



Configuring Advanced Voice Mail

This chapter contains the following procedures for configuring advanced Cisco Unity Express voice mail features:

- [Configuring IMAP, page 1](#) (optional)
- [Configuring Live Record, page 9](#) (optional)
- [Configuring Live Reply, page 13](#) (optional)
- [Configuring the Delivery of Future Messages, page 21](#) (optional)
- [Configuring Nonsubscriber Message Delivery, page 23](#) (optional)
- [Configuring Broadcast Messages, page 26](#) (optional)
- [Configuring Restriction Tables, page 32](#) (optional)

Configuring IMAP

This section discusses the following topics:

- [Overview, page 1](#)
- [IMAP Server, page 2](#)
- [E-mail Client Considerations, page 2](#)
- [Configuring Integrated Messaging, page 5](#)
- [Displaying IMAP Sessions, page 8](#)

Overview

Integrated messaging on Cisco Unity Express is the convergence feature for voicemail and e-mail systems. It allows subscribers to have an integrated view of their e-mails and voice-mail messages from a single e-mail client using IMAP Version 4 rev1.

Subscribers can delete voice-mail messages or mark them as read or unread in a manner similar to e-mail messages.

The voice-mail messages are downloaded as attachments to e-mail messages. Subscribers can access the voice-mail messages over the network or can download them selectively. If the messages are downloaded, subscribers can play them locally using standard media players without requiring a connection to Cisco Unity Express.

REVIEW DRAFT - CISCO CONFIDENTIAL

Accessing voice-mail messages from general delivery mailboxes (GDMs) is not supported.

To access this feature, subscribers must be configured with the vm-imap privilege.

**Note**

The Cisco Unity Express module cannot be used as an SMTP server for sending and receiving e-mails.

IMAP Server

The IMAP server must be enabled on Cisco Unity Express before the server allows e-mail clients to connect. The feature can be enabled in the following modes:

- Non-SSL

Non-SSL is the least secure mode.

- SSL
- Mixed

This mode allows both SSL and non-SSL connections.

If you change the connection mode on the IMAP server, verify the configuration on the clients, which may need to be changed to match the IMAP server configuration.

The maximum number of simultaneous IMAP connections is determined by the module type. See the [Release Notes for Cisco Unity Express](#) for more information.

Any changes to the IMAP configuration require a restart of the IMAP server. You can restart the IMAP server using the **enable (IMAP)** command-line interface (CLI) command or a graphical-user interface (GUI) option.

E-mail Client Considerations

[Table 19-1](#) lists the IMAP e-mail clients that are supported.

Table 19-1 **IMAP Client Support**

IMAP Client	Cisco Unity Express Release:				
	8.5	8.6	9.0.x	10.0.x	10.1.0
Thunderbird 60.7.1			X	X	X
Iphone third party clients	X	X			
Cisco Mobile 8.0 (supported on Iphone)		X			
Cisco Unified Personal Communicator (CUPC) 8.5 ¹		X			

REVIEW DRAFT - CISCO CONFIDENTIAL**Table 19-1** IMAP Client Support (continued)

IMAP Client	Cisco Unity Express Release:				
	8.5	8.6	9.0.x	10.0.x	10.1.0
Cisco Unified Communications Integration™ for Microsoft Office Communicator 8.0 ¹		X			
Microsoft Outlook 2016			X	X	X
Microsoft Outlook 2010		X			
Microsoft Outlook 2007	X	X			
Microsoft Outlook 2003	X	X			
Microsoft Outlook 2002	X	X			
Microsoft Outlook 2000	X				
Microsoft Outlook Express 6.0	X				
Microsoft Entourage 2008		X			
Microsoft Entourage 2004	X				
Microsoft Windows Live Mail 12.0		X			
IBM Lotus Notes 10			X	X	X
IBM Lotus Notes 8.5		X			
IBM Lotus Notes 8.0		X			
IBM Lotus Notes 7.0		X			
IBM Lotus Notes 6.5	X				
IBM Lotus Notes 6	X				

1. This client is based on Client Services Framework, but can access Cisco Unity Express voicemail using the IMAP interface. See the [“Support for Client Services Framework \(CSF\)-Based Clients”](#) section on page 8.

**Note**

See the client documentation for their procedures for establishing connections to an IMAP server.

REVIEW DRAFT - CISCO CONFIDENTIAL

To connect to Cisco Unity Express, configure the e-mail client to accept the user ID and password of the Cisco Unity Express subscriber.



Note Subscribers cannot use the numeric PIN to log in to Cisco Unity Express through the e-mail client.

If this feature is enabled in SSL mode only, verify that the e-mail client is configured to use SSL connections to the IMAP server.

The same subscriber can connect to Cisco Unity Express from one or more e-mail clients using one or more connection types (SSL or non-SSL). Each session counts against the maximum number of connections allowed to the IMAP server.

Subscribers cannot retrieve the following types of messages from their personal mailboxes:

- Broadcast messages
- Private messages

The voice-mail messages are downloaded as .wav attachments to the Inbox folder of the e-mail clients.

If a subscriber receives a new message or saves a voice-mail message in the Inbox folder, the Cisco Unity Express retains the message in its database. If mandatory message expiry is enabled on Cisco Unity Express, the message is subject to the expiry timer.

If a subscriber moves a voice-mail message from the Inbox folder to another folder on the e-mail client, Cisco Unity Express deletes the message from its database. Mandatory message expiry would not affect that message.



Note Mandatory message expiry is not enforced on e-mail clients but is enforced on messages in the Cisco Unity Express database.

Cisco Unity Express supports the following operations on the e-mail clients:

- Mark Read/Unread

The Mark Read operation on the e-mail client is equivalent to Message Save on the voice-mail system. Similarly, the Mark Unread on the e-mail client is equivalent to the Mark New on the voice-mail system.

- Delete/Undelete
- Expunge (Purge)

Errors displayed on the e-mail clients are dependent on the client implementation. See the client documentation for more information.

The protocols supported determine the port that the IMAP client uses to connect to Cisco Unity Express. [Table 19-2](#) lists the supported ports for Cisco Unity Express 8.5 and earlier. [Table 19-3](#) lists the supported ports for Cisco Unity Express 8.6 and later.

REVIEW DRAFT - CISCO CONFIDENTIAL**Table 19-2** *IMAP Protocols and Ports Supported (Cisco Unity Express 8.5 and Earlier)*

IMAP server session security command setting	Port 143	Port 993
none	Supported	Not supported
mixed	Supported	Supported
ssl	Supported	Supported

Table 19-3 *IMAP Protocols and Ports Supported (Cisco Unity Express 8.6 and Later)*

IMAP server session security command setting	Port 143	Port 993	Port 7993 ¹
none	Supported	Not supported	Not supported
mixed	Supported	Supported	Supported (STARTTLS/LOGIN DISABLED ²)
ssl	Supported (STARTTLS/LOGIN DISABLED)	Supported	Supported (STARTTLS/LOGIN DISABLED)

1. Used for secure messages from CSF clients.

2. With this setting, the IMAP server does not allow IMAP clients to login if the client has not called STARTTLS yet.

Configuring Integrated Messaging

Follow this procedure to configure the Integrated Messaging capability.

Prerequisites

The system must have a default security certificate and private key installed before SSL connections are permitted on Cisco Unity Express. Use the **show crypto key** command to display the system default certificate-key pair. If no default pair exists, follow the procedure in [“Configuring Security” on page 1](#).

Required Data for This Procedure

Name of a subscriber group that has the vm-imap privilege.

REVIEW DRAFT - CISCO CONFIDENTIAL**SUMMARY STEPS**

1. **config t**
2. **service imap**
3. **enable**
4. **maxsessions** *num-sessions*
5. **session idletimeout** *minutes*
6. **session security** {*ssl* | **none** | **mixed** | **keyLabel** *labelname*}
7. **no enable**
8. **enable**



Note Any changes to the IMAP server configuration require a restart of the IMAP server for the changes to take effect. Steps 7 and 8 restart the IMAP server.

9. **end**
10. **groupname** *groupname* **privilege vm-imap**
11. **end**
12. **username** *username* **group** *groupname*
13. (Optional) **show imap configurations**
14. (Optional) **show imap sessions**

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t Example: se-10-0-0-0# config t	Enters configuration mode.
Step 2	service imap Example: se-10-0-0-0(config)# service imap	Enters Integrated Messaging configuration mode.
Step 3	enable Example: se-10-0-0-0(config-imap)# enable	Enables the Integrated Messaging feature on a system-wide basis.
Step 4	maxsessions <i>num-sessions</i> Example: se-10-0-0-0(config-imap)# maxsessions 25	Specifies the maximum number of concurrent IMAP client sessions. Valid values are 1 to 50. Default is 50.

