CHAPTER 14

Cisco Unified Mobility

Cisco Unified Mobility extends the rich call control capabilities of Cisco Unified Communications Manager from the primary workplace desk phone of a mobile worker to any location or device of their choosing.

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 get redirected to the enterprise voice mailbox of the user (not to the mobile voice mailbox).

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.

See the user guide for a particular Cisco Unified IP 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.

Note For explanations and configuration of features that are related to Cisco Unified Mobility and that require additional configuration of Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator, see the "Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator Integration" chapter. The chapter also points to other documentation that explains configuration of Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator.

This chapter includes information on the following topics:

Configuration Checklist for Cisco Unified Mobility

Cisco Unified Mobility gives users the ability to redirect incoming IP calls from the Cisco Unified Communications Manager to up to ten different designated client devices such as mobile phones. For more information on Cisco Unified Mobility features, see the "List of Cisco Unified Mobility Features" section on page 14-6.

Table 14-1 summarizes the procedures for configuring Cisco Unified Mobility. For detailed instructions, see the chapters and sections that the table references. In addition, see the "Related Topics" section on page 14-62.

Table 14-1 Cisco Unified Mobility Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	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, See the *Cisco Unified Serviceability Administration Guide*.
Step 2	Configure user accounts. **Note** Make sure that you check the Enable Mobility check box and the Enable Mobile Voice Access check box in the End User Configuration window. **Note** Checking the Enable Mobility check box triggers User Connect License (UCL) to provide licensing for Mobile Connect.	End User Configuration, *Cisco Unified Communications Manager Administration Guide* For information on how licensing works with Mobile Connect, See "Licenses for Cisco Unified Mobility".
Step 3	Create access lists for Mobile Connect by assigning each list to the Mobile Connect user and specifying whether the list is an allowed or blocked list.	Access List Configuration, page 14-36.
Step 4	Create remote destination profiles and assign each user to a profile.	Remote Destination Profile Configuration, page 14-39.
Step 5	Associate desktop directory numbers (DNs) for the user.	Associating a Directory Number with a Remote Destination Profile, page 14-43.
Step 6	Add remote destinations by selecting the previously-defined profile as part of the configuration.	Remote Destination Configuration, page 14-43.
Step 7	In the Service Parameters Configuration window: • Choose **True** 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. **Note** 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. • Choose **True** for Enable Enterprise Feature Access to enable access to hold, resume, transfer, and conference features from remote destinations.	Service Parameter Configuration, *Cisco Unified Communications Manager Administration Guide*
Step 8	Configure the directory number for Mobile Voice Access.	Mobile Voice Access Directory Number Configuration, page 14-48.

Table 14-1 Cisco Unified Mobility Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 9	As an alternative, configure Enterprise Feature Access Two-Stage Dialing (also known as Enterprise Feature Access) by configuring a service parameter and the enterprise feature access DID directory number. **Note** Enterprise Feature Access provides the same functionality as Mobile Voice Access but does not support the IVR component. Also, Enterprise Feature Access does not require configuration of the H.323 gateway nor VXML.	Enterprise Feature Access Two-Stage Dialing, page 14-55
Step 10	Configure mobility settings for dual-mode phone handoff.	Handoff Mobility Configuration Settings, page 14-57.
Step 11	Configure a Mobility softkey for the phone user that uses Mobile Connect.	Mobility Softkey Configuration, page 14-61
Step 12	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.	Remote Destination Configuration, page 14-43.

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:

Additional Information

See the "Related Topics" section on page 14-62.

Definitions

Table 14-2 provides definitions of terms that are related to Cisco Unified Mobility.

