



# CHAPTER 13

## Cisco Unified Mobility

---

Cisco Unified Mobility gives users the ability to redirect incoming IP calls from the Cisco Unified Communications Manager to up to four different designated client devices such as mobile phones or Cisco Unified IP Phones.

For example, Cisco Unified Mobility associates a user mobile phone number with the user business IP phone number. Cisco Unified Mobility then directs incoming calls to ring on a user mobile phone as well as the business phone, thus providing a single number for callers to reach the user. Calls that go unanswered on all the designated devices are redirected to the user Cisco Unity messaging system.

Administrators can configure Cisco Unified Mobility, formerly known as Cisco Unified MobilityManager, by using the Cisco Unified Communications Manager Administration windows to configure the setup for end users. End users can use Cisco Unified CM User Options windows to configure their own personal settings.

Cisco Unified Mobility comprises a number of features that this chapter discusses. The chapter provides an overview of the configuration procedures that administrators follow.

Refer to the user guide for a particular Cisco Unified IP Phone phone model for procedures that end users follow to configure the Cisco Unified Mobility settings for their phones by using the Cisco Unified CM User Options windows.

This chapter includes information on the following topics:

- [Introducing Cisco Unified Mobility, page 13-2](#)
- [Definitions, page 13-2](#)
- [List of Cisco Unified Mobility Features, page 13-3](#)
- [Other Benefits of Cisco Unified Mobility Features, page 13-4](#)
- [Mobile Connect, page 13-5](#)
- [Mobile Voice Access, page 13-5](#)
- [Cisco Unified Mobile Communicator, page 13-6](#)
- [Dial-via-Office Reverse Callback, page 13-9](#)
- [Time-of-Day Access, page 13-10](#)
- [Directed Call Park via DTMF, page 13-13](#)
- [SIP URI Dialing, page 13-14](#)
- [Use Case Scenarios for Cisco Unified Mobility Features, page 13-15](#)
- [Interactions and Restrictions, page 13-18](#)
- [System Requirements, page 13-22](#)

- [Migrating from Cisco Unified MobilityManager, page 13-22](#)
- [Configuring Cisco Unified Mobility, page 13-22](#)
- [Cisco Unified Mobility Configuration Checklist, page 13-23](#)
- [Access List Configuration, page 13-24](#)
- [Remote Destination Profile Configuration, page 13-29](#)
- [Remote Destination Configuration, page 13-35](#)
- [Mobile Voice Access Media Resource Configuration, page 13-40](#)
- [H.323 Gateway Configuration for Mobile Voice Access, page 13-42](#)
- [Mobility Setting Configuration, page 13-48](#)
- [Mobility Softkey Configuration, page 13-48](#)
- [Related Topics, page 13-49](#)

## Introducing Cisco Unified Mobility

Administrators configure the basic setup of Cisco Unified Mobility for end users by using the Cisco Unified Communications Manager Administration windows.

This section discusses the following topics:

- [Definitions, page 13-2](#)
- [List of Cisco Unified Mobility Features, page 13-3](#)
- [Other Benefits of Cisco Unified Mobility Features, page 13-4](#)

### Additional Information

See the “[Related Topics](#)” section on [page 13-49](#).

## Definitions

[Table 13-1](#) provides definitions of terms that are related to Cisco Unified Mobility.

**Table 13-1**      **Definitions**

Term	Definition
Access List	List that determines the phone numbers that the system can pass or block from being passed to remote destinations.
Mobile Connect	Feature that allows users to answer incoming calls on the desktop phone or at a remote destination and to pick up in-progress calls on the desktop phone or at a remote destination without losing the connection.
Mobile Voice Access	Integrated voice response (IVR) system that is used to initiate Mobile Connect calls and to activate or deactivate Mobile Connect capabilities.

**Table 13-1** Definitions (continued)

Term	Definition
Remote Destination	Phones that are available for Mobile Connect responses and pickup, plus locations that are used to reach Mobile Voice Access. Remote destinations may include any of the following devices: <ul style="list-style-type: none"> <li>• Single-mode mobile (cellular) phones</li> <li>• Smart phones</li> <li>• Dual-mode phones</li> <li>• Enterprise IP phones that are not in the same cluster as the desktop phone</li> <li>• Home phone numbers in the PSTN.</li> </ul>
Remote Destination Profile	Set of parameters that apply to all remote destinations for the user.
Time-of-Day Access	Feature that associates ring schedules to access lists and determines whether a call will be extended to a remote destination during the time of day when such a call is received.

**Additional Information**

See the [“Related Topics”](#) section on page 13-49.

## List of Cisco Unified Mobility Features

This section provides a list of Cisco Unified Mobility features that administrators configure by using Cisco Unified Communications Manager Administration.

The following features, which were originally part of Cisco Unified MobilityManager, now reside in Cisco Unified Communications Manager:

- **Mobile Connect**—This feature enables users to manage business calls by using a single phone number to pick up in-progress calls on the desktop phone and the mobile phone. Refer to the [“Mobile Connect”](#) section on page 13-5 for a detailed discussion.
- **Desktop Call Pickup**—Users can switch between desktop phone and mobile phone during an active call without losing the connection. Based on the needs of the moment, they can take advantage of the reliability of the wired office phone or the mobility of the mobile phone.
- **Mobile Voice Access**—This feature extends Mobile Connect capabilities by providing an integrated voice response (IVR) system to initiate Mobile Connect calls and activate or deactivate Mobile Connect capabilities. Refer to the [“Mobile Voice Access”](#) section on page 13-5 for a detailed discussion.
- **Access List**—Users can restrict the set of callers that cause a designated remote destination to ring on an incoming call (allowed access list) or for which the remote destinations do *not* ring on an incoming call (blocked access list). Each remote destination presents a mobile or other phone that can be configured to accept transfers from the desktop phone for the user.

Cisco Unified Communications Manager in Release 6.0 added support for the following Cisco Unified Mobility features:

- **Midcall Enterprise Feature Support Using DTMF**—You can configure DTMF feature codes as service parameters: Hold (default equals \*81), exclusive hold (default equals \*82), resume (default equals \*83), transfer (default equal \*84), and conference (default equals \*85).
- **Two-stage Dialing**—Be aware that enterprise features are available with two-stage dialing for smartphones. Two-stage dialing allows smartphones to make outgoing calls through Cisco Unified Communications Manager if the smartphone is in business mode. The smartphone dials the Enterprise Feature Access number for Cisco Unified Communications Manager and then dials the destination number.
- **Dual-mode Phone Support**—Cisco Unified Mobility supports dual-mode phones.
- **Manual Handoff of Calls on a Dual-mode Phone**—Dual-mode devices offer an option to manually hand off calls from the PSTN to WLAN and vice versa.

Cisco Unified Communications Manager in Release 7.0 added support for the following Cisco Unified Mobility features:

- **Cisco Unified Mobile Communicator**—Cisco Unified Mobile Communicator (CUMC) specifies a phone device that uses Mobile Smart Client device protocol. You configure the Cisco Unified Mobile Communicator in the Phone Configuration window in Cisco Unified Communications Manager Administration. Refer to the [“Cisco Unified Mobile Communicator” section on page 13-6](#) for a detailed discussion.
- **Dial-via-Office Reverse Callback**—The Dial-via-Office Reverse Callback feature resembles the Mobile Voice Access feature, except that Cisco Unified Communications Manager makes both calls. From the CUMC client, using the data channel, the phone initiates the Reverse Callback feature. Cisco Unified Communications Manager then calls the remote destination first. When the remote destination answers, Cisco Unified Communications Manager calls the destination number. Refer to the [“Dial-via-Office Reverse Callback” section on page 13-9](#) for a detailed discussion.
- **Time-of-Day Access**—When the Mobile Connect feature is enabled, calls get extended to remote destinations if the associated DN is called based on time-of-day-access-based configuration. Refer to [“Time-of-Day Access” section on page 13-10](#) for a detailed discussion.
- **Directed Call Park via DTMF**—This feature allows a mobile phone user to park a call by transferring the parkee party to a park code, so the call can be retrieved later. The feature combines the standard Cisco Unified Communications Manager Directed Call Park feature with the DTMF feature. Refer to [“Directed Call Park via DTMF” section on page 13-13](#) for a detailed discussion.
- **SIP URI Dialing**—This feature supports SIP URI as an additional type of Remote Destination for Cisco Unified Mobility. Refer to [“SIP URI Dialing” section on page 13-14](#) for a detailed discussion.

#### Additional Information

See the [“Related Topics” section on page 13-49](#).

## Other Benefits of Cisco Unified Mobility Features

Cisco Unified Mobility allows flexible management of enterprise and mobile phone communications and provides these additional features and benefits:

- **Simultaneous desktop ringing**—Incoming calls ring simultaneously on the IP phone extension and the designated mobile handset. When the user answers one line, the unanswered line automatically stops ringing. Users can choose the preferred device each time that a call comes in.

- **Single enterprise voice mailbox**—The enterprise voice mailbox can serve as single, consolidated voice mailbox for all business, including calls to the desktop or configured remote devices. Incoming callers have a predictable means of contacting employees, and users can check multiple voice-messaging systems in less time.
- **System remote access**—A mobile phone for the user can initiate calls as if it were a local IP PBX extension. User-initiated calls can take advantage of local voice gateways and WAN trunking, and the enterprise can track employee call initiation.
- **Caller ID**—The system preserves and displays Caller ID on all calls. Users can take advantage of Mobile Connect with no loss of expected IP phone features.
- **Remote on/off control**—Users can turn their Mobile Connect features on or off from the mobile phone by using Mobile Voice Access or from the Cisco Unified CM User Options windows.
- **Call tracing**—The system logs detailed Mobile Connect calls and provides information to help the enterprise optimize trunk usage and debug connection problems.
- **Security and privacy for Mobile Connect calls**—During an active Mobile Connect call, the associated desktop IP phone remains secured. The system eliminates access to the call from the desktop as soon as the mobile connection becomes active, which precludes the possibility of an unauthorized person listening in on the call that is bridged to the mobile phone.
- **Smart phone support**—Users can use the enterprise hold, resume, transfer, and conference softkeys on the smartphone in an active call. Users can also enable or disable Mobile Connect from a smartphone.

**Additional Information**

See the [“Related Topics” section on page 13-49](#).

## Mobile Connect

Mobile Connect allows users to answer incoming calls on the desktop phone or mobile phone, to pick up in-progress calls on the desktop phone or mobile phone without losing the connection, and to originate enterprise calls from the mobile phone.

**Note**

You can use existing mobile phones, including Code Division Multiple Access (CDMA) and Global System for Mobile Communications (GSM) phones for Mobile Connect and Mobile Voice Access. In some cases, however, you may need to modify timer settings in Cisco Unified Communications Manager to ensure compatibility. See the [“Configuring Remote Destinations” section on page 13-36](#).

Refer to the [“Use Case Scenarios for Mobile Connect” section on page 13-15](#) for the use case scenarios that Cisco Unified Communications Manager supports with this feature.

**Additional Information**

See the [“Related Topics” section on page 13-49](#).

## Mobile Voice Access

Mobile Voice Access extends Mobile Connect capabilities by allowing users to originate a call from a remote destination such as a mobile phone as if dialing from the desktop phone. A remote destination represents a phone that is designated as available for Mobile Connect responses and pickup. The user

dials Mobile Voice Access from the remote destination. The system prompts the user for the PIN that is assigned to the user in Cisco Unified Communications Manager. After being authenticated, the user can make a call by using the same Mobile Connect features that would be available if the user originated the call from the enterprise desktop phone.

When Mobile Voice Access is called, the system prompts the user for the originating phone number in addition to the PIN if any of the following statements is true:

- The number from which the user is calling does not represent one of the remote destinations for the user.
- The user or the carrier for the user blocks the number (shown as “Unknown Number”).
- The number does not get accurately matched in the Cisco Unified Communications Manager database; for example, if the number is 510-666-9999, but it is listed as 666-9999 in the database, or the number is 408-999-6666, but it is entered as 1-408-999-6666 in the database.
- Mobile Voice Access is configured in hairpin mode.