REVIEW DRAFT - CISCO CONFIDENTIAL

	Command or Action	Purpose
Step 5	session idletimeout <i>minutes</i> Example: se-10-0-0-0(config-imap)# session idletimeout 45	Specifies the number of minutes an IMAP session can be idle. After this maximum is reached, the system automatically disconnects the session. Valid values are 30 to 120 minutes. The default is 30 minutes.
Step 6	session security { ssl none mixed keyLabel <i>labelname</i> } Example: se-10-0-0-0(config-imap)# session security ssl	Specifies the type of IMAP connections accepted from IMAP clients. Any IMAP client trying to make any other type of connection will be rejected. <ul style="list-style-type: none"> • ssl—Only SSL connections are permitted. • none—Only non-SSL connections are permitted. • mixed—Both SSL and non-SSL connections are permitted. • keylabel <i>labelname</i>—Associates the certificate-key pair to the SSL connection. If this option is not specified, then IMAP uses the default certificate key. <p>Note The system displays an error message if the certificate-key pair are not configured as the system default before configuring SSL connections for the IMAP client. Beginning with Cisco Unity Express 3.2, you can use the keyLabel option to associate the certificate-key pair to the SSL connection. See “Configuring Security” on page 1 to set the certificate-key pair.</p>
Step 7	no enable Example: se-10-0-0-0(config-imap)# no enable	Disables the Integrated Messaging feature on a system-wide basis.
Step 8	enable Example: se-10-0-0-0(config-imap)# enable	Enables the Integrated Messaging feature on a system-wide basis. This step restarts the IMAP server.
Step 9	end Example: se-10-0-0-0(config-imap)# end	Exits Integrated Messaging configuration mode
Step 10	groupname <i>groupname</i> privilege vm-imap Example: se-10-0-0-0(config)# groupname sales privilege vm-imap se-10-0-0-0(config-imap)# groupname imap-users privilege vm-imap	Specifies an existing group that will have access to the Integrated Messaging capability. Repeat this step if more than one group will have Integrated Messaging access.

REVIEW DRAFT - CISCO CONFIDENTIAL

	Command or Action	Purpose
Step 11	end Example: se-10-0-0-0(config)# end	Exits configuration mode.
Step 12	username <i>username</i> group <i>groupname</i> Example: se-10-0-0-0# username user4 group sales	Assigns a subscriber to the group.
Step 13	show imap configurations Example: se-10-0-0-0# show imap configuration	(Optional) Displays all Integrated Messaging configuration parameters.
Step 14	show imap sessions Example: se-10-0-0-0# show imap sessions	(Optional) Displays all active Integrated Messaging sessions.

Examples

The following example shows sample output from the **show imap configuration** command:

```
se-10-0-0-0# show imap configuration
```

```
Status:                enabled
Idle Timeout(minutes)  45
Max Sessions:          25
Security Mode:         ssl
```

The following example shows sample output from the **show imap sessions** command:

```
se-10-0-0-0# show imap sessions
```

```
Sessions      IP Address      Connect Time      User ID
=====
1             10.21.82.244    Wed Nov 16 07:35:02 CST 2005    sales
2             172.18.10.10    Wed Nov 16 08:23:15 CST 2005    imap-users
3             172.18.10.5     Wed Nov 16 10:11:40 CST 2005    imap-users
```

Displaying IMAP Sessions

To display IMAP sessions, see [“Monitoring Active IMAP and VoiceView Express Sessions”](#) on page 7.

Support for Client Services Framework (CSF)-Based Clients

Client Services Framework (CSF) is a common component that client applications use to integrate with the Cisco Unified Communications suite of products on Windows PC platforms. CSF delivers Cisco Unified Communications features/services to client applications in a common and consistent manner. Client applications based on CSF can access voicemail from CUE using the IMAP interface.

REVIEW DRAFT - CISCO CONFIDENTIAL

Cisco Unity Express 8.6 supports the following clients that are based on CSF:

- [Cisco Unified Personal Communicator \(CUPC\) 8.5](#)
- [Cisco Unified Communications Integration™ for Microsoft Office Communicator 8.0](#)

The configuration to support the CSF clients is the same as for configuring IMAP clients. See the [“Configuring IMAP” section on page 1](#).



Note

To support the receipt of incoming secure messages from CSF clients, the IMAP server **session security** command must be configured to either the “mixed” or “ssl” setting. The CSF client must use port 7993 to connect to Cisco Unity Express. For more information about secure messaging, see the [“Configuring Secure Messaging” section on page 33](#).

Configuring Live Record

This section discusses the following topics:

- [Overview, page 9](#)
- [Configuring Live Record, page 11](#)



Warning

For legal disclaimer information about this feature, see page ii.

Overview

This feature enables Cisco Unity Express subscribers to record live conversations and store the recording as a message in their mailbox. They can then play it or forward it to another subscriber or group of subscribers. This feature can also be used between Cisco Unity Express subscribers and nonsubscribers. Do this by conferencing the nonsubscriber’s call leg into a Cisco Unity Express recording session and then recording the conversation to the appropriate mailbox. To alert participants that the call is being recorded, Cisco Unity Express periodically beeps.

The recording stops automatically when the call leg to the Cisco Unity Express recording session is terminated or the subscriber’s voice mailbox is full, whichever occurs first. Depending on the Cisco Unified Communications Manager or Cisco Unified CME settings, the call leg can terminate either when the conference initiator ends the call or when the last participant ends the call. After the conference is terminated, the voice conversation can continue without further recording. When the live-record session is stopped, the recording is put in the new message state and the MWI is triggered.

Each recording can be saved, deleted, or forwarded just like any other voice mail message and are addressed as being from the subscriber. The recording is applied against the subscriber’s mailbox limit until it is deleted.

You can only enable the live-record feature globally for Cisco Unity Express; you cannot enable it on a per-user basis. To initiate a live-record session, users conference to an extension configured as call-forward-all on Cisco Unified Communications Manager or Cisco Unified CME and is setup to forward all incoming calls to the voice mail pilot number.

The maximum number of live-record sessions is controlled by the **voicemail pilot number maxsessions** trigger setting. The size of live-record messages is limited only by the amount of space remaining in the subscriber’s voice mailbox. Live-record messages do not trigger the cascading message notification feature.

REVIEW DRAFT - CISCO CONFIDENTIAL**Note**

Using a speaker phone with the live record feature can cause clipping of the recorded voice.

Configuration

To configure the live-record feature, you must:

- Configure ad-hoc conferencing for Live Record.

This configuration includes:

- Enabling dspfarm services on the voice-card that has voice DSPs for conferencing on the Cisco IOS voice gateway.
- Enabling SCCP on Cisco Unified CME and creating a SCCP CCM Group to register to Cisco Unified CME.
- Binding the SCCP protocol to an interface on the voice card or ethernet interface of the router.
- Setting up the Conferencing DSP Farm and enable all the codecs (taking into consideration local calls, a G711 codec leg to Cisco Unity Express and calls across SIP Trunk (if any) that will be using the Live Record feature.
- Associating the Cisco Unified CME to the DSP Profile and provide a device name for the conferencing resource to register with Cisco Unified CME.
- Enabling hardware conferencing on Cisco Unified CME (telephony-service) and specifying the device-name of the conferencing resource that will register with Cisco Unified CME.
- Defining an Ad-Hoc DN to support Ad-Hoc Conferencing

**Note**

Beginning with Cisco Unified CME 4.3, you can add an octo-line DN which has 8 channels on the DN. Each party will need one channel on the DN, so octo-line DN will support 8 conferencing parties. On Cisco Unified CME 4.1 and 4.2, the ephone-dn cannot be configured for octo-line so use dual-line and create four such dual-line DNs to support 8 party conference.

For more information on how to configure the Live Record feature on Cisco Unified CME, see the [Cisco Unified Communications Manager Express System Administrator Guide](#).

- Configure Live Record and Voicemail pilots numbers on Cisco Unified CME.
- Setup a Live Record DN and Call Forward it to the voice mail pilot number.
- Configure a dial-peer pointing the VM pilot to Cisco Unity Express.
- On Cisco Unified CME 4.3, optionally create a Live Record (LiveRcd) softkey for the ephones that will use the LiveRcd feature and assign the template to the ephones.

The LiveRcd softkey is used to start and stop a live recording.

- Configure a live-record pilot number on Cisco Unity Express.

Use the **voicemail live-record pilot-number digits** command and supply the live-record pilot number as the *digits* argument.

- Optionally configure the beep duration and interval for live record on Cisco Unity Express.

You can configure the beep duration and interval on Cisco Unity Express as needed to satisfy any applicable laws concerning notification that a call is being recorded. By default, the beep duration is 250 milliseconds and the beep interval is 15 seconds.

REVIEW DRAFT - CISCO CONFIDENTIAL

Using Live-Record

After live-record is properly configured, users can use the following sequence of steps to initiate a live-record session. This example assumes a call is already established. The subscriber wanting to record the conversation does not need to be the caller who initiated or received the call.

