Description
Registration Status	Displays the current Smart License registration status. • Registered—The device instance is registered with CSSM or Smart Software Manager satellite. • Unregistered—Smart Software Licensing is enabled on the device, but the device instance is not registered with CSSM or Smart Software Manager satellite. • Registration Expired—The registration is not renewed prior to the expiration date, and the device instance has been removed from CSSM or Smart Software Manager satellite.
Last Renewal Attempt	Displays the date and time of previous registration renewal.
Next Renewal Attempt	Displays the date and time of next registration renewal attempt.
Registration Expires	Displays the expiry date and time for the licenses. One year duration from the date of license registration.
Failure Reason	Provides the reason due to which the latest license registration failed.

Parameter	Description
License Authorization Status	Displays the current Smart License authorization status. • Evaluation Mode—The device is running in evaluation mode. The evaluation period expires after 90 days. • Authorized—Registration has been completed with a valid Smart Account and license consumption has begun. The number of licenses consumed is less than the licenses available for use. This is an indication of being in compliance. • Out of Compliance—The device has exceeded the number of licenses that were purchased. The virtual account containing the product instance has a shortage of one or more of license types used. • Evaluation Expired—The Evaluation period has expired and the device instance will be in unlicensed state. • Authorization Expired—The authorization is not renewed prior to the expiration date.
Last Authorization Attempt	Displays the date and time of previous authorization attempt.
Next Authorization Attempt	Displays the date and time of next authorization attempt.
Authorization Expires	Displays the expiry date and time for the license authorization.
Smart Account	Displays the name of the smart account to which the product is registered.
Virtual Account	Displays the name of the virtual account to which the product is registered.
Product Instance Name	Displays the name of the product instance. **Note** For 10.2.1 release, Once you change the hostname, perform reload to view the updated Product Instance Name.
Export-Controlled Functionality	Specifies if the export controlled functionality is enabled for the product instance (Not applicable for Cisco Unity Express because Export Control functions are part of the underlying infrastructure that Cisco Unity Express runs on).

Smart License Usage

Smart License Usage area displays the basic consumption statistics per license entitlement, and the compliance status for each license type.

Parameter	Description
License	Displays the name of the license.
Entitlement Tag	Unique string associated with the Cisco Unity Express smart licenses.

Parameter	Description
Count	Displays the number of active voice mailboxes or IVR sessions consumed by this product instance.
Status	Displays the compliance status of the license.

CHAPTER 41

Display Cisco Unity Express License Information

Use this procedure to display Cisco Unity Express license information:

Choose Administration > Licenses.

The Licenses display appears, showing the following fields:

- Product ID—The Cisco Unity Express hardware installed
- Serial Number—The serial number for the Cisco Unity Express hardware
- Feature—The installed license feature
- Description—Description of the license, such as voice mail mailboxes or IVR
- Type—Whether the license is a permanent or evaluation license
- State—Whether the license is Active, Inactive, In Use, or Not in Use
- Priority—The priority of the license, either High, Medium, or Low
- Usage—The number of the license that is used
- Validity Left—Days left that the license is valid (evaluation licenses only)

CHAPTER 42

Configure Trace Settings

Use this procedure to enable traces, or debug message output, for components in Cisco Unity Express. Components are modules, entities, and activities in the system. For more information, see the Cisco Unity Express Maintain and Operate Guides at the following URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps5520/prod_maintenance_guides_list.html

Step 1 Choose **Administration** > **Traces**. The window displays a hierarchical listing of the system components.

Step 2 To enable a trace on a system component, click the check box next to the name of the component.

- To expand the listing of components, click the + sign next to the upper-level components.
- Check the box next to an upper-level component (a module or entity) to enable the traces for all of the components under that component.
- Uncheck the box next to an upper-level component to disable the traces for all of the components under that component.

Step 3 Click **Apply** to save your changes.

Step 4 Click Ok in the confirmation window.

CHAPTER 43

Configure Historical Reporting

Historical reporting consists of collecting information about call and application activities and related statistics and sorts and sends the information to local or remote databases. Historical statistics database maintenance components consist of a database purging service that periodically removes older historical statistics data and a database synchronization service that simultaneously updates the local and remote databases. The remote database is typically able to store a larger amount of historical data.

Configure Historical Reporting

Use this procedure to configure historical reporting.

Step 1 Choose **Administration** > **Historical Reporting** >**Configuration**.

Step 2 Check the box to enable historical reporting.

Step 3 Click **Apply** to save your settings.

Configure Purge Settings

Configure Purge Scheduling

Use this procedure to configure the purge schedule.

Step 1 Choose **Administration** > **Historical Reporting** >**Purge Settings**.

Note The following steps are required.

Step 2 The system purges the historical reporting data every day. Choose a time when the system is relatively idle. Enter in hours and minutes the time that you want the system to be purged daily. You can enter any combination of hours and minutes within a 24-hour period in HH:MM format.

Step 3 The system periodically purges old data from the system. Enter the number of days when to purge data from the system. You can enter any number up to 1000.

Step 4 Purge the oldest data first when the system reaches a specified percent of capacity.

a) Enter the oldest data to purge, in number of days. You can choose any number.
b) Enter the percentage at which the database reaches capacity. You can choose any number up to 95.

Step 5 Click **Apply** to save your settings.

Configure Purge Notification

Use this procedure to configure purge notification settings.

Step 1 Choose **Administration** > **Historical Reporting** >**Purge Settings**.

Step 2 Specify to whom to send purge notifications by entering the recipient's full e-mail address.

The system notifies the e-mail recipient when the database size exceeds a specified percent of capacity. This step is required. Enter in number the percent at which the database reaches notification capacity. Range: 0-95.