If the user incorrectly enters any requested information (such as mobile phone number or PIN) three times in a row, the Mobile Voice Access call disconnects, and the system locks out the user for a period of time.

**Note**

Mobile Voice Access uses the first locale that displays in the Selected Locales pane in the Mobile Voice Access window in Cisco Unified Communications Manager Administration (**Media Resources > Mobile Voice Access**) when the IVR is used. For example, if English United States displays first in the Selected Locales pane, the Cisco Unified Mobility user receives English when the IVR is used during a call.

Refer to the [“Use Case Scenarios for Mobile Voice Access”](#) section on page 13-16 for the use case scenarios that Cisco Unified Communications Manager supports with this feature.

**Additional Information**

See the [“Related Topics”](#) section on page 13-49.

## Cisco Unified Mobile Communicator

The Cisco Unified Mobile Communicator (CUMC) specifies a device type that you can configure in Cisco Unified Communications Manager Administration in the Phone Configuration window. The Cisco Unified Mobile Communicator operates with the Mobile Smart Client device protocol and uses three Device License Units (DLUs), or one DLU, if adjunct.

See the following topics for configuration details:

- [Cisco Unified Mobile Communicator Configuration, page 13-7](#)
- [Cisco Unified Mobile Communicator Configuration Details, page 13-8](#)

**Additional Information**

See the [“Related Topics”](#) section on page 13-49.

## Cisco Unified Mobile Communicator Configuration

Table 13-2 summarizes the procedures for configuring the Cisco Unified Mobile Communicator for Cisco Unified Mobility. For detailed instructions, see the information that the table references.

**Table 13-2** Cisco Unified Mobile Communicator Configuration Checklist

Configuration Steps	Related Procedures and Topics
<p><b>Step 1</b> In Cisco Unified Communications Manager Administration, configure a Cisco Unified Mobile Communicator (CUMC) device.</p> <p>Use the <b>Device &gt; Phone</b> menu option.</p> <p><b>Note</b> Make sure that you check the Enable Mobility check box in the End User Configuration window.</p> <p><b>Note</b> Checking the Enable Mobility check box triggers licensing to consume device license units (DLUs) for Mobile Connect.</p>	<p><a href="#">Cisco Unified IP Phone Configuration</a>, <i>Cisco Unified Communications Manager Administration Guide</i></p> <p><a href="#">Cisco Unified Mobile Communicator Configuration Details</a>, page 13-8</p>
<p><b>Step 2</b> In Cisco Unified Communications Manager Administration, configure a security profile for a Cisco Unified Mobility Advantage (CUMA) server.</p> <p>Use the <b>System &gt; Security Profile &gt; CUMA Server Security Profile</b> menu option.</p>	<p>Refer to the <i>Cisco Unified Communications Manager Security Guide</i> for details.</p>
<p><b>Step 3</b> In Cisco Unified Communications Manager Administration, configure an application server for a CUMA server.</p> <p>Use the <b>System &gt; Application Server</b> menu option. In the Application Server Type drop-down list box, choose the CUMA Provisioning Server type.</p>	<p><a href="#">Application Server Configuration</a>, <i>Cisco Unified Communications Manager Administration Guide</i></p> <p><a href="#">Cisco Unified Mobile Communicator Configuration Details</a>, page 13-8</p>
<p><b>Step 4</b> In Cisco Unified Communications Manager Administration, configure the enterprise feature access directory number (DN).</p> <p>Use the <b>Call Routing &gt; Directory Number</b> menu option.</p> <p><b>Note</b> You must perform this configuration step for the Dial-via-Office features to work.</p>	<p><a href="#">Directory Number Configuration</a>, <i>Cisco Unified Communications Manager Administration Guide</i></p>

Table 13-2 Cisco Unified Mobile Communicator Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
<b>Step 5</b>	Allow the CUMA client to register with Cisco Unified Communications Manager.	Refer to the <i>Cisco Unified Communications Manager Security Guide</i> for details.
<b>Step 6</b>	<p>In the Cisco Unified CM User Options windows, configure end-user settings for the Cisco Unified Mobile Communicator, such as the following settings:</p> <ul style="list-style-type: none"> <li>• Device—End user specifies his own Cisco Unified Mobile Communicator.</li> <li>• Remote Destinations—End user chooses his own Cisco Unified Mobile Communicator as the remote destination profile.</li> </ul>	Refer to the User Guide for a particular Cisco Unified IP Phone model.

**Additional Information**

See the “[Related Topics](#)” section on page 13-49.

**Cisco Unified Mobile Communicator Configuration Details**

When you configure a Cisco Unified Mobile Communicator (CUMC), keep in mind the following configuration requirements as you configure the fields in the Phone Configuration window:

- When configuring a new Cisco Unified Mobile Communicator, select the phone type Cisco Unified Mobile Communicator in the Select Phone Type drop-down list box.
- Device Name—Ensure this name is unique. You need no MAC address.
- Mobility User ID—You must configure this field.
- Mobility Identity—This field must specify the CUMC-enabled smartphone mobile number as the destination number.
- Reroute CSS, CSS—Ensure these fields are configured for basic calls to work.
- DND Option—The Cisco Unified Mobile Communicator only supports the Call Reject DND option.

Ensure that a directory number is assigned to the Cisco Unified Mobile Communicator.

Keep in mind these other configuration requirements that apply to the Cisco Unified Mobile Communicator:

- Due to the lack of an integrated End User Configuration window for Cisco Unified Communications Manager and the Cisco Unified Mobility Advantage server, the CUMC client user must configure identical remote destination numbers in both Cisco Unified Communications Manager Administration and in the Cisco Unified Mobility Advantage server.
- If a CUMC client user ever changes his SIM card, the user must update the mobile number in the Cisco Unified Mobility Advantage server. The Cisco Unified Mobility Advantage server then uses AXL with the old mobile number to update Cisco Unified Communications Manager with the new mobile number and sends a new SIP REGISTER message to Cisco Unified Communications Manager.
- Ensure Cisco Unified Communications Manager nodes are statically created in the Cisco Unified Mobility Advantage server administration console.

- The Cisco Unified Mobility Advantage server only uses AXL to update the Cisco Unified Communications Manager database but does not listen to Cisco Unified Communications Manager database change notifications.

#### General Considerations

Keep in mind the following general considerations for the Cisco Unified Mobile Communicator device:

- You can add one or more remote destinations to the CUMC device (similar to the remote destination profile).
- No automatic migration support exists. You must manually reconfigure the device as a CUMC device.
- Only the first call gets supported, because in 2.5G, the data channel does not remain available after the voice call connects.
- The CUMA server can activate only one CUMC device per user.
- In configuration of the CUMC device, the reroute CSS and CSS represent key considerations.

#### Additional Information

See the [“Related Topics”](#) section on page 13-49.

## Dial-via-Office Reverse Callback

The Dial via Office Reverse Callback feature resembles the Mobile Voice Access feature, except that Cisco Unified Communications Manager makes both calls. From the CUMC client, using the data channel, the phone initiates the Reverse Callback feature. Cisco Unified Communications Manager then calls the remote destination first. When the remote destination answers, Cisco Unified Communications Manager calls the destination number.

#### Example of Dial-via-Office Reverse Callback

The following example illustrates the sequence of events that takes place in an instance of dial-via-office reverse callback:

- User invokes the Dial-via-Office feature on the phone and calls target DN 2000.
- Phone sends INVITE 2000 with the callback number that is specified in the SDP parameter “c=PSTN E164 4085551234.”
- Cisco Unified Communications Manager sends back 183 Session In Progress with Enterprise Feature Access Number (4085556666) in SDP parameter.
- Cisco Unified Communications Manager calls back remote destination 4085551234.
- When the remote destination answers the call, Cisco Unified Communications Manager redirects the call to the target DN 2000.

#### Dial-via-Office Reverse Callback to Remote Phone

Using the preceding example, the following characteristics apply to a Reverse Callback instance when a remote phone is called:

- Based on SDP parameter “a=setup:passive”, Cisco Unified Communications Manager determines its dial-via-office (reverse) call.
- Cisco Unified Communications Manager sends a “SIP/2.0 183 Session Progress” message.

- Based on SDP parameter “c=PSTN E164 4085551234,” Cisco Unified Communications Manager calls back remote phone.
- Remote phone answers and gets redirected to the target DN 2000.

CUMA support for this feature exists.

#### **Dial-via-Office Reverse Callback to Non-Remote Phone**

Using the preceding example, the following characteristics apply to a Reverse Callback instance when a non-remote phone is called:

- Based on SDP parameter “a=setup:passive”, Cisco Unified Communications Manager determines its dial-via-office (reverse) call.
- Cisco Unified Communications Manager sends “SIP/2.0 183 Session Progress” message.
- Based on SDP parameter “c=PSTN E164 4085553456,” Cisco Unified Communications Manager calls back the non-remote phone, which can be any PSTN phone at which the user wants to be contacted. A hotel phone represents an example of such a phone.
- Non-Remote Phone (4085553456) answers and gets redirected to the target DN 2000.

CUMA support for this feature exists.

Refer to the [“Use Case Scenarios for Dial-via-Office Reverse Callback”](#) section on page 13-16 for the use case scenarios that Cisco Unified Communications Manager supports with this feature.

#### **Additional Information**

See the [“Related Topics”](#) section on page 13-49.

## **Time-of-Day Access**

An access list determines whether a call should be extended to a remote destination that is enabled for the Mobile Connect feature. With the addition of time-based control, the Time-of-Day Access feature adds time as another determination factor. The feature allows administrators and users to determine whether a call should reach a remote destination based on the time of day when the call is received.

For calls to remote destinations, the Time-of-Day Access feature adds a ring schedule and associates the ring schedule with an access list to determine the time-of-day access settings for a remote destination.

The provisioning process includes provisioning the following entities:

- Access lists
- Remote destinations (configuring a ring schedule and associating the ring schedule with an access list for a remote destination)

As an extension to the existing access list feature, ensure the Time-of-Day Access feature is accessible to end users of Cisco Unified Communications Manager. Therefore, you can provision the feature through use of both Cisco Unified Communications Manager Administration (by administrators) and Cisco Unified CM User Options (by end users).

#### **Time-of-Day Access Example**

The following example illustrates a specific time-of-day access application:

Block 1800! during business hours for user browns.

**Further Topics**

This section includes the following topics:

- [Time-of-Day Access Configuration](#), page 13-11
- [Important Notes for Time-of-Day Access](#), page 13-12

The “[Use Case Scenarios for Time-of-Day Access](#)” section on page 13-16 provides use case scenarios for the time-of-day access feature with Cisco Unified Mobility, including migration considerations when migrating from a release of Cisco Unified Communications Manager prior to Release 7.0(x).

**Additional Information**

See the “[Related Topics](#)” section on page 13-49.

**Time-of-Day Access Configuration**

[Table 13-3](#) summarizes the procedures for configuring the Time-of-Day Access feature for Cisco Unified Mobility. For detailed instructions, see the chapters and sections that the table references.