1. Initiate a conference to the Cisco Unity Express live-record pilot number.
Press the conference softkey button. The current conversation is paused.
2. Dial the live-record pilot extension number.
3. The live-record pilot extension forwards the call request to the voice mail pilot number.
4. Cisco Unity Express answers the incoming call, detects the live-record pilot extension, and begins recording if the call referrer is a valid Cisco Unity Express subscriber.
5. Complete the conference.
Press the conference softkey button again. At this point, everything either party says is recorded except the beeps played by Cisco Unity Express.

To end the live-record session, remove the Cisco Unity Express from the conference and continue the call, or hang up and terminate the call.

Error Conditions

The following error conditions can occur for subscribers using live-record:

- No Ports Available — Busy tone plays to the caller
- Invalid Extension (caller is not a local subscriber) — Message plays that explains there is no mailbox associated with the extension.

Limitations

Create a conference soft key and a live-record speed dial key. This gives users the following three-button solution:

1. Press the conference soft key
2. Press the live-record speed dial key
3. Press the conference soft key

Live-record is only available to Cisco Unity Express local subscribers. Remote subscribers or external callers cannot use this feature because it uses the extension number assigned to the caller. However, this feature does not provide a prompt to ask the user to identify the extension and password and help prevent remote users from attempting to use the service.

Live-recorded messages do not trigger a message notification when delivered to the voice mailbox.

Configuring Live Record

Prerequisites

- Cisco Unity Express 3.0 or a later version

REVIEW DRAFT - CISCO CONFIDENTIAL

- Configure the Live Record feature on Cisco Unified CME and Cisco IOS voice gateway as described in the “Configuration” section on page 10 and the *Cisco Unified Communications Manager Express System Administrator Guide*.

Required Data for This Procedure

Configure the pilot number that you want to use for live recording (the extension number used to forward all incoming calls to the Cisco Unity Express voice mail pilot number).

SUMMARY STEPS

1. **config t**
2. **voicemail live-record pilot-number** *digits*
3. **voicemail live-record beep duration** *digits*
4. **voicemail live-record beep interval** *digits*
5. **end**
6. (Optional) **show voicemail live-record**

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t Example: se-10-0-0-0# config t	Enters configuration mode.
Step 2	voicemail live-record pilot-number <i>digits</i> Example: se-10-0-0-0(config)# voicemail live-record pilot-number 0210	Enables the live-record feature and sets the extension number used to forward all incoming calls to the Cisco Unity Express voice mail pilot number. All calls terminated on the Cisco Unity Express voice mail pilot number from this location will bypass the usual voice mail greeting and immediately start recording if the caller is a subscriber. Note Do not associate the Live Record pilot CTI port with the JTAPI user (for Cisco Unified Communications Manager environments).
Step 3	voicemail live-record beep duration <i>digits</i> Example: se-10-0-0-0(config)# voicemail live-record beep duration 240	Sets the duration of the live-record beep, which is the elapsed time from when a beep starts playing to when it finishes playing. The range is 50 to 1000 milliseconds.
Step 4	voicemail live-record beep interval <i>digits</i> Example: se-10-0-0-0(config)# voicemail live-record beep interval 12	Sets the live-record beep interval, which is the elapsed time from the end of one beep and the start of the next beep. The range is 1 to 30 seconds.

REVIEW DRAFT - CISCO CONFIDENTIAL

	Command or Action	Purpose
Step 5	end Example: se-10-0-0-0(config)# end	Exits to privileged EXEC mode.
Step 6	show voicemail live-record Example: se-10-0-0-0# show voicemail live-record	(Optional) Displays the current configuration for the live-record feature.

Examples

The following are samples of output for the **show voicemail live-record** command:

```
se-10-0-0-0# show voicemail live-record
```

```
Status: enabled
pilot number: 0295
Conversation beep settings
  duration: 250 milliseconds
  interval: 15 seconds
```

```
Status: disabled
pilot number: disabled
Conversation beep settings
  duration: disabled
  interval: 15 seconds
```

Configuring Live Reply

This section discusses the following topics:

- [Overview, page 13](#)
- [Configuring Live Reply, page 17](#)

Overview

This feature enables Cisco Unity Express subscribers who listen to the voice messages by phone or VVE to reply to another user's message by pressing 4-4. When this feature is invoked, Cisco Unity Express attempts to establish a call between the two parties. If the attempt is successful, the subscriber is connected to the called party or the voice call is forwarded based on rules defined by the called party. After the call is ended, the initial connection to voice mail is disconnected and the subscriber is not returned to their voice mail session. To review other voice mail messages after a successful live-reply session, the subscriber must redial the voice mail pilot number.

The behavior when there is a call failure is determined by the system's transfer-mode setting (see the transfer-mode subcommand for the **ccn subsystem sip** command). If transfer mode is set to *blind*, the connection to voice mail is lost when the call is either succeeds or fails. If transfer mode is *semi-attended* or *attended*, the connection to voice mail is retained when there is any call failure, such as an invalid number or busy. The message state is not changed by this feature. For example, if the subscriber is listening to a new message and decides to invoke this feature, the message remains in the new state.

REVIEW DRAFT - CISCO CONFIDENTIAL

Subscribers can use this feature with regular or deleted messages but cannot be used with messages from the local General Delivery Mailbox (GDM), broadcast messages, expired messages, NDR, or DDR. When subscribers attempt to use this feature with any of these messages, they receive an error voice prompt and are returned to the voice mail menu from which they tried to invoke this feature.

The following sections describe how the two methods of access this feature:

- [Accessing Live-Reply from the TUI, page 14](#)
- [Accessing Live-Reply from VVE, page 14](#)

Accessing Live-Reply from the TUI

Subscribers can use the live-reply feature from the following three TUI menus:

- New Messages
- Saved Messages
- Deleted Messages

To live-reply to a message, the subscriber must first listen to a message in one of the above queues. The subscriber can also use live reply when the message review menu is played giving the options to reply or forward the message. To use live reply, the subscriber must press 4-4 in sequence.

Accessing Live-Reply from VVE

Unlike the TUI, in VVE there is only one list of voice mail messages. All messages that qualify for live-reply have an additional menu that is displayed when you press the Reply button. This menu allows the subscriber to select the normal voice mail reply or allow a live reply if the caller's information is available.

If the message is forwarded, the live reply feature connects to the last number from which the message was forwarded.

By default, live-reply is disabled. Use either the CLI or GUI at the system level to enable live-reply. Users cannot configure this feature.

This feature uses the E.164 number to make the outbound call. Therefore, the number of the calling party returned as part of voice call must be dialable. How the senders E.164 number is determined depends on how the voice mail was delivered to the subscriber's mailbox. The two possible methods of delivery are:

- Telephone delivered voice mail
- VPIM (Network) delivered voice mail

These methods are discussed in the following sections.

Telephone Delivered Voice Mail

An example of this scenario is when the sender of voice mail calling a subscriber is forwarded to the subscriber's voice mailbox. If the calling party information exists for the sender, it is stored in the voice mail message envelope. The subscriber can listen to this message and attempt to live reply to this message. If the calling party information is not available, attempting to live-reply to a message results in an "Invalid option" error. For more information, see the ["Limitations" section on page 15](#).

REVIEW DRAFT - CISCO CONFIDENTIAL

VPIM (Network) Delivered Voice Mail

To support this feature, the network message delivered using VPIM between Cisco Unity Express nodes or between Cisco Unity Express and Cisco Unity contains the E.164 number, starting in version 3.0 (if it is configured and available for the subscriber).

You can configure the live-reply feature so that it can be used with existing VPIM capable systems that send only the subscriber's mailbox number (which may or may not be the appropriate E.164 number) instead of the E.164 number. Do this by setting up a rule to define each remote location in your Cisco Unity Express configuration that will be used to determine which E.164 number to dial to reach the author of the VPIM delivered voice mail. This determination is done based on network configuration location settings.

You can configure this rule to use one of the following options as the sender's E.164 number:

- Sender's mailbox ID as the E.164 phone number. This number is found in the VPIM message header from field in the digits before the "@" character.
- Combination of the configured network location prefix followed by the sender's mailbox ID. The network location prefix is given in the location subcommand with the command **voicemail phone-prefix** *prefix-digits*.
- Combination of the network location ID followed by the sender's mailbox ID. The network location ID is specified when defining a network location with the command **network location ID** *location-digits*.
- Concatenation of network location ID, followed by network location prefix, followed by mailbox ID.
- Concatenation of network location prefix, followed by network location ID, followed by mailbox ID.

By default, Cisco Unity Express uses the E.164 number supplied by a peer 3.1 or later version system in the VPIM header, if present. Otherwise it uses the configured rule to determine the E.164 number to use for this message.

In some cases, you can reconfigure remote sites to use the mailbox ID as the E.164 number to dial for live reply. You can use this configuration when:

- The Cisco Unity Express subscriber mailbox IDs are unique across the network and therefore, the mailbox ID is the same as the subscriber extension.
- The Cisco Unified Communications Manager or Cisco Unified CME is also configured to dial from site to site by subscriber extension.