Table 14-2 Definitions

Term	Definition
Access List	List that determines the phone numbers that the system can pass or block from being passed to remote destinations.
Session Handoff	Transfer of session/conversations such as voice, video, and meetings between various Unified Communications clients that associate with a single user. **Types of Session Handoff** Two-touch Session Handoff—In this type, no Unified Communications client proximity detection logic gets used; all devices under the same user ring and first one to accept gets the call.
Enterprise Feature Access	Feature that provides the ability for users to access midcall features (Hold, Resume, Transfer, Conference, Directed Call Park), two-stage dialing, and Mobile Connect activate and deactivate from a remote destination. With this method, the user does not get prompted for keypad entries and must be aware of the required key sequence.
Mobile Connect	Feature that allows users to answer incoming calls on the desk phone or at a remote destination and to pick up in-progress calls on the desk phone or at a remote destination without losing the connection.
Mobile Voice Access	Interactive voice response (IVR) system that is used to initiate two-stage dialed calls through the enterprise and to activate or deactivate Mobile Connect capabilities.
Remote Destination	Phones that are available for Mobile Connect answer and pickup and that can leverage Mobile Voice Access and Enterprise Feature Access for two-stage dialing. Remote destinations may include any of the following devices: • Single-mode mobile (cellular) phones • Smartphones • Dual-mode phones • Enterprise IP phones that are not in the same cluster as the desk phone • Home phone numbers in the PSTN.
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.
Toast	A pop-up indication that expects user input.

Additional Information

See the "Related Topics" section on page 14-62.

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 desk phone and the mobile phone. See the "Mobile Connect" section on page 14-8 for a detailed discussion.
- Desktop Call Pickup—Users can switch between desk 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. See the "Desktop Call Pickup" section on page 14-10 for a detailed discussion.
- Send Call to Mobile Phone(s)—Users access this feature on the IP phone via the Mobility softkey. The feature triggers a remote destination pickup, which allows the user to move an active mobility call from the user desk phone to a configured remote destination phone. See the "Send Call to Mobile Phone" section on page 14-10 for a detailed discussion.
- Mobile Voice Access—This feature extends Mobile Connect capabilities by providing an interactive voice response (IVR) system to initiate two-stage dialed calls through the enterprise and activate or deactivate Mobile Connect capabilities. See the "Mobile Voice Access" section on page 14-11 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 represents a mobile or other phone that can be configured to accept transfers from the desk phone for the user.

Cisco Unified Communications Manager supports the following Cisco Unified Mobility features:

- Midcall Enterprise Feature Access Support Using DTMF—You can configure DTMF feature codes as service parameters: enterprise hold (default equals *81), enterprise exclusive hold (default equals *82), resume (default equals *83), transfer (default equal *84), and conference (default equals *85). See the "Midcall Enterprise Feature Access Support Using DTMF" section on page 14-12 for a detailed discussion.

  Note *81 specifies enterprise hold. When invoked, enterprise hold allows the user to resume the call on the desk phone. *82 specifies enterprise exclusive hold. When invoked, enterprise exclusive hold does not provide the ability to resume the call on the desk phone. If a mobility call that is on enterprise hold disconnects in this state, the user can resume the call on the desk phone. Alternatively, if a mobility call that is on enterprise exclusive hold disconnects in this state, the user cannot resume the call on the desk phone.

- 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. See the "Two-Stage Dialing" section on page 14-12 for a detailed discussion.