**Table 13-3** *Time-of-Day Access Configuration Checklist*

<b>Configuration Steps</b>	<b>Related Procedures and Topics</b>
<p><b>Step 1</b></p> <p>In Cisco Unified Communications Manager Administration, configure an end user for whom you will enable the Time-of-Day Access feature.</p> <p>Use the <b>User Management &gt; End User</b> menu option.</p> <p><b>Note</b> Make sure that you check the Enable Mobility check box in the End User Configuration window.</p> <p><b>Note</b> Checking the Enable Mobility check box triggers licensing to consume device license units (DLUs) for Mobile Connect.</p>	<p><a href="#">End User Configuration</a>, <i>Cisco Unified Communications Manager Administration Guide</i></p> <p>For information on how licensing works with Mobile Connect, refer to the “<a href="#">Licenses for Cisco Unified Mobility</a>” section in the <i>Cisco Unified Communications Manager System Guide</i>.</p>
<p><b>Step 2</b></p> <p>For a particular user, configure access lists to use for Time-of-Day Access by assigning each list to the user. Create separate access lists for callers that are allowed and callers that are blocked.</p> <p><b>Note</b> An access list must have an owner. No system access list exists.</p> <p>Use the <b>Call Routing &gt; Class of Control &gt; Access List</b> menu option.</p>	<p><a href="#">Access List Configuration</a>, page 13-24</p>

Table 13-3 Time-of-Day Access Configuration Checklist (continued)

Configuration Steps	Related Procedures and Topics
<p><b>Step 3</b> Configure a remote destination for a user. Remote destinations represent the mobile (or other) phones that can accept transfers from the user desktop phone and that can initiate calls by using Mobile Voice Access.</p> <p>Use the <b>Device &gt; Remote Destination</b> menu option.</p> <p><b>Note</b> The same configuration also applies to dual-mode phones and to Cisco Unified Mobile Communicator Mobility Identity to set up time-of-day access.</p> <p>For successful time-of-day access configuration, you must configure the following areas in the Remote Destination Configuration window:</p> <ul style="list-style-type: none"> <li>• Use the Ring Schedule pane to configure a ring schedule for the remote destination.</li> <li>• Use the <i>When receiving a call during the above ring schedule</i> pane to specify the access list for which the Ring Schedule applies.</li> </ul> <p>Checking the Enable Mobile Connect check box for the remote destination enables Cisco Unified Mobility to apply the settings in the When Mobile Connect is Enabled pane to calls that are made to this remote destination. If the Enable Mobile Connect check box is not checked, the settings do not apply to incoming calls to this remote destination, but the settings remain intact for future use.</p>	<p><a href="#">Remote Destination Configuration, page 13-35</a></p>

**Additional Information**

See the [“Related Topics”](#) section on page 13-49.

**Important Notes for Time-of-Day Access**

The following important notes apply to time-of-day access configuration:

- A ring schedule associates with the time zone of a remote destination, not with the time zone of the Cisco Unified Communications Manager server. Use the Time Zone field in the Remote Destination Configuration window to specify the time zone of the remote destination.
- If a remote destination has no time-of-day access configuration, all calls get extended to the remote destination. By default, the All the time ring schedule radio button and the Always ring this destination radio button are checked, so that all calls get extended to the remote destination.
- Cisco recommends that you always configure an access list with members; avoid creating an empty access list that contains no members. If an empty access list is chosen in the *Ring this destination only if the caller is in* drop-down list box, all calls get blocked (instead of allowed). If an empty access list is chosen in the *Do not ring this destination if the caller is in* drop-down list box, all calls are allowed during the specified ring schedule. Either use of an empty access list could cause unnecessary confusion for end users.

Refer to the [“Use Case Scenarios for Time-of-Day Access” section on page 13-16](#) for the use case scenarios that Cisco Unified Communications Manager supports with this feature.

Refer to the user guide for the applicable Cisco Unified IP Phone model for details of the settings that end users can configure to customize their time-of-day access settings by using the Cisco Unified CM User Options windows.

#### **Additional Information**

See the [“Related Topics” section on page 13-49](#).

## **Directed Call Park via DTMF**

A user can park an existing call by using DTMF digits. Using Directed Call Park from the mobile phone, a user parks a call and inputs a unique mobility user park code. The user can subsequently retrieve the call with the code or have someone else retrieve the call with the code. This feature proves useful for certain vertical markets that require different departments or users to pick up calls.

When a user is in the enterprise and picks up a call on their mobile phone, they may want to pick the call up on a Cisco Unified IP Phone in a conference room or desk where the DN is not visible. The user can park the call and pick up the parked call with only their code.

When the mobile phone user is on an active call, by using the DTMF transfer feature, the user can park the call by transferring the parkee party to the park code that the system administrator configures and assigns to the user.

This feature allows the mobile phone user to park a call by transferring the parkee party to a user-selected park code. When the mobile phone user is on an active call, by using the DTMF transfer feature, the user can park the call by transferring the parkee party to the user-selected park code. The dialing sequence resembles the DTMF transfer sequence, except that a preconfigured parking code replaces the transfer number.

#### **Example of Directed Call Park via DTMF—Parking the Call**

In the following example, \*82 specifies exclude hold, \*84 specifies transfer, the pin specifies 12345, and the call park code specifies 3215. The following actions take place from the mobile phone:

1. Dial \*82 (to put the call on enterprise hold).
2. If necessary, put the mobile phone call on Hold, depending on the mobile phone model.
3. Make a new call to the enterprise with feature DID.
4. After the call connects, dial this digit sequence: 12345##84#3215##84#.

Cisco Unified Communications Manager puts the parkee party on hold and provides dial tone to the parker party, just like the Call Transfer feature.

After Cisco Unified Communications Manager receives the dialed park code digit, the digit analysis engine verifies whether the dialed park code digits are valid. If so, the Directed Call Park feature intercepts the park code and verifies whether the park code is available. If the dialed park code is valid and available, the parker party receives the ringback tone, and the secondary call terminates to a Cisco Unified Communications Manager generic device that associates with the selected park code. The generic device automatically answers and place the parker party on hold with music on hold (MOH) or tone on hold. The last \*84 completes the transfer of the parkee to the Cisco Unified Communications Manager generic device that associates with the selected park code. After the transfer completes, the parkee party receives the MOH or tone on hold, and the parkee gets parked on this selected park code and waits for retrieval.

If another user is already using the user-selected park code, Directed Call Park feature logic in Cisco Unified Communications Manager rejects that selected park code and plays busy tone to the parker party. The user gets to select another park code.

If the user-selected park code is not valid, Cisco Unified Communications Manager plays reorder tone to the parker party, and the user gets to select another park code.

For the Directed Call Park feature, be aware that the park code and code range are configurable across a cluster. Every Cisco Unified Communications Manager server in the cluster shares the park code and code range.

#### Example of Directed Call Park via DTMF—Retrieving the Parked Call

When a user attempts to retrieve the parked call, the user can go off hook on another mobile phone, and the user must use two-stage dialing to dial a digit string that contains the Directed Call Park retrieval prefix digits (for example, 22) plus the park code/code range (for example, 3215). The following sequence of events takes place:

1. Dial Enterprise Feature DID on mobile phone.
2. Upon connection, press PIN#1#223215 to retrieve the parked call.

Just like the existing Call Park feature, if the call does not get retrieved on time, the parked call reverts back to the phone number that is associated with the parker party by default.

If a shared line is configured for the phone line of the parker, all phones that are associated with the shared line will ring. In addition, the dPark feature allows the user to configure a call park reversion number in the Call Park Administration window, so if the call park reversion number is configured, the non-retrieved call reverts to this number, instead of to the parker party number.

Refer to [“Use Case Scenarios for Directed Call Park via DTMF”](#) section on page 13-17 for the use case scenarios that Cisco Unified Communications Manager supports with this feature.

#### Additional Information

See the [“Related Topics”](#) section on page 13-49.

## SIP URI Dialing

This feature supports Session Initiation Protocol (SIP) Universal Resource Identifier (URI) as an additional type of remote destination for Cisco Unified Mobility. When the DN is called, Cisco Unified Communications Manager extends the call to a SIP trunk that digit analysis selects with this SIP URI in the To: header.

This feature only allows routing that is based only on the domain name, not based on the full SIP URI.

When a remote destination of this type is configured, other Cisco Unified Mobility features, such as two-stage dialing, transformation to DN number when calling into Cisco Unified Communications Manager, Interactive Voice Response (IVR) support, caller ID match, or DTMF transfer and conferencing, do not get supported.

#### SIP URI Administration Details

The SIP URI dialing feature entails a relaxation of the business rules to allow the entry of a URI in the Destination Number field of the Remote Destination Configuration window. (From the Cisco Unified Communications Manager Administration menu bar, choose the **Device > Remote Destination** menu option.)

An additional requirement for this feature specifies that a SIP route pattern that matches the configured URI domain must be configured for the feature to work. To configure a SIP route pattern, from the Cisco Unified Communications Manager Administration menu bar, choose the **Call Routing > SIP Route Pattern** menu option.

#### SIP URI Example

For a remote destination, the SIP URI *user@corporation.com* gets configured. A SIP route pattern that specifies *corporation.com* must also get configured for the SIP URI remote destination to resolve correctly.

#### Additional Information

See the [“Related Topics”](#) section on page 13-49.

## Use Case Scenarios for Cisco Unified Mobility Features

The following sections describe the following use case scenarios that Cisco Unified Communications Manager supports for Cisco Unified Mobility features:

- [Use Case Scenarios for Mobile Connect, page 13-15](#)
- [Use Case Scenarios for Mobile Voice Access, page 13-16](#)
- [Use Case Scenarios for Dial-via-Office Reverse Callback, page 13-16](#)
- [Use Case Scenarios for Time-of-Day Access, page 13-16](#)
- [Use Case Scenarios for Directed Call Park via DTMF, page 13-17](#)

#### Additional Information

See the [“Related Topics”](#) section on page 13-49.

## Use Case Scenarios for Mobile Connect

Mobile Connect supports these use case scenarios:

- Receiving an outside call on desktop phone or mobile phone—An outside caller dials the user desktop extension. The desktop phone and mobile phone ring simultaneously. When the user answers one phone, the other phone stops ringing. The user can switch from the desktop phone to a mobile phone during a call without losing the connection. Switching gets supported for incoming and outgoing calls.
- Moving back from a mobile phone to a desktop phone—If a call was initiated to or from the desktop phone and then shifted to the mobile phone, the call can get shifted back to the desktop phone.
- Using mid-call enterprise features—During a Mobile Connect call, users can perform mid-call functions, including hold/resume, exclusive hold, transfer, and conference.
- Using enterprise features with two-stage dialing—When a user wants to place a call from a smartphone and the smartphone is in business mode, the call gets made through Cisco Unified Communications Manager. Consider the function as similar to Mobile Voice Access, but without voice prompts. Users can also use this method to turn Mobile Connect on or off.

#### Additional Information

See the [“Related Topics”](#) section on page 13-49.

## Use Case Scenarios for Mobile Voice Access

Mobile Voice Access supports these use case scenarios:

- Initiating a mobility call from a remote phone, such as a mobile phone—Users can use Mobile Voice Access to initiate calls from a mobile phone as if dialing from the desktop phone.
- Moving from a mobile phone to a desktop phone during a mobile-phone-initiated call—If the user initiated a call from a mobile phone by using Mobile Voice Access, the user can shift to the desktop phone during the call without losing the connection and can shift back again as needed.

### Additional Information

See the [“Related Topics”](#) section on page 13-49.

## Use Case Scenarios for Dial-via-Office Reverse Callback

The Dial Via Office Reverse Callback feature supports the following use case scenarios:

- Mobile user invokes Reverse Callback feature to remote destination and succeeds.
- Mobile user invokes Reverse Callback feature to non-remote destination and succeeds.
- Mobile user invokes Reverse Callback feature and fails.

### Additional Information

See the [“Related Topics”](#) section on page 13-49.

## Use Case Scenarios for Time-of-Day Access

The use case scenarios that follow detail the function of the time-of-day access feature with activated access lists that were configured prior to the addition of the time-of-day access feature in Release 7.0(1) of Cisco Unified Communications Manager, as well as with new provisioning that takes place for the feature starting with Release 7.0(1) of Cisco Unified Communications Manager.

### Supported Use Cases for Migrating Activated Access Lists from an Earlier Cisco Unified Communications Manager Release

The following use cases detail the function of the Time-of-Day Access feature with Cisco Unified Mobility when migration of an activated access list from a previous release of Cisco Unified Communications Manager to Release 7.0(x) or later takes place.

- Use Case #1—No allowed or blocked access list got configured prior to Release 7.0(x) of Cisco Unified Communications Manager.

Result after migration: The system allows all calls at all hours. The Remote Destination Configuration window displays the When Mobile Connect is Enabled pane. In the Ring Schedule pane, the All the time radio button is checked. In the When Receiving a call during the above ring schedule pane, the Always ring this destination radio button is checked.