You probably have overlapping extensions between sites. In this case, Cisco Unity Express could be configured to use the remote systems phone prefix with the subscriber's mailbox ID to derive the E.164 number to dial. You can use this method if you configure your Cisco Unified Communications Manager or Cisco Unified CME to implement this dial plan and transform the mailbox ID received in the VPIM message into a unique E.164 address.

In addition to determining how to derive the E.164 phone number to use with live reply, you can also set the precedence of the VPIM E.164 number over the rule derived phone number.

Limitations

Live-reply cannot apply call restrictions on a per-subscriber basis. Because the outbound dialing is from Cisco Unity Express on behalf of the user, any restrictions on dialed numbers must be applied to all users equally. There cannot be a privileged set of Cisco Unity Express subscribers that have a broader set of

REVIEW DRAFT - CISCO CONFIDENTIAL

live-reply dialed numbers. For example, subscribers cannot be divided into groups (such as employees and management) where one group (management) can live-reply to all locations and the other group (employees) can only live-reply to local extensions.

If you use a complex dial-plan, it might be difficult or impossible to configure live-reply to correctly handle remotely delivered VPIM messages. If the remote system is Cisco Unity or an earlier version of Cisco Unity Express, the live-reply number is not included in the VPIM header. This makes it difficult or impossible to determine the E.164 number Cisco Unity Express must dial to reach the sender. For example, a dial plan where mailbox IDs are unrelated to user extensions may make it impossible for the system to derive the E.164 number to call.

Configuration

You can configure the following items for the Live Reply feature:

- Network-precedence
- Calling-number-rule
- Prepend digits for the calling-number-rule
- Restriction table

These items are explained in the following sections.

Network Precedence

Network precedence determines which E.164 number Cisco Unity Express dials when making a live-reply to a VPIM delivered message. It specifies the priority of the following methods of determining the live-reply E.164 number:

- Use only the number of the sender contained in a VPIM message (if present).
- Use the number of the sender contained in a VPIM message (if present). Otherwise, use the number derived using the calling-number-rule CLI described below.
- Use only the number derived using the calling-number-rule CLI described below.

Calling Number Rule

The calling number rule specifies how the live-reply extension is derived from configuration and VPIM vcard data. Knowing the callers E.164 number is essential for live-reply functionality. Note however, knowing the E.164 number for the sender of a voice mail is not required if live-reply disabled.

Table 19-4 defines the behavior of the options for deriving a sender's E.164 number. The last column shows an example of the derived number, assuming that the location ID is configured as 111, the location prefix is configured to 444, and the mailbox ID of the incoming VPIM message is 5678.

REVIEW DRAFT - CISCO CONFIDENTIAL**Table 19-4 Behavior of the Options for Deriving a Sender's E.164 Number**

Option	Description	Example
extension	Use the sender's mailbox ID as the E.164 phone number. This number is in the VPIM message header from field in the digits before the "@" character.	5678
prefix-extension	Use the combination of the configured network location prefix followed by the sender's mailbox ID. The network location prefix is in the location subcommand with the command voicemail phone-prefix <i>prefix-digits</i>	444-5678
location-extension	Use the combination of the network location ID followed by the sender's mailbox ID. The network location ID is specified when defining a network location with the command network location ID <i>location-digits</i> .	111-5678
location-prefix-extension	Use the concatenation of network location ID, followed by network location prefix, followed by mailbox ID.	111-444-5678
prefix-location-extension	Use the concatenation of network location prefix, followed by network location ID, followed by mailbox ID.	444-111-5678

Prepend Digits

This setting specifies any additional digits that you want to be dialed before the calling-number rule derived E.164 number for a remote subscriber.

Restriction Table

The restriction table enable you to control how the live reply feature is used. As described in the [“Configuring Restriction Tables” section on page 32](#), use the following parameters to define a restriction table:

- **preference** — Order of this string in the restriction table. The system searches the strings in order of preference, starting with 1. Valid values are 1 to 10.
- **pattern** — Call pattern to be matched. Valid characters are digits 0 to 9, asterisk (*), or dot (.). The table accepts duplicate call patterns.
- **allowed** — Permits phone numbers with this pattern to be assigned to message notification devices.
- **disallowed** — Prevents phone numbers with this pattern from being assigned to message notification devices.
- **insert** — Inserts the dial string in the proper place in the table.

Configuring Live Reply**Prerequisites**

- Cisco Unity Express 3.0 or a later version
- To restrict specified extensions from using this feature, you must configure a restriction table as described in the [“Configuring Restriction Tables” section on page 32](#).

REVIEW DRAFT - CISCO CONFIDENTIAL

Required Data for This Procedure

This procedure requires the prepend digits (any additional digits that you want dialed before the calling-number rule derived E.164 number for a remote subscriber).

SUMMARY STEPS

- 1. `config t`
- 2. `voicemail live-reply enable`
- 3. `voicemail live-reply network-precedence {phonenumberE164 [calling-number-rule] | calling-number-rule}`
- 4. `voicemail live-reply calling-number-rule {extension | prefix-extension | location-extension | location-prefix-extension | prefix-location-extension}`
- 5. `voicemail live-reply restriction table-name`
- 6. `network location id ID_number`
- 7. `calling-number-rule prepend-digits digits`
- 8. `end`
- 9. (Optional) `show voicemail live-reply`
- 10. (Optional) `show network detail location id loc-id`
- 11. (Optional) `show voicemail live-reply restriction-table`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>config t</code> Example: <code>se-10-0-0-0# config t</code>	Enters configuration mode.
Step 2	<code>voicemail live-reply enable</code> Example: <code>se-10-0-0-0(config)# voicemail live-reply enable</code>	Enables the Live Reply feature on a system-wide basis.

REVIEW DRAFT - CISCO CONFIDENTIAL

	Command or Action	Purpose
Step 3	voicemail live-reply network-precedence {phonenumberE164 [calling-number-rule] calling-number-rule} Example: se-10-0-0-0(config)# voicemail live-reply network-precedence calling-number-rule	Determines which live-reply E.164 number Cisco Unity Express dials when making a live-reply to a VPIM delivered message. Specifies the use of one of the following methods of determining the live-reply E.164 number: <ul style="list-style-type: none"> • Use only the number of the sender contained in a VPIM message (if present) • Use the number of the sender contained in a VPIM message (if present). Otherwise, use the number derived using the calling-number-rule CLI described in Step 4 below. • Use only the number derived using the calling-number-rule CLI described in Step 4 below.
Step 4	voicemail live-reply calling-number-rule {extension prefix-extension location-extension location-prefix-extension prefix-location-extension} Example: se-10-0-0-0(config)# voicemail live-reply calling-number-rule location-extension	Specifies how the live-reply extension is derived from the configuration and the VPIM vcard data. This determines how to construct the remote subscriber's E.164 phone number. For more information, see the “Calling Number Rule” section on page 16 Table 19-3 .
Step 5	voicemail live-reply restriction table-name Example: se-10-0-0-0(config)# voicemail live-reply restriction live-reply-r-table	Associates a restriction table to the live reply feature.
Step 6	network location id ID_number Example: se-10-0-0-0(network)# network location id 112	Enters network location mode.
Step 7	calling-number-rule prepend-digits digits Example: se-10-0-0-0(config)# calling-number-rule prepend-digits 91	Specifies additional digits to dial before the calling-number rule derived E.164 number for a remote subscriber.
Step 8	end Example: se-10-0-0-0(config)# end	Exits to privileged EXEC mode.
Step 9	show voicemail live-reply Example: se-10-0-0-0# show voicemail live-reply	(Optional) Displays the current configuration for the live-reply feature.

REVIEW DRAFT - CISCO CONFIDENTIAL

	Command or Action	Purpose
Step 10	show network detail location id <i>loc-id</i> Example: se-10-0-0-0# show network detail location id 112	(Optional) Displays information about the current network location, including the prepend digits setting.
Step 11	show voicemail live-reply restriction-table Example: se-10-0-0-0# show voicemail live-reply restriction-table	(Optional) Displays the restriction-table associated with the live-reply feature.

Examples

The following is sample output for the **show voicemail live-reply** command:

```
se-10-0-0-0# show voicemail live-reply

Status:                enabled
Remote subscriber dialing
    calling number rule: location+prefix+extension
    number preference:   E164 number then calling number rule

Restriction Table:      live-reply-restriction
Minimum digits allowed: 1
Maximum digits allowed: 30
Dial Strings:
Preference    Call Pattern    Allowed
1             19000...        yes
2             170000          yes
3             *            yes
```

The following example shows information about the remote Cisco Unity Express location with the ID of 102:

```
se-10-0-0-0# show network detail location id 102

Name:                Dallas/Fort Worth
Abbreviation:         DFW
Email domain:         dfw.mycompany.com
Minimum extension length: 2
Maximum extension length: 15
Phone prefix:         4
VPIM encoding:        dynamic
Send spoken name:     enabled
Send vCard:           enabled
State:               enabled
VPIM broadcast ID:    vpim-broadcast
Sent msg count:       0
Received msg count:   0
Live-reply calling number rule prepend: 91
```

The following is sample output for the **show voicemail live-reply restriction-table** command:

```
se-10-0-0-0# show voicemail live-reply restriction-table

Restriction Table: live-reply-restriction
Minimum digits allowed: 1
Maximum digits allowed: 30
```

REVIEW DRAFT - CISCO CONFIDENTIAL

Dial Strings:

Preference	Call Pattern	Allowed
1	19000...	yes
2	170000	yes
3	*	yes

Configuring the Delivery of Future Messages

Cisco Unity Express subscribers may create and schedule voice-mail messages for future delivery to one or more subscribers on the local system or on configured remote network locations.