- 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.
- 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. See the "Time-of-Day Access" section on page 14-12 for a detailed discussion.
- Directed Call Park via DTMF—This feature allows a mobile phone user to park a call by transferring the parked 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. Support of the Directed Call Park via DTMF feature leverages the Midcall Enterprise Transfer feature. See the "Directed Call Park via DTMF" section on page 14-15 for a detailed discussion.
- SIP URI Dialing—This feature supports SIP URI as an additional type of remote destination for Cisco Unified Mobility. See the "SIP URI Dialing" section on page 14-16 for a detailed discussion.
- Intelligent Session Control—This feature modifies the behavior of outgoing calls placed from the enterprise directly to mobile phones and anchors such calls to the user desktop number. (Prior to the implementation of this feature, if an enterprise user made a direct call to a mobile phone, the call was treated like a normal outgoing PSTN call: the call got directed to the mobile phone only, the call was not anchored to the user desk phone, and the mobile user could not invoke any mobility features.) During such calls, the user can invoke mobility features such as midcall features and Session Handoff from the user mobile phone. See the "Intelligent Session Control" section on page 14-17 for a detailed discussion.
- Session Handoff—This feature leverages the existing Cisco Unified Communications Manager experience by allowing the user to move voice, video, and meeting sessions and conversations between different Unified Communications clients, such as Cisco Unified Personal Communicator (running on a PC in Softphone as well as CTI control mode), Cisco Unified Mobile Communicator (running on a mobile phone), and Cisco Unified IP Phone Series 9900 and legacy phones that are running SIP.

  The conversation can be moved from mobile phone to any other Unified Communications client. All devices that the user owns and that share the same line ring or show a toast, and the call gets answered by whichever device picks it up first. Upon answer, all the other shared-line devices enter Remote in Use mode. See the "Session Handoff" section on page 14-19 for a detailed discussion.

  Note that the only client that can actually hand off a session (because it is the only client that has an anchored DTMF path back to Cisco Unified Communications Manager) is Cisco Unified Mobile Communicator. Neither Cisco Unified Personal Communicator nor 9900 series Cisco Unified IP Phones can initiate a session handoff. These devices can, however, handle an incoming session handoff.

Additional Information

See the "Related Topics" section on page 14-62.

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—User can turn Mobile Connect feature. See "Methods for Enabling and Disabling Mobile Connect" section on page 14-8 for details.
- 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.

Additional Information

See the "Related Topics" section on page 14-62.

Mobile Connect

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

Note You can use any mobile phone, 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 "Remote Destination Configuration" section on page 14-43.

Methods for Enabling and Disabling Mobile Connect

The following methods are available for enabling and disabling the Mobile Connect feature. This list provides the methods that are available to the administrator and to end users.

- Cisco Unified Communications Manager Administration windows. Menu path specifies **Device > Phone**, then configure the Mobility Identity of the Cisco Unified Mobile Communicator by checking the Enable Mobile Connect check box (to enable Mobile Connect) or by unchecking this check box (to disable Mobile Connect).
- Cisco Unified CM User Options windows: URL specifies http://<Unified CM IP address>/ccmuser. Within the application, specify the **User Options > Mobility Settings > Remote Destinations > Enable Mobile Connect** menu path.
- Desk phone by using the Mobility softkey. To configure, use these menu options:
  - **Device > Phone**, and specify the Mobility softkey template in the Softkey Template field.
  - **Device > Phone**, and assign the same mobility user ID on the remote destination profile as the desk phone owner user ID.

- Mobile phone by using Mobile Voice Access (uses IVR prompts; **2** to enable or **3** to disable)
- Mobile phone by using Enterprise Feature Access (after PIN entry, **2** to enable or **3** to disable). The sequence specifies <PIN>#2# or <PIN>#3#.
- Cisco Unified Mobile Communicator client: The client offers the mobile user the option to change the user Mobile Connect status. See "Enable/Disable Mobile Connect From Mobile Phone" section on page 16-6 for details.

Mobile Connect Status

If at least one configured remote destination for a user is enabled for Mobile Connect, the user desk phone displays Mobile Connect as Enabled.

RDNIS/Diversion Header

The RDNIS/diversion header for Mobile Connect enhances this Cisco Unified Mobility feature to include the RDNIS or diversion header information on the forked call to the mobile device. Service providers and customers use the RDNIS for correct billing of end users who make Cisco Unified Mobility Mobile Connect calls.

For Mobile Connect calls, the Service Providers use the RDNIS/diversion header to authorize and allow calls to originate from the enterprise, even if the caller ID does not belong to the enterprise Direct Inward Dial (DID) range.