- Use Case #2—Only an allowed access list got configured prior to Release 7.0(x) of Cisco Unified Communications Manager.

Result after migration: Only the callers that belong to the allowed access list can reach the associated remote destination. The Remote Destination Configuration window displays the When Mobile Connect is Enabled pane. In the Ring Schedule pane, the All the time radio button is checked. In the When Receiving a call during the above ring schedule pane, the Ring this destination only if caller is in radio button is checked, and the access list displays in the corresponding drop-down list box.

- Use Case #3—Only a blocked access list got configured prior to Release 7.0(x) of Cisco Unified Communications Manager.

Result after migration: The callers that belong to the blocked access list cannot reach the associated remote destination, but all other callers can call the remote destination at all hours. The Remote Destination Configuration window displays the When Mobile Connect is Enabled pane. In the Ring Schedule pane, the All the time radio button is checked. In the When Receiving a call during the above ring schedule pane, the Do not ring this destination if caller is in radio button is checked, and the access list displays in the corresponding drop-down list box.

#### Use Cases for Time-of-Day Access with the Current Cisco Unified Communications Manager Release

The following use cases detail the function of the Time-of-Day Access feature with Cisco Unified Mobility with the current release of Cisco Unified Communications Manager:

- Use Case #4—Only allow calls during business hours.

Configuration: Configure a ring schedule that specifies business hours from Monday to Friday and choose the Always ring this destination radio button.

Result: The system allows all callers during business hours, but no calls get extended to this remote destination outside business hours.

- Use Case #5—Only allow calls from certain numbers (for example, from coworkers) during business hours.

Configuration: Configure a ring schedule that specifies business hours from Monday to Friday, choose the Ring this destination only if the caller is in radio button, and specify an access list.

Result: Only callers that belong to the access list can call the remote destination during business hours; all other callers get blocked during business hours. Outside business hours, no calls ring this remote destination.

- Use Case #6—Block certain numbers (for example, 1800 numbers) during business hours.

Configuration: Configure a ring schedule that specifies business hours from Monday to Friday, choose the Don't ring this destination if the caller is in radio button, and specify an access list.

Result: Only callers that belong to the access list get blocked from calling the remote destination during business hours; all other callers can call the remote destination during business hours. Outside business hours, no calls ring this remote destination.

#### Additional Information

See the [“Related Topics” section on page 13-49](#).

## Use Case Scenarios for Directed Call Park via DTMF

The Directed Call Park via DTMF feature of Cisco Unified Mobility supports the following use cases:

- Mobile phone user parks call on selected park code.
- Mobile phone user parks call on selected park code that is unavailable.
- Mobile phone user parks call on selected park code that is invalid.
- Mobile phone user fails to enter park code after entering the DTMF transfer code.
- Parkee party disconnects while the parker party attempts to park the call.
- Parkee party disconnects while it is parked on a selected park code and is waiting for retrieval.
- User dials Directed Call Park retrieval digits plus a park code that has not been occupied.

- Administrator configures a translation pattern, so the length of the string of digits to park a call and to retrieve a call are the same.
- User retries a parked call.
- A parked call reverts.
- While a park code is occupied, one of the following entities gets modified or deleted: the park code or code range, the Directed Call Park park-prefix digits, or the Directed Call Park retrieval-prefix digits.
- Directed call park gets specified when the network is partitioned.

**Additional Information**

See the [“Related Topics”](#) section on page 13-49.

## Interactions and Restrictions

Most standard Cisco Unified Communications Manager features are fully compatible with Cisco Unified Mobility features, except as indicated in the following sections:

- [Interactions](#), page 13-18
- [Restrictions](#), page 13-20

**Additional Information**

See the [“Related Topics”](#) section on page 13-49.

## Interactions

The following sections detail the interactions between Cisco Unified Mobility and other Cisco Unified Communications Manager components:

- [Licensing](#), page 13-19
- [Number of Supported Calls](#), page 13-19
- [Auto Call Pickup](#), page 13-19

**Additional Information**

See the [“Related Topics”](#) section on page 13-49.

## Licensing

Mobile Connect uses licensing. Checking the Enable Mobility check box in the End User Configuration window triggers licensing to consume device license units (DLUs) for Mobile Connect; the number of licenses that get consumed depends on whether you assign an adjunct device to the end user specifically for Cisco Unified Mobility. For specific information on how licensing works with Cisco Unified Mobility, see the following sections:

- [“Licenses for Cisco Unified Mobility”](#) section in the *Cisco Unified Communications Manager System Guide*.
- [“End User Configuration Settings”](#) in the *Cisco Unified Communications Manager Administration Guide*.

**Additional Information**

See the [“Related Topics” section on page 13-49](#).

## Number of Supported Calls

Up to two simultaneous Mobile Connect calls get supported at one time. Any additional calls that come in automatically get transferred to the user voice mail.

Each remote destination supports a maximum of two active calls. For Cisco Unified Mobility, each remote destination supports a maximum of two active calls via Cisco Unified Communications Manager. Using the enterprise feature access directory number (DID number) to transfer or conference with DTMF counts as one call. When a Cisco Unified Mobility user receives a call while the user has two active calls for the remote destination or while the user is using DTMF to transfer/conference a call from the remote destination, the received call does not reach the remote destination and instead goes to the enterprise voice mail; that is, if Call Forward No Answer (CFNA) is configured or if the call is not answered on a shared line.

**Additional Information**

See the [“Related Topics” section on page 13-49](#).

## Auto Call Pickup

Cisco Unified Mobility interacts with auto call pickup based on the service parameter selection. When the Auto Call Pickup Enabled service parameter is set to True, end users need only to press the PickUp softkey to pick up a call.

If the Auto Call Pickup Enabled service parameter is set to False, end users need to press the PickUp, GPickUp, or OPickUp softkey and then the Answer softkey.

**Example**

Phone A, phone B (Cisco Unified Mobility subscriber), and phone C belong to the Engineering group; phone D, phone E, and phone F belong to the Accounting group.

Phone D calls phone A in the Engineering Group. Phone A rings, and phone B and phone C in the group receive pickup notice.

If Auto Call Pickup is enabled, press the PickUp softkey from phone B to use Cisco Unified Mobility features later on.

If Auto Call Pickup is not enabled, press PickUp softkey from phone B, which causes the remote destinations that are associated with phone B to ring. Press the Answer softkey on phone B, which causes the remote destinations to stop ringing. The user can subsequently perform mobile-phone pickup and desktop pickup.

**Additional Information**

See the [“Related Topics” section on page 13-49](#).

## Restrictions

Cisco Unified Mobility enforces the following restrictions in operating with other Cisco Unified Communications Manager components.

**Forced Authorization Code and Client Matter Code**

The Forced Authorization Code and Client Matter Code (FAC/CMC) feature does not work with Mobile Voice Access.

The Forced Authorization Code (FAC) does not get invoked for Mobile Connect [Single Number Reach (SNR)] calls to a remote destination.

**Multilevel Precedence and Preemption (MLPP)**

Mobile Connect does not work with Multilevel Precedence and Preemption (MLPP). If a call is preempted with MLPP, Mobile Connect features get disabled for that call.

**Video Calls**

Mobile Connect services do not extend to video calls. A video call that is received at the desktop phone cannot get picked up on the mobile phone.

**Remote Destinations**

Ensure remote destinations are Time Division Multiplex (TDM) devices. You cannot configure IP phones within a Cisco Unified Communications Manager cluster as remote destinations.

Ensure remote destinations specify PSTN numbers or numbers across ICT trunks.

Remote destinations cannot resume calls that Cisco Unified IP Phones put on hold.

**Remote Destination Profiles**

When configuring a directory number that is associated with a remote destination profile, you must use only ASCII characters in the Display (Internal Caller ID) field on the Directory Number Configuration window.

**Conferencing**

Users cannot initiate a meet-me conference as conference controller by using Mobile Voice Access but can join a meet-me conference.

If an existing conference call is initiated from a shared-line IP phone or dual-mode phone or smartphone that is a remote destination, no new conference party can get added to the existing conference after the call is sent to a mobile phone or a dual-mode handoff action occurs. To permit the addition of new conference parties, use the Advanced Ad Hoc Conference Enabled service parameter.

**QSIG**

Mobility does not support QSIG.

**QSIG Path Replacement**

QSIG (Q Signaling) path replacement does not get supported.

**Dual-Mode Handoff and Caller ID**

Dual-mode handoff requires that caller ID be available in the cellular network.

**Dual-Mode Phones**

While a dual-mode phone is in Wi-Fi enterprise mode, no CTI applications control it nor monitor it.

The In Use Remote indicator for dual-mode phones on a shared line call in the WLAN will disappear if the dual-mode phone goes out of WLAN range.

**Enterprise Features in GSM That Is Using DTMF**

Availability of enterprise features in GSM that is using DTMF depends upon the features that are supported in the third-party smartphones.

**Gateways and Ports**

Only H.323 VoIP gateways get supported for Mobile Voice Access.

Mobile Connect features do not get supported for T1 CAS, FXO, FXS and BRI.

**Enterprise Features From Cellular Networks**

Enterprise features from cellular networks require out-of-band DTMF.

**Call Anchoring**

Call anchoring, which is performed based on caller ID, gets supported only from calls from registered single-mode or dual-mode phones

**Call Forwarding**

You do not need to configure settings for call forward unregistered, if the end user has configured remote destinations. Appropriate call forwarding will get handled as part of the Mobile Connect process.

**Multiple-Node Cluster Environment**

In a multiple-node cluster environment, if the Cisco Unified Communications Manager Release 6.0 (or later) publisher is unreachable, any changes that end users make to turn Mobile Connect off or on by way of Mobile Voice Access or two-stage dialing do not get saved.

**Service Parameters**

Enterprise feature access service parameters apply to standard phones and smartphones; however, smartphones generally use one-touch keys to send the appropriate codes. Administrators must configure any smartphones that will be used with Mobile Connect to use either the default codes for enterprise feature access or the codes that are specified in the smartphone documentation.

**Note**

---

The enterprise feature access virtual device is always in the Default region. If you change the default to another region, the field still remains as Default.

---

**Additional Information**

See the [“Related Topics” section on page 13-49](#).

## System Requirements

Mobile Connect and Mobile Voice Access work with Cisco Unified IP Phones 7906, 7911, 7941/61, 7962/42, 7970/71, 7975 that are running SIP or SCCP. They require the following software components:

- Cisco Unified Communications Manager 6.0 or later.
- Cisco Unified Mobile Voice Access service, which runs only on the publisher.
- Cisco Unified Communications Manager Locale Installer (if you want to use non-English phone locales or country-specific tones).

**Additional Information**

See the [“Related Topics”](#) section on page 13-49.

## Migrating from Cisco Unified MobilityManager

Follow this process to migrate standalone Cisco Unified MobilityManager data to Cisco Unified Communications Manager Release 6.0(1) or later:

1. Upgrade the Cisco Unified MobilityManager system to Release 1.2(5), if necessary. See the *Release Notes for Cisco Unified MobilityManager Release 1.2(5)*.
2. Log in to Cisco Unified MobilityManager and export the configuration data in CSV format. For instructions, see the *Release Notes for Cisco Unified MobilityManager Release 1.2(5)*.
3. Log in to Cisco Unified Communications Manager Administration Release 6.0(1) (or later) and use the Bulk Administration Import/Export windows to import the CSV data files that were previously exported from Cisco Unified MobilityManager. Refer to the “Access List,” “Remote Destination,” and “Remote Destination Profile” chapters in the *Cisco Unified Communications Manager Bulk Administration Guide*.

**Additional Information**

See the [“Related Topics”](#) section on page 13-49.

## Configuring Cisco Unified Mobility

This section provides an overview checklist of the procedures and steps that are necessary for an administrator to configure Cisco Unified Mobility in Cisco Unified Communications Manager Administration. The section also includes detailed procedures for each Cisco Unified Communications Manager Administration menu option.