You do not need to configure this feature for subscribers.

Subscribers can schedule message delivery for up to 1 year in advance.

Senders can readdress, rerecord, and review the message before scheduling it for delivery. After the system confirms the date and time for the future delivery, the sender cannot change or delete the message.

You can display and delete messages marked for future delivery.

A subscriber can schedule any number of messages for future delivery if the subscriber's mailbox has enough space. The system counts all the sender's future messages against the sender's quota until a message is sent. After a future message is delivered, it is counted against the recipient's quota.

The following sections describe this feature:

- [Permitted Subscribers, page 21](#)
- [Message Delivery Time, page 21](#)
- [System Status Impact, page 22](#)
- [Unsuccessful Message Delivery, page 22](#)
- [Loss of Future Messages, page 22](#)
- [Incorrect Message Delivery, page 22](#)
- [Backup and Restore of Future Messages, page 23](#)
- [Displaying and Deleting Future Messages, page 23](#)

Permitted Subscribers

No special privileges are required to use this feature.

All subscribers configured on the system have access to this feature.

Message Delivery Time

Any change or drift in the system time impacts the message delivery. For example, a sender schedules a message for a 4:00 p.m. delivery when the system time is 3:00 p.m.

- If the system time jumps ahead by 15 minutes, the system delivers the message at its new 4:00 p.m. Only 45 minutes, not 1 hour, separates the original scheduling of the message delivery and the actual delivery.
- If the system clock falls behind by 15 minutes, the system delivers the message at 4:00 p.m., which is 1 hour and 15 minutes from the time of the original scheduling.

REVIEW DRAFT - CISCO CONFIDENTIAL

- If the system time moves forward beyond the scheduled time, such as by 2 hours, the system delivers the message immediately after the time change.

System Status Impact

If the sending system is in a shutdown state with messages scheduled to be delivered during that time, the system delivers the messages when the system is up again.

If the sending system is in an “offline” state with messages scheduled to be delivered during that time, the system delivers the messages when the system returns to the “online” state.

Unsuccessful Message Delivery

If you change the IP address or hostname of the remote location before delivery of a scheduled message, the system delivers the message successfully.

Message delivery fails in the following situations:

- Networking is disabled on a sending system before delivering a scheduled message to a remote network location.

For example, location A has a message scheduled for delivery to remote location B on 15-April-2006. You disable location A on 14-April-2006. Message delivery fails.

- Networking is disabled on the remote location before delivery of the scheduled message.
- The remote location is disabled before delivery of the scheduled message.

In all cases, the system generates a nondelivery receipt (NDR).

Loss of Future Messages

Multiple scenarios can cause the loss of future messages:

- If you delete a sender's mailbox, the system deletes any scheduled messages from that sender.
- If the sender's mailbox is disabled, the system does not delete the messages immediately. At the scheduled time, the system checks the status of the sender's mailbox. If the mailbox is enabled, the system delivers the scheduled message. If the mailbox is disabled, the system deletes the messages.
- If the recipient or remote location of a scheduled message is deleted, the system does not delete the scheduled message immediately. At the time of delivery, the system checks if the recipient or remote location is deleted. If the recipient or remote location is restored, the system delivers the message successfully. If the recipient or remote location is deleted, the system deletes the message and generates an NDR.

Incorrect Message Delivery

Subscriber or network configuration changes may impact delivery of scheduled messages.

- A message is scheduled for delivery on 12-April-2006 to Subscriber1 at extension 1234 at remote location A. On 11-April-2006, you change Subscriber1's extension to 5678. The system cannot deliver the message and generates an NDR.

REVIEW DRAFT - CISCO CONFIDENTIAL

- A message is scheduled for delivery on 12-April-2006 to Subscriber1 at extension 1234 at remote location A. On 11-April-2006, you delete Subscriber1 and gives Subscriber1's extension to Subscriber2. The system delivers the scheduled message successfully to Subscriber2.

Backup and Restore of Future Messages

The system backs up messages scheduled for future delivery as part of a data backup. When that backup is restored, the system delivers the scheduled messages at the appropriate times. If the scheduled delivery time is in the past, the system delivers those messages when as the system is restored.

Recipients may receive a scheduled message more than once. For example, you back up the system on 20-March-2006. This backup contains messages scheduled for 25-March-2006. On 26-March-2006, the system experiences a power outage. The administrator uses the 20-March-2006 backup to restore the system. The system redelivers the scheduled messages contained in the backup file.

Displaying and Deleting Future Messages

To display and delete future messages, see [“Monitoring Future Messages” on page 6](#).

Configuring Nonsubscriber Message Delivery

This section discusses the following topics:

- [Overview, page 23](#)
- [Configuring Nonsubscriber Message Delivery, page 24](#)

Overview

This feature gives Cisco Unity Express subscribers the ability to record a voice message and send it to an external number or nonsubscriber at the predefined time up to 1 year in advance. The subscriber who is sending the message can readdress and rerecord the message, change the message delivery options, and review the message while setting it up for delivery. You can also use the same functionality to simply forward a voice message.

Messages with no audio, typically faxes and fax NDR, may not be forwarded to an external number. Only faxes with a voice attachment are allowed.

After subscribers configure messages for delivery, they do not receive any indication that there are messages marked for delivery to nonsubscribers. However, the administrator can view and delete any messages that are marked for future delivery to nonsubscribers. To provide this functionality, enhancements to the future delivery commands are included with this feature.

Limitations to this functionality include:

- Messages that are composed and sent immediately cannot be deleted or recalled.
- No validations are performed for the external numbers. (However, they are checked against the dialing restriction table with which they are associated.)
- You can use a maximum of five external numbers for addressing a message.
- The number of simultaneous calls out to external numbers is limited to two.

REVIEW DRAFT - CISCO CONFIDENTIAL

The subscribers use the same method as before 3.0 to send messages or to compose messages for future delivery. To send a message to nonsubscribers, subscribers enter the nonsubscriber number when the TUI prompts them to enter the recipients' number after pressing #4. The system does not attempt to validate any of these numbers.

The message is delivered to the called number regardless of who answers the phone or whether the called number is forwarded to another number. The messages are delivered based on the current system time (within a grace period of 5 minutes of the actual scheduled time). A message is delivered successfully when:

- The called number picks up and answers.
- The called number is forwarded to another number and is then picked up and answered.

If a system is shutdown or offline and it has messages scheduled to be delivered during that period, those messages are delivered when the system is running again.

When a subscriber's mailbox is deleted, all messages scheduled for delivery by that subscriber are also deleted. However, the messages are not deleted when a subscriber's mailbox is disabled. When a message is scheduled to be delivered, the system verifies that sender's mailbox is enabled. A message is discarded only if the mailbox is disabled at that time.

Any messages scheduled for delivery are backed up as part of a regular data backup. When you restore a backup, all messages in the backup that are scheduled for delivery are sent to the recipients as specified. If the scheduled delivery time of some of the messages have passed, they are sent when the system is up after the restore. Therefore, it is possible for recipients to receive a message more than once.

Messages to nonsubscribers are contained in the future message queue until their scheduled time of delivery. These messages are counted as part of the sender's quota until they are removed from the message queue. A subscriber can schedule any number of messages for the delivery, if there is space available in their mailbox.

When a message is delivered, the prompt played to nonsubscribers is one of the following:

- "Hello. This is the Cisco Unity Express Messaging System. You have a message from *spoken_name* at *E164_extension*. To listen to the message, press 1."
- "Hello. This is the Cisco Unity Express Messaging System. You have a message from *E164_extension*. To listen to the message, press 1."
- "Hello. This is the Cisco Unity Express Messaging System. You have a message from an unknown sender. To listen to the message, press 1."

After listening to a message, a nonsubscriber can repeat the playing of the message up to two times by responding to the prompt "To repeat this message, press 1."

When a subscriber sends a message to a nonsubscriber and the sending subscriber's mailbox is full, the message cannot be delivered. If this is the case, the following prompt is played to the sender:

"Your message could not be delivered to extension *external_number*. Your mailbox is full. You cannot send messages to a phone number. To send another message, press 1. To exit, press *."

Configuring Nonsubscriber Message Delivery

Prerequisites

- Cisco Unity Express 3.0 or a later version
- To restrict this feature from delivering messages to specified external numbers, you must configure a restriction table as described in the ["Configuring Restriction Tables" section on page 32](#).