Step 3 Click **Apply** to save your settings.

On-Demand Purging

Use this procedure to enable on-demand purging.

Step 1 Choose **Administration** > **Historical Reporting** >**Purge Settings**.

Step 2 Purge data older than a specified number of days by entering any number.

Step 3 Click the **Purge Now** button.

Note A warning dialog box appears alerting you that this operation is not reversible and that the action may delete historical reporting data.

Step 4 Select **Ok** or **Cancel** to complete the task.

CHAPTER 44

Reports

View Voice-Mail Reports

The Voice Mail Report window allows you to view the number of mailboxes currently configured, allocated mailbox space, time allotted for messages and greetings, and the total number of stored messages and greetings.

Choose **Reports** > **Voice Mail**. The Voice Mail Report contains the information shown in the following table. You cannot modify any information in this window.

Field	Description
# general delivery mailboxes	Number of group mailboxes that are configured.
# personal mailboxes	Number of individual mailboxes that are configured.
# orphaned mailboxes	Number of configured mailboxes that are not assigned to an individual or group.
Total message time (seconds)	Amount of time that is used for currently stored voice messages.
Total number of messages	The total number of voice messages that are stored.
Average message length (seconds)	Average length of voice messages that are stored.
Total greeting time (seconds)	The total amount of time used by the configured greetings.
Total number of greetings	The total number of greetings that are configured.
Average greeting time (seconds)	Average length of greetings that are configured.
Maximum voice message store (minutes)	Maximum storage capacity that is available for voice messages.

Field	Description
Total allocated space (minutes)	Amount of space that is allocated to the configured mailboxes.
Broadcast message count	Number of active broadcast messages in the system.
Future message count	The total number of future message queues.
Networking message count	Number of network messages in the network queue.
Messages left since boot	Number of messages left since the last reboot of the system.
Messages played since boot	Number of messages played since the last reboot of the system.
Messages deleted since boot	Number of messages deleted since the last reboot of the system.

View Mailboxes

Use this procedure to view Mailbox Reports.

Step 1 Choose **Reports** > **Mailboxes**. The window contains the following fields:

- Owner
- Number of messages
- New messages
- Saved messages
- Deleted messages
- Broadcast messages
- Future messages
- Faxes
- Time (in seconds)
- Used (percentage of the mailbox size that is in use)

Step 2 (Optional) You can select the number of rows to view per page from the drop-down in the lower left corner of the screen

View the Backup History Report

Use this procedure to view t he Backup History Report.

Choose **Reports** > **Backup History**. The Backup History report contains the following fields:

- ID—ID of the backup.
- Server URL—The server where the backup history is stored.
- Backup Time and Date—Date and time when the system was last backed up.
- Result—Status of the last backup procedure. Result shows Success or Fail.

View the Restore History Report

Use this procedure to view the Restore History Report.

Choose **Reports** > **Restore History**. The Restore History Report shows the history of all the restore processes done on the current system since installation.

View the Network Time Protocol Report

Use this procedure to view the Network time protocol (NTP) report.

Choose **Reports** > **Network Time Protocol**. The report contains the following fields:

- NTP Server—IP address or hostname of the NTP server.
- Status—Indicates if the NTP server connected with Cisco Unity Express or if it was rejected.
- Time Difference (secs)—Time offset between the NTP server and the client.
- Time Jitter (secs)—Estimated time error of the system clock, measured as an exponential average of RMS time differences.

Real Time Reporting

The Real time reporting (RTR) subsystem maintains real time statistics for various call-related and application-related events. You can configure various thresholds for system usage and these thresholds are used for displaying the system summary reports. These thresholds can be configured from the RTR applet only. If changed, the changed values will take effect immediately. Once configured, the threshold values will be saved by the subsystem and will persist across system reloads. The statistics are maintained in memory so a system reload will cause the statistics to get lost.

Use this procedure to initiate Real Time Reporting.

Choose **Reports** > **Real Time Reports**. Select from the following options:

- Reports—Displays a summary of the statistics, active contacts or applications, and database usage
- Tools—Choose from manual statistics reset options
- Settings—Configure polling related options and customize the look and feel of the applet. Allows you to configure the thresholds for system summary reports. These thresholds are used by the various System Summary report charts to delineate the color scheme. Green, yellow and red color codes to indicate normal, warning, and critical levels.
- System Summary—Displays active statistics and a summary of the statistics since last midnight.

CHAPTER 45

Help

About Help

If you have multiple Site names configured on the system, they will be listed in the About Cisco Communications Manager Express table. Use this procedure to view operating system information.

Choose **About** . The About window appears and contains the following information for your system:

- Cisco Unity Express version

  Cisco Unified Communications Manager Express information (CUCME mode only)

- Cisco Unified Communications Manager Express information includes the following:
  - Site Name
  - Operating System Router
  - Cisco IOS Software version
  - Cisco Unified CME version
  - Feature Package/Cisco IOS Image

Licensing Information

- Licensing information includes the following:
  - Default number of personal mailboxes
  - Default number of general delivery mailboxes
  - Maximum number of configurable mailboxes
  - Maximum message space, in minutes
  - Maximum number of telephony ports
  - Maximum number of voice-mail (VM)/auto attendant (AA) ports

- Maximum number of IVR ports
- Installed packets
- Installed languages

View System Reports

Use this procedure to view system reports.

Choose Help > System Information.

The following system specifications can be viewed from the System Information window:

- CPU Model
- CPU Speed (MHz)
- CPU Cache (KB)
- System Uptime
- Chassis Type
- Chassis Serial
- Module Type
- Module Serial