End users use the Cisco Unified CM User Options windows to further configure or modify the Cisco Unified Mobility settings that apply to their mobile phones.

This section covers the following topics:

- [Cisco Unified Mobility Configuration Checklist, page 13-23](#)
- [Access List Configuration, page 13-24](#)
- [Remote Destination Profile Configuration, page 13-29](#)
- [Remote Destination Configuration, page 13-35](#)
- [Mobile Voice Access Media Resource Configuration, page 13-40](#)
- [H.323 Gateway Configuration for Mobile Voice Access, page 13-42](#)
- [Mobile Voice Access Configuration by Service Parameter, page 13-47](#)
- [Mobility Setting Configuration, page 13-48](#)
- [Mobility Softkey Configuration, page 13-48](#)

**Additional Information**

See the [“Related Topics”](#) section on page 13-49.

## Cisco Unified Mobility Configuration Checklist

Table 13-4 summarizes the procedures for configuring Cisco Unified Mobility. For detailed instructions, see the chapters and sections that the table references.

**Table 13-4** Cisco Unified Mobility Configuration Checklist

Configuration Steps		Related Procedures and Topics
<b>Step 1</b>	Activate the Cisco Unified Mobile Voice Access Service in Cisco Unified Serviceability. You must activate this service on the first node in the cluster.	For information on activating services, refer to the <i>Cisco Unified Serviceability Administration Guide</i> .
<b>Step 2</b>	Configure user accounts. <b>Note</b> Make sure that you check the Enable Mobility and Mobile Voice Access check boxes in the End User Configuration window. <b>Note</b> Checking the Enable Mobility check box triggers licensing to consume device license units (DLUs) for Mobile Connect.	<a href="#">End User Configuration</a> , <i>Cisco Unified Communications Manager Administration Guide</i> For information on how licensing works with Mobile Connect, refer to the “ <a href="#">Licenses for Cisco Unified Mobility</a> ” section in the <i>Cisco Unified Communications Manager System Guide</i> .
<b>Step 3</b>	Create access lists for Mobile Connect by assigning each list to the Mobile Connect user and specifying whether the list is allowed.	<a href="#">Access List Configuration</a> , page 13-24.
<b>Step 4</b>	Create remote destination profiles and assign each user to a profile.	<a href="#">Remote Destination Profile Configuration</a> , page 13-29.
<b>Step 5</b>	Associate desktop directory numbers (DNs) for the user.	<a href="#">Associating a Directory Number with a Remote Destination Profile</a> , page 13-31.
<b>Step 6</b>	Add remote destinations by selecting the previously-defined profile as part of the configuration.	<a href="#">Remote Destination Configuration</a> , page 13-35.
<b>Step 7</b>	In the Service Parameters Configuration window: <ul style="list-style-type: none"> <li>Choose <b>True</b> for Enable Mobile Voice Access and enter the Mobile Voice Access number, which is the DID number that end users use to reach Mobile Voice Access.</li> </ul> <b>Note</b> To make Mobile Voice Access calls, you must configure these service parameters and check the Enable Mobile Voice Access check box in the End User Configuration window. <ul style="list-style-type: none"> <li>Choose <b>True</b> for Enable Enterprise Feature Access to enable access to hold, resume, transfer, and conference features from remote destinations.</li> </ul>	<a href="#">Service Parameters Configuration</a> , <i>Cisco Unified Communications Manager Administration Guide</i>
<b>Step 8</b>	Configure the media resources for Mobile Voice Access.	<a href="#">Mobile Voice Access Media Resource Configuration</a> , page 13-40.

Table 13-4 Cisco Unified Mobility Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
<b>Step 9</b>	As an alternative, configure Mobile Voice Access by configuring a service parameter and the enterprise feature access DID directory number.	
<b>Step 10</b>	Configure mobility settings for dual-mode phone handoff.	<a href="#">Mobility Setting Configuration, page 13-48.</a>
<b>Step 11</b>	Configure time-of-day access for users. Use the fields in the When Mobile Connect is Enabled pane of the Remote Destination Configuration window to do so.	<a href="#">Remote Destination Configuration, page 13-35.</a>

**Additional Information**

See the “[Related Topics](#)” section on page 13-49.

## Access List Configuration

After the remote destination profiles are created, you can define access lists to explicitly allow or block the use of specific phone numbers for Mobile Connect.

To configure access lists, see the following sections:

- [Finding Access Lists, page 13-25](#)
- [Configuring Access Lists, page 13-26](#)
- [Deleting Access Lists, page 13-27](#)

**Additional Information**

See the “[Related Topics](#)” section on page 13-49.

## Finding Access Lists

Because you might have several access lists in your network, Cisco Unified Communications Manager lets you locate specific access lists by using specific criteria as the basis. Use the following procedure to locate access lists.

**Note**

During your work in a browser session, Cisco Unified Communications Manager Administration retains your access list search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your access list search preferences until you modify your search or close the browser.

**Procedure**

**Step 1** In the menu bar, choose **Call Routing > Class of Control > Access List**.

The Find and List Access Lists window displays. Records from an active (prior) query may also display in the window.

**Step 2** To find all records in the database, ensure the dialog box is empty; go to [Step 3](#).

To filter or search records

- From the first drop-down list box, choose a search parameter.
- From the second drop-down list box, choose a search pattern.
- Specify the appropriate search text, if applicable.



**Note** To add additional search criteria, click the **+** button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the **-** button to remove the last added criterion or click the **Clear Filter** button to remove all added search criteria.

**Step 3** Click **Find**.

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.



**Note** You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking **Delete Selected**. You can delete all configurable records for this selection by clicking **Select All** and then clicking **Delete Selected**.

**Step 4** From the list of records that display, click the link for the record that you want to view.



**Note** To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

#### Additional Information

See the [“Related Topics” section on page 13-49](#).

## Configuring Access Lists

The following procedure describes how to configure an access list.

### Procedure

**Step 1** In the menu bar, choose **Call Routing > Class of Control > Access List**.

The Find and List Access Lists window displays.

**Step 2** Perform one of the following tasks:

- To copy an existing access list, locate the appropriate access list as described in the [“Finding Access Lists” section on page 13-25](#). Click the **Copy** icon next to the access list that you want to copy. The window displays the copy of the access list. Change the value in the Name field, and continue with [Step 3](#).
- To add a new access list, click the **Add New** button and continue with [Step 3](#).

- To update an existing access list, locate the appropriate access list as described in the [“Finding Access Lists”](#) section on page 13-25, and continue with [Step 3](#).
- Step 3** Enter values for the parameters that are described in [Table 13-5](#).
- Step 4** Click **Save**.
- If you are configuring a new access list, the window reopens to display Access List Member Information area.
- Step 5** If you want to configure the members of an access list, click **Add Member**.
- The Access List Member Detail window opens.
- Step 6** Enter values for the parameters that are described in [Table 13-6](#).
- Step 7** Click **Save**.
- The Access List Configuration window reopens to show the new number or filter in the Selected Filters area.
- Step 8** From the Access Configuration window, add additional filters and also modify any existing access list as needed:
- To modify a DN mask, click the link for the directory number at the bottom of the window under Access List Members, enter your change, and click **Save**.
  - To delete a filter, select the filter and click **Delete**.
  - To inactivate a filter without deleting it, select the filter in the Selected Filters pane and click the down arrow to move the filter to the Removed Filters pane.
  - To activate a filter, select the filter in the Removed Filters pane and click the up arrow to move the filter to the Selected filters area.
  - To create a new access list with the same members as the existing list, click **Copy**.
- 

#### Additional Information

See the [“Related Topics”](#) section on page 13-49.

## Deleting Access Lists

To delete an access list in Cisco Unified Communications Manager Administration, perform the following procedure.

#### Before You Begin

You cannot delete access lists that remote destinations are using. To find out which items are using the access list, choose **Dependency Records** from the Related Links drop-down list box that is on the Access List Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the [“Accessing Dependency Records”](#) section on page A-2. If you try to delete an access list that is in use, Cisco Unified Communications Manager displays a message. Before deleting an access list that is currently in use, you must perform either or both of the following tasks:

- Assign a different access list to any remote destinations that are using the access list that you want to delete. See the [“Remote Destination Configuration”](#) section on page 13-35.
- Delete the remote destinations that are using the access list that you want to delete. See the [“Deleting Remote Destinations”](#) section on page 13-37.

### Procedure

- 
- Step 1** Locate the access list that you want to delete, as described in the “[Finding Access Lists](#)” section on page 13-25.
- Step 2** After the Access Lists window displays, click **Delete**.
- Step 3** To continue with the deletion, click **OK**.
- 

### Additional Information

See the “[Related Topics](#)” section on page 13-49.

## Access List Configuration Settings

[Table 13-5](#) describes the available settings in the Access List Configuration window.

**Table 13-5** Access List Configuration Settings

Field	Description
<b>Access List Information</b>	
Name	Enter a unique name (between 1 and 50 characters) for this access list.  You may use all characters except quotes (“), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).
Description	Enter a text description (between 1 and 128 characters) for this access list.  You may use all characters except nonprinting characters, such as tabs and quotes (“).
Owner	From the drop-down list box, choose the end user to whom the access list applies.
Allowed	Click this radio button to allow calls from member phone numbers to be passed to the remote destinations.
Blocked	Click this radio button to block calls from member phone numbers from being passed to the remote destinations.

**Table 13-5 Access List Configuration Settings (continued)**

Field	Description
<b>Access List Member Information</b>	
Selected Filters	<p>This pane displays the current members of this access list. Members comprise the following types:</p> <ul style="list-style-type: none"> <li>• Private—This filter applies to calls that come from private numbers, which do not display caller ID.</li> <li>• Not Available—This filter applies to calls that come from numbers that do not have caller ID.</li> <li>• Directory Number—This filter specifies a directory number that is specified between parentheses. For example, (12345). Valid values include the digits 0 through 9, the wildcard X, !, and #.</li> </ul> <p>Use the arrows below this pane to move the access list members to or from this pane.</p> <p><b>Add Member</b>—Click this button to add a new member to the Selected Filters pane. The Add List Member Detail window displays. See the <a href="#">“Access List Member Detail Configuration Settings”</a> section on page 13-29 for details.</p>
Removed Filters	<p>This pane specifies filters that have been defined for this access list but that are not currently selected.</p> <p>Use the arrows above this pane to move the access list members to or from this pane.</p>

**Additional Information**

See the [“Related Topics”](#) section on page 13-49.

## Access List Member Detail Configuration Settings

Table 13-6 describes the available settings in the Access List Member Detail window.

**Table 13-6** Access List Member Detail Configuration Settings

Field	Description
Filter Mask	Select an option from the drop-down list box. You can choose to enter a directory number, filter out calls that do not have caller ID (Not Available), or specify a number that will be allowed or blocked without displaying the caller ID (Private).
DN Mask	If you chose Directory Number in the Filter Mask field, enter a phone number or filter in the DN Mask field. You can use the following wild cards to define a filter: <ul style="list-style-type: none"> <li>• X (upper or lower case)—Matches a single digit.</li> <li>• !—Matches any number of digits.</li> <li>• #—Used as a single digit for exact match.</li> </ul> Examples: <ul style="list-style-type: none"> <li>• 408! matches any number that starts with 408.</li> <li>• 408555123X matches any number between 4085551230 and 4085551239.</li> </ul>

### Additional Information

See the “[Related Topics](#)” section on page 13-49.

## Remote Destination Profile Configuration

To configure remote destination profiles, see the following sections:

- [Finding Remote Destination Profiles](#), page 13-29
- [Configuring a Remote Destination Profile](#), page 13-31
- [Deleting Remote Destination Profiles](#), page 13-31

### Additional Information

See the “[Related Topics](#)” section on page 13-49.

## Finding Remote Destination Profiles

Because you might have several remote destination profiles in your network, Cisco Unified Communications Manager lets you locate specific remote destination profiles by using specific criteria as the basis. Use the following procedure to locate remote destination profiles.