REVIEW DRAFT - CISCO CONFIDENTIAL**Required Data for This Procedure**

Name of the restriction table you want to associate with this feature.

SUMMARY STEPS

1. **config t**
2. **voicemail non-subscriber restriction** *table-name*
3. **end**
4. (Optional) **show voicemail messages future**
5. (Optional) **show voicemail non-subscriber restriction-table**

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t Example: se-10-0-0-0# config t	Enters configuration mode.
Step 2	voicemail non-subscriber restriction <i>table-name</i> Example: se-10-0-0-0(config)# voicemail non-subscriber restriction non-subscriber-r-table	Associates a restriction table to the nonsubscriber message delivery feature
Step 3	end Example: se-10-0-0-0(config)# end	Exits to privileged EXEC mode.
Step 4	show voicemail messages future Example: se-10-0-0-0# show voicemail messages future	(Optional) Displays the future message delivery, including the external numbers. The external numbers are suffixed with (External).
Step 5	show voicemail non-subscriber restriction-table Example: se-10-0-0-0# show voicemail non-subscriber restriction-table	(Optional) Displays the restriction-table associated with the nonsubscriber voice mail feature.

Examples

```
se-10-0-0-0# show voicemail messages future

Message ID:      JMX0637L023-NM-FOC08221WRB-731357131983
Sender:          User1
Recipient(s):    UserA
Length(sec):     30
Delivery time:   Mon, 11 April 2006 08:0000-0800 (PST)
```

REVIEW DRAFT - CISCO CONFIDENTIAL

Message ID: JMX0637L023-NM-FOC08221WRB-731183375855
 Sender: User2
 Recipient(s): UserB, 95550041 (External)
 Length(sec): 20
 Delivery time: Wed, 13 April 2006 10:15:00-0800 (PST)

se-10-0-0-0# **show voicemail msg-notification restriction-table**

Restriction Table: msg-restriction
 Minimum digits allowed: 1
 Maximum digits allowed: 30
 Dial Strings:

Preference	Call Pattern	Allowed
1	19000...	yes
2	170000	yes
3	*	yes

Configuring Broadcast Messages

This chapter describes the procedures for configuring the networking capability on the local Cisco Unity Express voice-mail system and contains the following sections:

- [Overview of Broadcast Messages, page 26](#) (optional)
- [Configuring Broadcast Messages, page 27](#) (optional)
- [Enabling the MWI Lights for Broadcast Messages, page 28](#) (optional)
- [Displaying Broadcast Messages, page 29](#) (optional)
- [Deleting a Broadcast Message, page 30](#) (optional)
- [Changing Broadcast Message Start and End Times, page 30](#) (optional)
- [Disabling Broadcast Privileges for a Group, page 31](#) (optional)
- [Disabling MWI Lights for Broadcast Messages, page 31](#) (optional)
- [Configuring the Local-Broadcast Privilege, page 31](#) (optional)

Overview of Broadcast Messages

Cisco Unity Express permits sending broadcast messages to local and remote network locations. Cisco Unity Express permits subscribers with the broadcast privilege to send local and network broadcast messages. Subscribers obtain this privilege as members of a group that has the broadcast privilege.

Sending a broadcast message is available through the Cisco Unity Express telephone user interface (TUI).

The broadcast message sender has the option to readdress, rerecord, and review the message before sending it out. The sender also can set the start and end times for the message and the number of days the broadcast message plays before the system deletes it. The maximum life of a broadcast message is 365 days. The default message lifetime is 30 days.

The sender can include any or all of the remote locations configured on the local system. The remote addresses can be location numbers or location names. When using the location name, the number of matches may resolve into several locations. If the number of locations is less than or equal to 4, the system gives the sender the option to select the exact location. If the number of matches is greater than 4, the sender must enter more letters to narrow the search.

REVIEW DRAFT - CISCO CONFIDENTIAL

All subscribers at the remote location receive the broadcast message. The recipients hear the message immediately after logging in to their voice mailboxes. The recipients cannot interrupt the message with any DTMF key. Recipients can save or delete the broadcast message; they cannot reply or forward a broadcast message.

The system administrator at each location determines how or when the message waiting indicator (MWI) lights.

It is possible for the MWI lights to turn on for a broadcast message on some systems but not for others.

Configuring Broadcast Messages

Perform the following procedures to configure broadcast messages:

- [Configuring a Group with Broadcast Privileges, page 27.](#)
- [Configuring the Broadcast Message Length and Expiration Time, page 27](#)

Configuring a Group with Broadcast Privileges

Use the following EXEC mode command to configure a group with broadcast privileges:

```
group group-name privilege broadcast
```

where *group-name* is the set of subscribers who will have the capability of creating and sending broadcast messages.

The following example assigns the broadcast privilege to a group named managers:

```
se-10-0-0-0# group managers privilege broadcast
```

Configuring the Broadcast Message Length and Expiration Time

Use the following procedure to configure the local system for broadcast messages.

Required Data for This Procedure

The following information is required to configure the broadcast message length and expiry time:

- Broadcast message length, in seconds
- Broadcast message expiry time, in days

SUMMARY STEPS

1. **config t**
2. **voicemail broadcast recording time *broadcast-length***
3. **voicemail default broadcast expiration time *broadcast-days***
4. **exit**

REVIEW DRAFT - CISCO CONFIDENTIAL**DETAILED STEPS**

	Command or Action	Purpose
Step 1	config t Example: se-10-0-0-0# config t se-10-0-0-0(config)#	Enters configuration mode.
Step 2	voicemail broadcast recording time <i>broadcast-length</i> Example: se-10-0-0-0(config)# voicemail broadcast recording time 120	Specifies the maximum length of broadcast messages, in seconds. Valid values are 10 to 3600.
Step 3	voicemail default broadcast expiration time <i>broadcast-days</i> Example: se-10-0-0-0(config)# voicemail default broadcast expiration time 90	Specifies the number of days to store broadcast messages. The maximum value is 365 days.
Step 4	exit Example: se-10-0-0-0(config)# exit se-10-0-0-0#	Exits configuration mode.

Examples

The following example sets the broadcast message length to 20 seconds and the expiration time to 2 days.

```
se-10-0-0-0# config t
se-10-0-0-0(config)# voicemail broadcast recording time 20
se-10-0-0-0(config)# voicemail default broadcast expiration time 2
se-10-0-0-0(config)# exit
```

Enabling the MWI Lights for Broadcast Messages

Use the following Cisco Unity Express configuration mode command to enable the MWI lights when a voice mailbox receives a broadcast message.

voicemail broadcast mwi

The following example illustrates enabling the MWI lights for broadcast messages:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# voicemail broadcast mwi
se-10-0-0-0(config)# end
```

REVIEW DRAFT - CISCO CONFIDENTIAL

Displaying Broadcast Messages

Multiple commands are available to display information about broadcast messages.

Displaying Current Broadcast Messages

Use the following EXEC mode command to display broadcast messages:

show voicemail broadcast messages

The output for this command may appear similar to the following:

```
se-10-0-0-0# show voicemail broadcast messages

Message ID:      JMX0824L4R4-NM-FOC08221WSQ-1103139552166-NBCM
Sender:          1005@nyc.mycompany.com
Length(secs):    10
Start time:      21:12:54 Nov 23 2005 PST
End time:        11:48:06 Dec 4 2005 PST

Message ID:      JMX0824L4R4-NM-FOC08221WSQ-1103084723247-NBCM
Sender:          /sw/local/users/user45
Length(secs):    30
Start time:      08:41:09 Dec 7 2005 PST
End time:        09:00:00 Jan 3 2006 PST
```

If a subscriber at a remote network location sends the broadcast message, the e-mail domain of the remote sender appears in the Sender field. If a local subscriber sends the message, the pathname to the sender appears in the field.

If no broadcast messages are active, the output may appear similar to this:

```
se-10-0-0-0# show voicemail broadcast messages
No Broadcast Messages
```

Displaying Broadcast Messages Received Per Mailbox

The following command is modified to display broadcast message information:

show voicemail mailboxes

The column BCST displays the number of broadcast messages received by the mailboxes. The output for this command may appear similar to the following:

```
se-10-0-0-0# show voicemail mailboxes

OWNER      MSGS  NEW  SAVE  DEL  BCST  MSGTIME  MBXSIZE  USED
user1      16   16   0     0    4    3000     3000    100%
user2      16   16   0     0    4    3000     3000    100%
user3      16   16   0     0    4    3000     3000    100%
user4      16   16   0     0    4    3000     3000    100%
```

Displaying Broadcast Messages Received by the Voice-Mail System

The following command is modified to display broadcast message information:

show voicemail usage

REVIEW DRAFT - CISCO CONFIDENTIAL

The row **broadcast message count** displays the number of broadcast messages received by the voice mail system. The output for this command may appear similar to the following:

```
se-10-0-0-0# show voicemail usage

personal mailboxes:          120
general delivery mailboxes:  0
orphaned mailboxes          0
capacity of voicemail (minutes): 6000
allocated capacity (minutes): 6000.0
total message time used (seconds): 7543
total message count:         7001
average message length (seconds): 1.0774175117840308
broadcast message count:     4
future message count:        0
networking message count:    0
greeting time used (seconds): 3
greeting count:              1
average greeting length (seconds): 3.0
total time used (seconds):    7546
total time used (minutes):    125.76667022705078
percentage time used (%):     2
messages left since boot:     0
messages played since boot:   0
messages deleted since boot:  0
```

Deleting a Broadcast Message

Use the following EXEC mode command to delete a broadcast message:

voicemail broadcast message *message-id* delete

where *message-id* is the coded identifier for the message. Use the **show voicemail broadcast messages** command to obtain the message ID.

The following example deletes a broadcast message:

```
se-10-0-0-0# voicemail broadcast message JMX0824L4R4-NM-FOC08221WSQ-1103139552166-NBCM
delete
```

Changing Broadcast Message Start and End Times

Use the following EXEC mode commands to change the start and end times of a broadcast message:

voicemail broadcast message *message-id* starttime *time date*

voicemail broadcast message *message-id* endtime *time date*

where *message-id* is the coded identifier for the message, *time* is the time in the 24-hour clock format, and *date* has the format YYYY-MM-DD. Use the **show voicemail broadcast messages** command to obtain the message ID.

The following examples change the start and end times for a broadcast message:

```
se-10-0-0-0# voicemail broadcast message JMX0824L4R4-NM-FOC08221WSQ-1103139552166-NBCM
starttime 10:00 2004-09-15
se-10-0-0-0# voicemail broadcast message JMX0824L4R4-NM-FOC08221WSQ-1103139552166-NBCM
endtime 15:30 2004-09-16
```

REVIEW DRAFT - CISCO CONFIDENTIAL

Disabling Broadcast Privileges for a Group

Use the following EXEC mode command to remove the broadcast privileges from a group:

```
no group groupname privilege broadcast
```

where *groupname* is the group to have the broadcast privileges removed.

The following example disables the broadcast privilege for the group named managers:

```
se-10-0-0-0# no group managers privilege broadcast
```

Disabling MWI Lights for Broadcast Messages

Use the following Cisco Unity Express configuration mode command to disable the MWI lights for broadcast messages.

```
no voicemail broadcast mwi
```

The following example illustrates how to disable the MWI lights for broadcast messages:

```
se-10-0-0-0# config t  
se-10-0-0-0(config)# no voicemail broadcast mwi  
se-10-0-0-0(config)# end
```

Configuring the Local-Broadcast Privilege

Cisco Unity Express provides a local-broadcast privilege that permits subscribers to send broadcast messages only to other subscribers on the local system. The local-broadcast privilege is a subset of the broadcast privilege, which permits subscribers to send broadcast messages to all configured subscribers and locations on the network.

Cisco Unity Express does not create a default group for local-broadcast subscribers. The administrator must create a group of subscribers and assign the local-broadcast privilege to it.

To configure this option from the GUI, use the **Configure > Groups** option and select a group.

Prerequisites

Name of the group that will be assigned to the local-broadcast privilege. Verify that the group exists before assigning the privilege.

SUMMARY STEPS

1. **config t**
2. **groupname *groupname* privilege local-broadcast**
3. **end**
4. (Optional) **show groups privileges**

REVIEW DRAFT - CISCO CONFIDENTIAL**DETAILED STEPS**

	Command or Action	Purpose
Step 1	config t Example: se-10-0-0-0# config t	Enters configuration mode.
Step 2	groupname groupname privilege local-broadcast Example: se-10-0-0-0(config)# groupname engineers privilege local-broadcast	Assigns the local-broadcast privilege to the group <i>groupname</i> .
Step 3	end Example: se-10-0-0-0(config)# end	Exits configuration mode.
Step 4	show groups privileges Example: se-10-0-0-0# show groups privileges	(Optional) Displays the privileges assigned to configured groups.

Example

The following example displays the privileges for multiple groups.

```
se-10-0-0-0# show groups privileges
```

```

GROUPID                                PRIVILEGES
Administrators                          superuser ManagePrompts ManagePublicList
Administrators                          ViewPrivateList
Broadcasters                           broadcast
managers                               broadcast ViewPrivateList
engineers                              local-broadcast

```

Configuring Restriction Tables

This section discusses the following topics:

- [Overview, page 32](#)
- [Toll Fraud Prevention, page 34](#)
- [Configuring Restriction Tables, page 36](#)

Overview

The following features use restriction tables to enable you to restrict access to the feature's functionality:

- Fax

REVIEW DRAFT - CISCO CONFIDENTIAL

- Live reply
- Message notification
- Nonsubscriber message delivery
- Caller call flow customization (see [“Configuring Call Flow Customization”](#) section on page 18.)

For each of these features, the restriction table controls the phone numbers that subscribers can use to access the feature. These restrictions are available only for phone devices and numeric pagers.

The system provides a predefined table that can be modified by the administrator. The table applies to all subscribers and groups on the system. A typical use of this table is to prevent the use of long-distance or international numbers for the feature.

The system checks the restriction table when the subscriber is assigning phone numbers to phone devices (such as a cell phone, home phone, or work phone), to a numeric pager, and before making an outcall. If a phone number is listed in the table as restricted, the system sends a message to the subscriber.

If a subscriber has a number configured for a device and the administrator later restricts that number system-wide, notification calls will not be made to that number. The administrator must remove the number for the individual subscriber.

Cisco Unity Express provides a default restriction table that defines two requirements:

- Minimum and maximum number of digits, including access codes, allowed in a phone number. The minimum is 1 digit and the maximum is 30 digits. The default is 1 digit.
- A maximum of 10 dial strings that represent the restricted numbers. Each string consists of a call pattern and a setting that specifies if a phone number matching the pattern is restricted or not.

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.

Valid setting values are allowed or disallowed.

When a subscriber tries to set up or change a phone number assigned to a device, the system verifies that the number has the allowed number of digits. If it does not, the subscriber receives a system message.

If the number of digits is acceptable, the system checks the number against the dial patterns in the restriction table, starting with the first pattern (preference 1). If the number does not match the first pattern, the system checks the next pattern in the table (preference 2), and so forth until a match is found. The system either permits or restricts the call as specified in the dial string.

The default restriction table permits all phone numbers to be used, as shown in [Table 19-5](#).

Table 19-5 Default Restriction Table

Preference	Call Pattern	Allowed
1	*	Yes

You can change only the preference and permission of this pattern.

The restriction table can contain identical dial strings, which have the same call pattern and permission setting. This includes the default pattern. You can delete any of these dial strings if the table contains *at least one* default pattern.

[Table 19-6](#) illustrates a restriction table with international numbers and restricted numbers.

REVIEW DRAFT - CISCO CONFIDENTIAL**Table 19-6 Restriction Table with International Numbers**

Preference	Call Pattern	Allowed
1	9011*	No
2	91.....	No
3	*	Yes

Table 19-7 illustrates a restriction table that permits one number in an area code but restricts all other numbers in that area code.

Table 19-7 Restriction Table with Restricted Area Code

Preference	Call Pattern	Allowed
1	9011*	No
2	912225550150	Yes
3	91222.....	No
4	*	Yes

Following are the parameters that you can configure for restriction tables:

- **min-digits** — Minimum number of digits for a specified restriction table. Valid values for the minimum number of digits are 1 to 30. The default is 1.
- **max-digits** — Maximum number of digits for a specified restriction table. Valid values for the maximum number of digits are 1 to 30. The default is 1.
- **preference** — Order of this string in the restriction table. The system searches the strings in order of preference, starting with 1. Valid values are 1 to 10.
- **pattern** — Call pattern to be matched. Valid characters are digits 0 to 9, asterisk (*), or dot (.). The table accepts duplicate call patterns.
- **allowed** — Permits phone numbers with this pattern to be assigned to message notification devices.
- **disallowed** — Prevents phone numbers with this pattern from being assigned to message notification devices.
- **insert** — Inserts the dial string in the proper place in the table.

Toll Fraud Prevention

When a Cisco router platform is installed with a voice-capable Cisco IOS software image, appropriate features must be enabled on the platform to prevent potential toll fraud exploitation by unauthorized users. Deploy these features on all Cisco router Unified Communications applications that process voice calls, such as Cisco Unified Communications Manager Express (CME), Cisco Survivable Remote Site Telephony (SRST), Cisco Unified Border Element (UBE), Cisco IOS-based router and standalone analog and digital PBX and public-switched telephone network (PSTN) gateways, and Cisco contact-center VoiceXML gateways. These features include, but are not limited to, the following:

REVIEW DRAFT - CISCO CONFIDENTIAL

- Disable secondary dial tone on voice ports—By default, secondary dial tone is presented on voice ports on Cisco router gateways. Use private line automatic ringdown (PLAR) for foreign exchange office (FXO) ports and direct-inward-dial (DID) for T1/E1 ports to prevent secondary dial tone from being presented to inbound callers.
- Cisco router access control lists (ACLs)—Define ACLs to allow only explicitly valid sources of calls to the router or gateway, and therefore to prevent unauthorized Session Initiation Protocol (SIP) or H.323 calls from unknown parties to be processed and connected by the router or gateway.
- Close unused SIP and H.323 ports—If either the SIP or H.323 protocol is not used in your deployment, close the associated protocol ports. If a Cisco voice gateway has dial peers configured to route calls outbound to the PSTN using either time division multiplex (TDM) trunks or IP, close the unused H.323 or SIP ports so that calls from unauthorized endpoints cannot connect calls. If the protocols are used and the ports must remain open, use ACLs to limit access to legitimate sources.
- Change SIP port 5060—If SIP is actively used, consider changing the port to something other than well-known port 5060.
- SIP registration—If SIP registration is available on SIP trunks, turn on this feature because it provides an extra level of authentication and validation that only legitimate sources can connect calls. If it is not available, ensure that the appropriate ACLs are in place.
- SIP Digest Authentication—If the SIP Digest Authentication feature is available for either registrations or invites, turn this feature on because it provides an extra level of authentication and validation that only legitimate sources can connect calls.
- Explicit incoming and outgoing dial peers—Use explicit dial peers to control the types and parameters of calls allowed by the router, especially in IP-to-IP connections used on Cisco Unified CME, Cisco Unified SRST, and Cisco UBE. Incoming dial peers offer additional control on the sources of calls, and outgoing dial peers on the destinations. Incoming dial peers are always used for calls. If a dial peer is not explicitly defined, the implicit dial peer 0 is used to allow all calls.
- Explicit destination patterns—Use dial peers with more granularity than .T for destination patterns to block disallowed off-net call destinations. Use class of restriction (COR) on dial peers with specific destination patterns to allow even more granular control of calls to different destinations on the PSTN.
- Translation rules—Use translation rules to manipulate dialed digits before calls connect to the PSTN to provide better control over who may dial PSTN destinations. Legitimate users dial an access code and an augmented number for PSTN for certain PSTN (for example, international) locations.
- Tcl and VoiceXML scripts—Attach a Tcl/VoiceXML script to dial peers to do database lookups or additional off-router authorization checks to allow or deny call flows based on origination or destination numbers. Tcl/VoiceXML scripts can also be used to add a prefix to inbound DID calls. If the prefix plus DID matches internal extensions, then the call is completed. Otherwise, a prompt can be played to the caller that an invalid number has been dialed.
- Host name validation—Use the “permit hostname” feature to validate initial SIP Invites that contain a fully qualified domain name (FQDN) host name in the Request Uniform Resource Identifier (Request URI) against a configured list of legitimate source hostnames.
- Dynamic Domain Name Service (DNS)—If you are using DNS as the “session target” on dial peers, the actual IP address destination of call connections can vary from one call to the next. Use voice source groups and ACLs to restrict the valid address ranges expected in DNS responses (which are used subsequently for call setup destinations).

For more configuration guidance, see the “[Cisco IOS Unified Communications Toll Fraud Prevention](#)” paper.

REVIEW DRAFT - CISCO CONFIDENTIAL

Configuring Restriction Tables

The following sections describe how to configure restriction tables:

- “Creating a Restriction Table” section on page 36 (optional)
- “Deleting a Restriction Table” section on page 37 (optional)
- “Configuring a Restriction Table” section on page 38 (optional)

Creating a Restriction Table

Prerequisites

Cisco Unity Express 3.0 or a later version

Required Data for This Procedure

None.

SUMMARY STEPS

1. **config t**
2. **restriction *table-name***
3. **end**
4. (Optional) **show restriction table [*table-name* | all]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t Example: se-10-0-0-0# config t	Enters configuration mode.
Step 2	restriction <i>table-name</i> create Example: se-10-0-0-0(config)# restriction live-reply create	Creates a restriction table.
Step 3	end Example: se-10-0-0-0(config)# end	Exits to privileged EXEC mode.
Step 4	show restriction table [<i>table-name</i> all] Example: se-10-0-0-0# show restriction table live-reply	(Optional) Displays the specified restriction tables.

REVIEW DRAFT - CISCO CONFIDENTIAL**Examples**

The following is sample output for the **show restriction-table** *table-name* command:

```
se-10-0-0-0# show restriction-table fax-restriction
```

```
Restriction Table:      fax-restriction
Minimum digits allowed: 1
Maximum digits allowed: 30
Dial Strings:
Preference   Call Pattern   Allowed
1            19000...       yes
2            170000         yes
3            *              yes
```

Deleting a Restriction Table**Prerequisites**

None.

Required Data for This Procedure

None.

SUMMARY STEPS

1. **config t**
2. **restriction** *table-name* **delete**
3. **end**
4. (Optional) **show restriction table** [*table-name* | **all**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t Example: se-10-0-0-0# config t	Enters configuration mode.
Step 2	restriction <i>table-name</i> delete Example: se-10-0-0-0(config)# restriction live-reply delete	Deletes a restriction table.

REVIEW DRAFT - CISCO CONFIDENTIAL

	Command or Action	Purpose
Step 3	end Example: se-10-0-0-0(config)# end	Exits to privileged EXEC mode.
Step 4	show restriction table [<i>table-name</i> all] Example: se-10-0-0-0# show restriction table live-reply	(Optional) Displays the specified restriction tables.

Examples

To see sample output for the **show restriction-table** *table-name* command, see the [“Examples” section on page 37](#).

Configuring a Restriction Table

To configure a restriction table, you can set any of the following parameters or you can accept the default values:

- Minimum digits
- Maximum digits
- Dial-string preference

Prerequisites

To use restriction tables with the following features, you must have Cisco Unity Express 3.0 or a later version:

- Fax
- Live reply
- Message notification
- Nonsubscriber message delivery.

Required Data for This Procedure

None.

SUMMARY STEPS

1. **config t**
2. **restriction** *table-name* **dial-string preference** *number pattern pattern-string* {**allowed**|**disallowed**} [**insert**]
3. **restriction** *table-name* **min-digits** *num-of-digits*
4. **restriction** *table-name* **max-digits** *num-of-digits*
5. **end**
6. (Optional) **show restriction table** [*table-name* | **all**]

REVIEW DRAFT - CISCO CONFIDENTIAL**DETAILED STEPS**

	Command or Action	Purpose
Step 1	config t Example: se-10-0-0-0# config t	Enters configuration mode.
Step 2	restriction table-name dial-string preference preference-number pattern pattern-string {allowed disallowed} [insert] Example: se-10-0-0-0(config)# restriction msg-notification dial-string preference 2 pattern 91222* disallowed se-10-0-0-0(config)# restriction msg-notification dial-string preference 2 pattern 91800* allowed insert	<p>(Optional) Specifies the dial string that the system uses to verify a phone number assigned to a phone device or numeric pager. Use this command to add a new dial string to the restriction table or to modify an existing dial string.</p> <ul style="list-style-type: none"> • <i>preference-number</i>—Order of this string in the restriction table. The system searches the strings in order of preference, starting with 1. Valid values are 1 to 10. The default pattern * has preference 1 by default. The administrator can modify this setting. • <i>pattern-string</i>—Call pattern to be matched. Valid characters are digits 0 to 9, asterisk (*), or dot (.). The table accepts duplicate call patterns. The default pattern * cannot be deleted or modified. • allowed—Permits phone numbers with this pattern to be assigned to message notification devices. The default pattern * is allowed by default. The administrator can modify this setting. • disallowed—Prevents phone numbers with this pattern from being assigned to message notification devices. • insert—(Optional) Inserts the dial string in the proper place in the table. The system increases the preference number of existing strings appropriately. The system displays a system message if the preference number is less than 1 or greater than 10. If insert is not used, the system replaces any existing dial string with the given preference with this new dial string. The system displays a system message if no existing dial string has the given preference.

REVIEW DRAFT - CISCO CONFIDENTIAL

	Command or Action	Purpose
Step 3	restriction msg-notification min-digits <i>minimum-digits</i> Example: se-10-0-0-0(config)# restriction msg-notification min-digits 5	(Optional) Specifies the minimum number of digits for a notification phone number. Valid values are 1 to 30. The default is 1. This value applies only to phone devices and numeric pagers.
Step 4	restriction msg-notification max-digits <i>maximum-digits</i> Example: se-10-0-0-0(config)# restriction msg-notification max-digits 12	(Optional) Specifies the maximum number of digits for a restricted number. Valid values are 1 to 30. The default is 1. A system message appears if max-digits is a smaller value than min-digits . This value applies only to phone devices and numeric pagers.
Step 5	end Example: se-10-0-0-0(config)# end	Exits to privileged EXEC mode.
Step 6	show restriction table [<i>table-name</i>] all Example: se-10-0-0-0# show restriction table live-reply	(Optional) Displays the specified restriction tables.

Examples

To see sample output for the **show restriction-table** *table-name* command, see the [“Examples” section on page 37](#).