**Note**

---

During your work in a browser session, Cisco Unified Communications Manager Administration retains your remote destination profile search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your remote destination profile search preferences until you modify your search or close the browser.

---

**Procedure**

---

**Step 1** In the menu bar, choose **Device > Device Settings > Remote Destination Profile**.

The Find and List Remote Destination Profiles window displays. Records from an active (prior) query may also display in the window.

**Step 2** To find all records in the database, ensure the dialog box is empty; go to [Step 3](#).

To filter or search records

- From the first drop-down list box, choose a search parameter.
- From the second drop-down list box, choose a search pattern.
- Specify the appropriate search text, if applicable.

**Note**

---

To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the **Clear Filter** button to remove all added search criteria.

---

**Step 3** Click **Find**.

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

**Note**

---

You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking **Delete Selected**. You can delete all configurable records for this selection by clicking **Select All** and then clicking **Delete Selected**.

---

**Step 4** From the list of records that display, click the link for the record that you want to view.

**Note**

---

To reverse the sort order, click the up or down arrow, if available, in the list header.

---

The window displays the item that you choose.

---

**Additional Information**

See the [“Related Topics”](#) section on page 13-49.

## Configuring a Remote Destination Profile

The remote destination profile contains the parameters that apply to all remote destinations for the user. After configuring user accounts for Mobile Connect (refer to the “[End User Configuration](#)” chapter in the *Cisco Unified Communications Manager Administration Guide*), you can create a remote destination profile for the user.

To configure a remote destination profile, perform the following procedure:

### Procedure

- 
- Step 1** In the menu bar, choose **Device > Device Settings > Remote Destination Profile**.
- Step 2** Perform one of the following tasks:
- To copy an existing remote destination profile, locate the appropriate remote destination profile as described in the “[Finding Remote Destination Profiles](#)” section on page 13-29. Click the **Copy** icon next to the remote destination profile that you want to copy. The window displays the copy of the remote destination profile. Change the value in the Name field and continue with [Step 3](#).
  - To add a new remote destination profile, click the **Add New** button and continue with [Step 3](#).
  - To update an existing remote destination profile, locate the appropriate remote destination profile as described in the “[Finding Remote Destination Profiles](#)” section on page 13-29 and continue with [Step 3](#).
- Step 3** Enter the appropriate settings as described in [Table 13-7](#).
- Step 4** Click **Save**.
- 

### Additional Information

See the “[Related Topics](#)” section on page 13-49.

## Associating a Directory Number with a Remote Destination Profile

After creating a remote destination profile, you must associate the DN record for the desktop phone or phones for the user. Click the Add a New DN link on the Remote Destination Profile Configuration window and follow the instructions in the “[Directory Number Configuration](#)” chapter of the *Cisco Unified Communications Manager Administration Guide*.



### Note

If the remote destination profile is dissociated on the Directory Number configuration window, you must check the Line Association check box for the DN on the Remote Destination window to reassociate it.

### Additional Information

See the “[Related Topics](#)” section on page 13-49.

## Deleting Remote Destination Profiles

To delete a remote destination profile in Cisco Unified Communications Manager Administration, perform the following procedure.

**Before You Begin**

You cannot delete remote destination profiles that remote destinations and directory numbers are using. To find out which items are using the remote destination profiles, choose **Dependency Records** from the Related Links drop-down list box that is on the Remote Destination Profile Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the [“Accessing Dependency Records” section on page A-2](#). If you try to delete a remote destination profile that is in use, Cisco Unified Communications Manager displays a message. Before deleting a remote destination profile that is currently in use, you must perform either or both of the following tasks:

- Assign a different remote destination profile to any remote destinations and directory numbers that are using the remote destination profile that you want to delete. See the [“Remote Destination Configuration” section on page 13-35](#).
- Delete the remote destinations and directory numbers that are using the remote destination profile that you want to delete. See the [“Remote Destination Configuration” section on page 13-35](#) and the [“Directory Number Configuration” chapter in the Cisco Unified Communications Manager Administration Guide](#).

**Procedure**

- 
- Step 1** Locate the remote destination profile that you want to update, as described in the [“Finding Remote Destination Profiles” section on page 13-29](#).
  - Step 2** After the Remote Destination Profiles window displays, click **Delete**.
  - Step 3** To continue with the deletion, click **OK**.
- 

**Additional Information**

See the [“Related Topics” section on page 13-49](#).

**Remote Destination Profile Configuration Settings**

[Table 13-7](#) describes the available settings in the Remote Destination Profile Configuration window.

**Table 13-7 Remote Destination Profile Configuration Settings**

Field	Description
<b>Remote Destination Profile Information</b>	
Name	Enter a text name for the remote destination profile.
Description	Enter a text description of the remote destination profile.
User ID	Choose the user to whom this profile is assigned. The selection must match the ID of a user in the End User Configuration window where Enable Mobility is checked.
Device Pool	Choose the device pool that applies to this profile. The device pool defines sets of common characteristics for devices, such as region, date/time group, softkey template, and MLPP information.
Calling Search Space	Choose the calling search space to be used for routing Mobile Connect and Mobile Voice Access calls.

**Table 13-7 Remote Destination Profile Configuration Settings (continued)**

Field	Description
User Hold Audio Source	Choose the audio option for users on hold for Mobile Connect and Mobile Voice Access calls.
Network Hold MOH Audio Source	Choose the audio source from the IOS gateway that provides multicasting audio source for Mobile Connect and Mobile Voice Access calls.
Privacy	Choose a privacy option for the profile.  For more configuration information, refer to <a href="#">Barge and Privacy</a> in the <i>Cisco Unified Communications Manager Features and Services Guide</i> .
Rerouting Calling Search Space	Choose a calling search space to be used if Mobile Connect calls need to be rerouted.  <b>Note</b> Ensure that the gateway that is configured for routing mobile calls is assigned to the partition that belongs to the Rerouting Calling Search Space. Cisco Unified Communications Manager determines how to route calls based on the remote destination number and the Rerouting Calling Search Space.
Calling Party Transformation CSS	Choose the calling search space for transformations. This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device.  <b>Note</b> The partitions in the calling search space should contain only calling party transformations.  <b>Note</b> Ensure the calling search space is not null because no transformations can apply to null partitions.  <b>Note</b> The device takes on the attributes of the Calling Party Transformation Pattern because you assign the pattern to a partition where the Calling Party Transformation CSS exists. For example, when you configure the Calling Party Transformation CSS under <b>Call Routing &gt; Class of Control &gt; Calling Search Space</b> , you assign the CSS to a partition; when you configure the Calling Party Transformation CSS under <b>Call Routing &gt; Transformation Pattern &gt; Calling Party Transformation Pattern</b> , you choose the partition where the Calling Party Transformation CSS is assigned.
Use Device Pool Calling Party Transformation CSS	To use the Calling Party Transformation CSS that is configured in the device pool that is assigned to this device, check this check box. If you do not check this check box, the device uses the Calling Party Transformation CSS that you configured in the Remote Destination Profile Configuration window.

Table 13-7 Remote Destination Profile Configuration Settings (continued)

Field	Description
User Locale	<p>From the drop-down list box, choose the locale that is associated with the phone user interface. The user locale identifies a set of detailed information, including language and font, to support users.</p> <p>Cisco Unified Communications Manager makes this field available only for phone models that support localization.</p> <p><b>Note</b> If no user locale is specified, Cisco Unified Communications Manager uses the user locale that is associated with the device pool.</p> <p><b>Note</b> If the users require information to display (on the phone) in any language other than English, verify that the locale installer is installed before configuring user locale. Refer to the Cisco Unified Communications Manager Locale Installer documentation.</p>
Ignore presentation indicators (internal calls only)	Check the check box if you want to ignore the connected line ID presentation. Use this configuration for internal calls.
<b>Associated Remote Destinations</b>	
Add a New Remote Destination	Click this link to open the Remote Destination Configuration window, where you can configure a new remote destination to associate with this remote destination profile. By default, the current remote destination profile is selected in the Remote Destination Profile field of the new remote destination. Refer to the <a href="#">“Remote Destination Configuration”</a> section on page 13-35 for details.
Name	For a remote destination that already exists and has been associated with this remote destination profile, this column displays the name of the remote destination.
Destination Number	For a remote destination that already exists and has been associated with this remote destination profile, this column displays the destination number of the remote destination.
<b>Do Not Disturb</b>	
Do Not Disturb	Check this check box to enable Do Not Disturb on the phone.
DND Option	<p>This Call Reject option specifies that no incoming call information gets presented to the user.</p> <p><b>Note</b> For mobile devices, dual-mode phones, and phones that are running SCCP, you can only choose the Call Reject option. When you activate DND Call Reject on a mobile device or dual-mode phone, no call information gets presented to the device.</p>

**Additional Information**

See the [“Related Topics”](#) section on page 13-49.

## Remote Destination Configuration

After remote destination profiles and access lists are created, you can enter individual remote destinations and assign each to a profile. Each remote destination presents a mobile or other phone that can be configured to accept transfers from the desktop phone of the user.

After you save a new remote destination, the Association Information pane displays in the window. This section lists the desk phone numbers that have been assigned to the remote destination profile. You can click a link to open the associated Directory Number Information window. See [Configuring a Directory Number](#) in the *Cisco Unified Communications Manager Administration Guide*.

**Note**

This section describes how to access remote destination records by opening the Remote Destination window. You can also open an existing or new record in the Remote Destination Configuration window by clicking the Add a New Remote Destination link at the bottom of the remote destination profile. See the [“Finding Remote Destination Profiles”](#) section on page 13-29 for instructions on displaying a remote destination profile.

To configure remote destinations, refer to the following sections:

- [Finding Remote Destinations, page 13-35](#)
- [Configuring Remote Destinations, page 13-36](#)
- [Deleting Remote Destinations, page 13-37](#)
- [Remote Destination Configuration Settings, page 13-38](#)

**Additional Information**

See the [“Related Topics”](#) section on page 13-49.

## Finding Remote Destinations

Because you might have several remote destinations in your network, Cisco Unified Communications Manager lets you locate specific remote destinations by using specific criteria as the basis. Use the following procedure to locate remote destinations.

**Note**

During your work in a browser session, Cisco Unified Communications Manager Administration retains your remote destination search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your remote destination search preferences until you modify your search or close the browser.

**Procedure**

- Step 1** In the menu bar, choose **Device > Remote Destination**.  
The Find and List Remote Destinations window displays. Records from an active (prior) query may also display in the window.
- Step 2** To find all records in the database, ensure the dialog box is empty; go to [Step 3](#).  
To filter or search records
  - From the first drop-down list box, choose a search parameter.
  - From the second drop-down list box, choose a search pattern.

- Specify the appropriate search text, if applicable.



---

**Note** To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the **Clear Filter** button to remove all added search criteria.

---

**Step 3** Click **Find**.

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.



---

**Note** You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking **Delete Selected**. You can delete all configurable records for this selection by clicking **Select All** and then clicking **Delete Selected**.

---

**Step 4** From the list of records that display, click the link for the record that you want to view.



---

**Note** To reverse the sort order, click the up or down arrow, if available, in the list header.

---

The window displays the item that you choose.

---

**Additional Information**

See the [“Related Topics”](#) section on page 13-49.

## Configuring Remote Destinations



---

**Note** End users can create their own remote destinations in the Cisco Unified CM User Options windows. For information on how to perform this task, refer to the user guide for the phone model.

---

To add configure a remote destination, perform the following procedure:

**Procedure**

---

**Step 1** In the menu bar, choose **Device > Remote Destination**.

The Remote Destination Configuration window displays.

**Step 2** Perform one of the following tasks:

- To copy an existing remote destination, locate the appropriate remote destination as described in the [“Finding Remote Destinations”](#) section on page 13-35. Click the **Copy** icon next to the remote destination that you want to copy. The window displays the copy of the remote destination. Change the value in the Name field and continue with [Step 3](#).
- To add a new remote destination, click the **Add New** button and continue with [Step 3](#).
- To update an existing remote destination, locate the appropriate remote destination as described in the [“Finding Remote Destinations”](#) section on page 13-35 and continue with [Step 3](#).

**Step 3** Enter the appropriate settings as described in [Table 13-8](#).



**Note** Be aware that the appropriate timer settings in [Table 13-8](#) may be vendor-specific. If difficulties in transferring calls by using the default timer settings occur, you may need to adjust the settings to be compatible with the vendor of the remote destination phone.

**Step 4** Check the Line Association check boxes for the desktop phones that will be used with this remote destination. You must perform this step for Mobile Connect to work.

**Step 5** Click **Save**.

---

#### Additional Information

See the [“Related Topics” section on page 13-49](#).

## Deleting Remote Destinations

To delete a remote destination in Cisco Unified Communications Manager Administration, perform the following procedure.

#### Before You Begin

You cannot delete remote destinations that other devices are using. To find out which items are using the remote destination, choose **Dependency Records** from the Related Links drop-down list box that is on the Remote Destination Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the [“Accessing Dependency Records” section on page A-2](#). If you try to delete a remote destination that is in use, Cisco Unified Communications Manager displays a message. Before deleting a remote destination that is currently in use, you must perform either or both of the following tasks:

- Assign a different remote destination to any devices that are using the remote destination that you want to delete.
- Delete the devices that are using the remote destination that you want to delete.

#### Procedure

---

**Step 1** In the menu bar, choose **Device > Remote Destination**.

The Remote Destination Configuration window displays.

**Step 2** Locate the remote destination that you want to update, as described in the [“Finding Remote Destinations” section on page 13-35](#).

**Step 3** After the Remote Destination window displays, click **Delete**.

**Step 4** To continue with the deletion, click **OK**.

---

#### Additional Information

See the [“Related Topics” section on page 13-49](#).

## Remote Destination Configuration Settings

Table 13-8 describes the available settings in the Remote Destination window.

**Table 13-8 Remote Destination Configuration Settings**

Field	Description
<b>Remote Destination Information</b>	
<b>Mobile Identity Information</b>	
Name	Enter a name that identifies the remote destination.
Destination Number	<p>Enter the telephone number for the destination. Include the area code and any additional digits that are required to obtain an outside line. Maximum field length equals 24 characters; individual characters can take the values 0-9, *, and #. Cisco recommends that you configure the caller ID of the remote destination.</p> <p><b>Note</b> Add the necessary translation pattern or route patterns to route the destination number.</p> <p>For the SIP URI feature, you can also enter a Universal Resource Indicator (URI) in this field, such as <i>user@corporation.com</i>, up to 126 characters in length. Keep in mind that a SIP route pattern must also be configured.</p>
Answer Too Soon Timer	<p>Enter the minimum time in milliseconds that must pass before the mobile phone can be answered.</p> <p>Range: 0 - 10,000 milliseconds</p> <p>Default: 1,500 milliseconds</p>
Answer Too Late Timer	<p>Enter the maximum time in milliseconds that can pass before the mobile phone must be answered.</p> <p>Range: 10,000 - 300,000 milliseconds</p> <p>Default: 19,000 milliseconds</p>
Delay Before Ringing Timer	<p>Enter the time that elapses before the mobile phone rings when a call is transferred from the desktop phone.</p> <p>Range: 0 - 30,000 milliseconds</p> <p>Default: 4,000 milliseconds</p>
Remote Destination Profile	From the drop-down list box, choose the remote destination profile that you want to use for this remote destination.
Cisco Unified Mobile Communicator	This field displays the Cisco Unified Mobile Communicator device with which this Mobility Identity associates. Click the Configure Device link to display the Phone Configuration window, where you can change the settings of the specified device.
Dual Mode Phone	This field displays a dual-mode phone with which this Mobility Identity associates. The field displays the device name. Click the Configure Device link to display the Phone Configuration window, where you can change the settings of the specified device.

**Table 13-8 Remote Destination Configuration Settings (continued)**

Field	Description
Mobile Phone	<p>Check the check box if you want calls that the desktop phone answers to be sent to your mobile phone as the remote destination.</p> <p><b>Note</b> You must check this check box for Mobile Connect to work with this remote destination.</p>
Enable Mobile Connect	Check the check box to allow an incoming call to ring your desktop phone and remote destination at the same time.
<b>When Mobile Connect Is Enabled</b>	
<b>Ring Schedule</b>	
All the time	If the Enable Mobile Connect check box is checked for this remote destination, clicking this radio button allows this remote destination to ring all the time. This setting works in conjunction with the setting in the <i>When receiving a call during the above ring schedule</i> pane below.
As specified below	If the Enable Mobile Connect check box is checked for this remote destination, clicking this radio button allows this remote destination to ring according to the schedule that the subsequent rows specify. This setting works in conjunction with the setting in the <i>When receiving a call during the above ring schedule</i> pane below.
(day of week)	<p>If the Enable Mobile Connect check box is checked and the As specified below radio button is selected, click the check box for each day of the week when the remote destination should receive calls. You can specify a ring schedule for each day of the week.</p> <p><b>(day of the week)</b>—Check the check box for a day of the week, such as Monday, to specify the ring schedule for that day.</p> <p><b>All Day</b>—Click this check box next to a day of the week to specify that the remote destination should ring at all hours of the day as specified by the setting in the <i>When receiving a call during the above ring schedule</i> pane below.</p> <p><b>(drop-down list box) to (drop-down list box)</b>—For a particular day of the week, specify a ring schedule by choosing a starting time and ending time for that day. Specify the starting time by choosing a value in the drop-down list box that precedes <b>to</b> and specify the ending time by choosing a value in the drop-down list box that follows <b>to</b>. For a particular day, the default ring schedule specifies <i>No Office Hours</i>. The values that you specify in the drop-down list boxes relate to the time zone that you specify in the <b>Time Zone</b> field for the remote destination.</p>
Time Zone	<p>From the drop-down list box, choose a time zone to use for this remote destination.</p> <p><b>Note</b> The time-of-day access feature uses the time zone that you choose for this remote destination to allow or block calls to this remote destination.</p>

**Table 13-8 Remote Destination Configuration Settings (continued)**

Field	Description
<b>When receiving a call during the above ring schedule</b>	
Always ring this destination	Click this radio button to cause incoming calls to always ring this remote destination according to the Ring Schedule that you specify. This setting applies only if the Enable Mobile Connect check box is checked for this remote destination.
Ring this destination only if caller is in	<p>Click this radio button to allow incoming calls to ring this remote destination only if the caller belongs to the access list that is specified in the drop-down list box and according to the Ring Schedule that you specify in the Ring Schedule pane. This setting applies only if the Enable Mobile Connect check box is checked for this remote destination.</p> <p>From the drop-down list box, choose an access list that applies to this setting. If you want to view the details of an access list, click the View Details link. (To modify an access list, you must use the <b>Call Routing &gt; Class of Control &gt; Access List</b> menu option.)</p> <p>Choosing an access list that contains no members equates to choosing to never ring this destination.</p>
Do not ring this destination if caller is in	<p>Click this radio button to prevent incoming calls from ringing this remote destination if the caller belongs to the access list that is specified in the drop-down list box and according to the Ring Schedule that you specify in the Ring Schedule pane. This setting applies only if the Enable Mobile Connect check box is checked for this remote destination.</p> <p>From the drop-down list box, choose an access list that applies to this setting. If you want to view the details of an access list, click the View Details link. (To modify an access list, you must use the <b>Call Routing &gt; Class of Control &gt; Access List</b> menu option.)</p> <p>Choosing an access list that contains no members equates to choosing the Always ring this destination radio button.</p>
<b>Association Information</b>	
Line	This entry displays a line that can associate with this remote destination.
Line Association	Check this check box if you want to associate a particular line with this remote destination.

**Additional Information**

See the [“Related Topics”](#) section on page 13-49.

## Mobile Voice Access Media Resource Configuration

Use the Mobile Voice Access window under Media Resources to assign sets of localized user prompts for Mobile Voice Access.

To assign localized users prompts for Mobile Voice Access, perform the following procedure:

#### Procedure

- 
- Step 1** In the menu bar, choose **Media Resources > Mobile Voice Access**.
- Step 2** Enter values for the parameters that are described in [Table 13-9](#).
- Step 3** Click **Save**.
- 

#### Additional Information

See the “[Related Topics](#)” section on page 13-49.

## Mobile Voice Access Configuration Settings

[Table 13-9](#) describes the available settings in the Mobile Voice Access window.

**Table 13-9** *Mobile Voice Access Configuration Settings*

Field	Description
<b>Mobile Voice Access Information</b>	
Mobile Voice Access Directory Number	Enter the internal DN to receive Mobile Voice Access calls from the gateway.
Mobile Voice Access Partition	From the drop-down list box, choose a partition for Mobile Voice Access. The combination of directory number and partition makes the Mobile Voice Access directory number unique.

**Table 13-9 Mobile Voice Access Configuration Settings (continued)**

Field	Description
<b>Mobile Voice Access Localization</b>	
Available Locales	<p>This pane displays the locales that have been configured. Refer to the Cisco Unified Communications Manager Locale Installer documentation for details.</p> <p>Use the Down Arrow key to move the locales that you select to the Selected Locales pane.</p> <p><b>Note</b> Cisco Unified Mobility supports a maximum of nine locales. If more than nine locales are installed for Cisco Unified Communications Manager, they will display in the Available Locales pane, but you can only save up to nine locales in the Selected Locales pane. If you attempt to configure more than nine locales for Cisco Unified Mobility, the following message displays: “Update failed. Check constraint (informix.cc_ivruserlocale_orderindex) failed.”</p>
Selected Locales	<p>Use the arrows above this pane to move the locales that you want to select to or from this pane.</p> <p><b>Note</b> Remember that you can select a maximum of nine locales, even if more locales are available in the system.</p> <p>Use the arrow keys to the right of this pane to reorder the locales that are listed in the pane. Choose a locale by clicking the locale name; then, use the arrow key to change the order of the chosen locale.</p> <p><b>Note</b> Mobile Voice Access uses the first locale that displays in the Selected Locales pane in the Mobile Voice Access window when the IVR is used. For example, if English United States displays first in the Selected Locales pane, the Cisco Unified Mobility user receives English when the IVR is used during a call.</p>

**Additional Information**

See the “[Related Topics](#)” section on page 13-49.

## H.323 Gateway Configuration for Mobile Voice Access

To configure H.323 gateways for Mobile Voice Access, you have two options available, depending on whether you are using PRI:

- [Configuring an H.323 Gateway for System Remote Access by Using PRI, page 13-43](#)
- [Configuring an H.323 Gateway for System Remote Access by Using Hairpinning, page 13-45](#)

**Additional Information**

See the “[Related Topics](#)” section on page 13-49.

## Configuring an H.323 Gateway for System Remote Access by Using PRI

If you already have an H.323 gateway that is configured in Cisco Unified Communications Manager, you can use it to support system remote access. If you do not have an H.323 gateway, you must add and configure one. For more information, refer to the “[Adding a Cisco IOS H.323 Gateway](#)” section in the *Cisco Unified Communications Manager Administration Guide*.

**Note**

When a Mobile Connect call is placed from an internal extension, the system presents only the internal extension as the caller ID. If an H.323 gateway is used, you can use translation patterns to address this issue.

To configure the gateway, follow these steps.

**Procedure**

**Step 1** Configure the T1/E1 controller for PRI from PSTN.

Sample configuration:

- controller T1 1/0
- framing esf
- linecode b8zs
- pri-group timeslots 1-24

**Step 2** Configure the serial interface for the PRI (T1/E1).

Sample configuration:

- interface Serial 1/0:23
- ip address none
- logging event link-status none
- isdn switch-type primary 4ess
- isdn incoming-voice voice
- isdn bchan-number-order ascending
- no cdp enable

**Step 3** Load the VXML application from the Cisco Unified Communications Manager server (Publisher).

Sample configuration for IOS Version 12.3 (13) and later:

- application service CCM
- <http://<Unified CM cluster Publisher IP Addr>:8080/ccmivr/pages/IVRMainpage.vxml>

Sample configuration before IOS Version 12.3(12):

- call application voice Unified CCM
- <http://<Unified CM cluster Publisher IP Addr>:8080/ccmivr/pages/IVRMainpage.vxml>

**Note**

Although VXML was added in Version 12.2(11), Versions 12.3(8), 12.3(9), 12.3(14)T1, and 12.2(15) have VXML issues, and you should not be use them.

**Step 4** Configure the dial-peer to associate Mobile Connect application with system remote access.

Sample configuration for IOS 12.3(13) and later:

- dial-peer voice 58888 pots
- service CCM (*Mobile Connect VXML application*)
- incoming called-number 58888
- no digit-strip

Sample configuration for IOS 12.3(12) and earlier:

- dial-peer voice 100 pots
- application CCM (*Mobile Connect VXML application*)
- incoming called-number 58888 (*where 58888 represents the Mobile Voice Access number*)
- no digit-strip

**Step 5** Add a dial-peer to transfer the calls to the Mobile Voice Access DN that is configured in the [“Mobile Voice Access Media Resource Configuration”](#) section on page 13-40.

Sample configuration for primary Cisco Unified Communications Manager:

- dial-peer voice 101 voip
- preference 1
- destination-pattern <Mobile Voice Access DN>




---

**Note** If a generic dial-peer is already configured to terminate the calls and is consistent with the Mobile Voice Access DN, you do not need to perform this step.

---

- session target ipv4:10.1.30.3
- codec g711ulaw
- dtmf-relay h245-alphanumeric
- no vad

Sample configuration for secondary Cisco Unified Communications Manager (if needed):

- dial-peer voice 102 voip
- preference 2
- destination-pattern <Mobile Voice Access DN>




---

**Note** If a generic dial-peer is already configured to terminate the calls and is consistent with the Mobile Voice Access DN, you do not need to perform this step.

---

- session target ipv4:10.1.30.4
  - codec g711ulaw
  - dtmf-relay h245-alphanumeric
  - no vad
-

**Additional Information**

See the “[Related Topics](#)” section on page 13-49.

## Configuring an H.323 Gateway for System Remote Access by Using Hairpinning

If you do not have an H.323 gateway, do not want to connect a separate PRI to H.323 gateway, and want to use a H.323 gateway only to support System Remote Access, you must add and configure one. For more information, refer to the “[Adding a Cisco IOS H.323 Gateway](#)” section in the *Cisco Unified Communications Manager Administration Guide*.

**Note**

When you are adding an H.323 gateway in Cisco Unified Communications Manager for hairpin configuration, you must check the Media Termination Point Required check box. If this check box is not checked, calls might not complete properly for most gateway images.

To configure the gateway, follow these steps.

**Procedure**

**Step 1** Load the VXML application from the Cisco Unified Communications Manager server (Publisher).

Sample configuration for IOS Version 12.3 (13) and later:

- application service CCM
- <http://<Unified CM cluster Publisher IP Addr>:8080/ccmivr/pages/IVRMainpage.vxml>

Sample configuration before IOS Version 12.3(12):

- call application voice CCM
- <http://<Unified CM cluster Publisher IP Addr>:8080/ccmivr/pages/IVRMainpage.vxml>



**Note** Although VXML was added in Version 12.2(11), Versions 12.3(8), 12.3(9), 12.3(14)T1, and 12.2(15) have VXML issues, and you should use them.

**Step 2** Configure the dial-peer to associate Mobile Connect application with system remote access.

Sample configuration for IOS 12.3(13) and later:

- dial-peer voice 1234567 voip
- service CCM
- incoming called-number 1234567
- codec g711u
- session target ipv4:<ip\_address of call manager>

Sample configuration for IOS 12.3(12) and earlier:

- dial-peer voice 1234567 voip
- application CCM
- incoming called-number 1234567
- codec g711u
- session target ipv4:<ip\_address of call manager>

**Step 3** Add a dial-peer for transferring calls to the Mobile Voice Access DN.

Sample configuration for primary Cisco Communications Manager:

- dial-peer voice 101 voip
- preference 1
- destination-pattern <Mobile Voice Access DN>




---

**Note** If a generic dial-peer is already configured to terminate the calls and is consistent with the Mobile Voice Access DN, you do not need to perform this step.

---

- session target ipv4:10.1.30.3
- voice-class h323 1
- codec g711ulaw
- dtmf-relay h245-alphanumeric
- no vad

Sample configuration for secondary Cisco Communications Manager (if needed):

- dial-peer voice 102 voip
- preference 2
- destination-pattern <Mobile Voice Access DN>




---

**Note** If a generic dial-peer is already configured to terminate the calls and is consistent with the Mobile Voice Access DN, you do not need to perform this step.

---

- session target ipv4:10.1.30.4
- voice-class h323 1
- codec g711ulaw
- dtmf-relay h245-alphanumeric
- no vad

**Step 4** Configure hairpin.

- voice service voip
  - allow-connections h323 to h323
- 

#### Additional Information

See the [“Related Topics”](#) section on page 13-49.

## Mobile Voice Access Configuration by Service Parameter

To configure Mobile Voice Access without using an H.323 gateway, use the following procedure.

### Procedure

- 
- Step 1** Choose **System > Service Parameters**.
- Step 2** For the Cisco CallManager service, set the following service parameters in the Clusterwide Parameters (System - Mobility) area:
- Set the Enable Enterprise Feature Access service parameter to **True**.
  - Set the Mobile Voice Access Number service parameter to the number that is configured in the H.323 gateway for this feature.
  - Set the Matching Caller ID for Remote Destination service parameter. Choose either *Complete Match* or *Partial Match*. If you choose *Partial Match*, proceed to set a value for the Number of Digits for Caller ID Partial Match service parameter.
  - If you set the Matching Caller ID for Remote Destination service parameter to *Partial Match*, set the Number of Digits for Caller ID Partial Match service parameter.
- Step 3** To save the service parameter settings, click **Save**.
- Step 4** Choose **Call Routing > Mobility Configuration**.
- Step 5** In the Mobility Configuration window, configure the Mobile Access DID by specifying a value in the Enterprise Feature Access Directory Number field that matches the value that you configured for the Mobile Voice Access Number service parameter.
- Step 6** Specify the partition by choosing a value for the Enterprise Feature Access Directory Number Partition.
- Step 7** To save the Mobility Configuration settings, click **Save**.
- 

When a caller calls the DID, Cisco Unified Communications Manager matches the calling number to the destination number that is configured in the Remote Destination Configuration window. In the scenario where Cisco Unified Communications Manager Administration prepends the digit 9 to get an outside line, the administrator can manipulate the quantity of digits of this number by modifying these service parameters in the Clusterwide Parameters (System - Mobility) section:

- Matching Caller ID with Remote Destination
- Number of Digits for Caller ID Partial Match

No IVR exists with this configuration, so callers do not receive a prompt.

Refer to the User Guide of the remote phone model for the steps that users perform to make outbound calls and to use Mobile Voice Access.

### Additional Information

See the [“Related Topics” section on page 13-49](#).

## Mobility Setting Configuration

To configure mobility settings for handoff of dual-mode phones between the Wi-Fi and Global System for Mobile communication (GSM) or Code Division Multiple Access (CDMA) networks, perform the following procedure.

### Procedure

- 
- Step 1** Choose **Call Routing > Mobility Configuration**.  
The Mobility Configuration window displays.
  - Step 2** Enter the appropriate settings as described in [Table 13-10](#).
  - Step 3** Click **Save**.
- 

### Additional Information

See the “[Related Topics](#)” section on page 13-49.

## Mobility Configuration Settings

[Table 13-10](#) describes the available settings in the Mobility Configuration window.

**Table 13-10** *Mobility Configuration Settings*

Field	Description
Handoff Number	Enter the DID number for handoff between the Wi-Fi and GSM or CDMA networks. The handoff feature requires this number.
Handoff Number Partition	From the drop-down list box, choose the partition to which the handoff direct inward dial (DID) belongs.
Enterprise Feature Access Directory Number	Enter the DID number that is required for enterprise feature access. This number supports transfer, conference, and resume and for two-stage dialing from smartphones. <b>Note</b> Ensure that each DID number is unique.
Enterprise Feature Access Directory Number Partition	From the drop-down list box, choose the partition of the DID that is required for enterprise feature access.

### Additional Information

See the “[Related Topics](#)” section on page 13-49.

## Mobility Softkey Configuration

To configure mobility handoff settings for dual-mode phones that are used for Mobile Connect, perform the following procedure:

### Procedure

---

- Step 1** Choose **Device > Device Settings > Softkey Template**.
- Step 2** To list the existing templates, click **Find**.
- Step 3** To create the new template, click **Standard User** and then click **Copy**.
- Step 4** Enter a name and description for the Softkey template and click **Save**.
- Step 5** Select **Configure Software Layout** from the Go next to Related Link menu in the upper, right corner of the window and click **Go**.
- Step 6** Select **On Hook** from the pull-down list box.
- Step 7** Add Mobility to the selected Softkeys and click **Save**.
- Step 8** Select **Connected** from the pull-down list box.
- Step 9** Add Mobility to the selected Softkeys and click **Save**.
- Step 10** Open the Phone Configuration window and associate the Softkey Template with the created Softkey template. See [Configuring Cisco Unified IP Phones](#) in the *Cisco Unified Communications Manager Administration Guide*.
- Step 11** Choose the Owner User ID for the Mobile Connect phone user.
- Step 12** Click **Save**.
- 

### Additional Information

See the “[Related Topics](#)” section on page 13-49.

## Related Topics

- [Introducing Cisco Unified Mobility, page 13-2](#)
- [Definitions, page 13-2](#)
- [List of Cisco Unified Mobility Features, page 13-3](#)
- [Other Benefits of Cisco Unified Mobility Features, page 13-4](#)
- [Mobile Connect, page 13-5](#)
- [Mobile Voice Access, page 13-5](#)
- [Cisco Unified Mobile Communicator, page 13-6](#)
- [Cisco Unified Mobile Communicator Configuration, page 13-7](#)
- [Cisco Unified Mobile Communicator Configuration Details, page 13-8](#)
- [Dial-via-Office Reverse Callback, page 13-9](#)
- [Time-of-Day Access, page 13-10](#)
- [Time-of-Day Access Configuration, page 13-11](#)
- [Important Notes for Time-of-Day Access, page 13-12](#)
- [Directed Call Park via DTMF, page 13-13](#)
- [SIP URI Dialing, page 13-14](#)

- [Use Case Scenarios for Cisco Unified Mobility Features](#), page 13-15
- [Interactions and Restrictions](#), page 13-18
- [Licensing](#), page 13-19
- [Number of Supported Calls](#), page 13-19
- [Auto Call Pickup](#), page 13-19
- [System Requirements](#), page 13-22
- [Migrating from Cisco Unified MobilityManager](#), page 13-22
- [Configuring Cisco Unified Mobility](#), page 13-22
- [Cisco Unified Mobility Configuration Checklist](#), page 13-23
- [Access List Configuration](#), page 13-24
- [Remote Destination Profile Configuration](#), page 13-29
- [Remote Destination Configuration](#), page 13-35
- [Mobile Voice Access Media Resource Configuration](#), page 13-40
- [H.323 Gateway Configuration for Mobile Voice Access](#), page 13-42
- [Mobile Voice Access Configuration by Service Parameter](#), page 13-47
- [Mobility Setting Configuration](#), page 13-48
- [Mobility Softkey Configuration](#), page 13-48
- [End User Configuration](#), *Cisco Unified Communications Manager Administration Guide*
- [Service Parameters Configuration](#), *Cisco Unified Communications Manager Administration Guide*
- [Licenses for Cisco Unified Mobility](#), *Cisco Unified Communications Manager System Guide*

**Additional Cisco Documentation**

- *Cisco Unified Serviceability Administration Guide*
- *Cisco Unified Communications Manager Security Guide*
- Applicable Cisco Unified IP Phone User Guides
- Applicable Cisco Unified IP Phone Administration Guides