Example RDNIS/Diversion Header Use Case

Consider a user that has the following setup:

Desk phone number specifies 89012345.

Enterprise number specifies 4089012345.

Remote destination number specifies 4088810001.

User gets a call on desk phone number (89012345) that causes the remote destination (4088810001) to ring as well.

If the user gets a call from a nonenterprise number (5101234567) on the enterprise number (4089012345), the user desk phone (89012345) rings, and the call gets extended to the remote destination (4088810001) as well.

Prior to the implementation of the RDNIS/diversion header capability, the fields populated as follows:

Calling Party Number (From header in case of SIP): 5101234567

Called Party Number (To header in case of SIP): 4088810001

After implementation of the RDNIS/diversion header capability, the Calling Party Number and Called Party Number fields populate as before, but the following additional field gets populated as specified:

Redirect Party Number (Diversion Header in case of SIP): 4089012345

Thus, the RDNIS/diversion header specifies the enterprise number that is associated with the remote destination.

Configuration of RDNIS/Diversion Header in Cisco Unified Communications Manager Administration

To enable the RDNIS/diversion header capability for Mobile Connect calls, ensure the following configuration takes place in Cisco Unified Communications Manager Administration:

All gateways and trunks must specify that the **Redirecting Number IE Delivery — Outbound** check box gets checked.

In Cisco Unified Communications Manager Administration, you can find this check box by following the following menu paths:

- For H.323 and MGCP gateways, execute **Device > Gateway** and find the gateway that you need to configure. In the Call Routing Information - Outbound calls pane, ensure that the **Redirecting Number IE Delivery - Outbound** check box gets checked. For T1/E1 gateways, check the **Redirecting Number IE Delivery - Outbound** check box in the PRI Protocol Type Information pane.
- For SIP trunks, execute **Device > Trunk** and find the SIP trunk that you need to configure. In the Outbound Calls pane, ensure that the **Redirecting Diversion Header Delivery - Outbound** check box gets checked.

Use Case Scenarios for Mobile Connect

See the "Use Case Scenarios for Mobile Connect" section on page 14-21 for the use case scenarios that Cisco Unified Communications Manager supports with this feature.

Additional Information

See the "Related Topics" section on page 14-62.

Desktop Call Pickup

User can perform desktop call pickup on in-progress mobility calls either by hanging up the call on the mobile phone or by putting the mobility call on hold with the midcall hold feature. When hanging up or ending the call at the mobile phone, the user can then resume the call on the desk phone within 10 seconds (default). When the remote destination hangs up, Cisco Unified Communications Manager puts the associated desk phone in Hold state, which allows the user to resume the call by pressing the Resume softkey. The Maximum Wait Time for Desk Pickup setting on the End User Configuration window determines the amount of time the call remains on hold after the hang-up at the remote destination. The default specifies 10000 milliseconds (10 seconds).

Alternatively, the user can also perform desktop call pickup by placing the call on the mobile phone on enterprise hold with the midcall hold feature (*81) and then resuming the call on the desk phone. When Cisco Unified Communications Manager receives the *81, Cisco Unified Communications Manager places the associated desk phone in a Hold state so the user can resume the call. Note that with this method, the Maximum Wait Time for Desk Pickup timer does not apply to the hold state and the call gets held indefinitely until the user resumes the call.

Additional Information

See the "Related Topics" section on page 14-62.

Send Call to Mobile Phone

User can perform remote destination pickup on in-progress mobility calls by using the Send Call to Mobile Phone feature. To do so, the user presses the Mobility softkey on the desk phone and selects Send Call to Mobile Phone, which generates calls to all of the remote destinations that are configured for the user. The user can then answer this call at the desired remote destination and continue the call.

When a desk phone invokes the Send Call to Mobile Phone feature and the remote destination specifies a dual-mode smartphone, the following behavior results:

- If the dual-mode smartphone is registered to Wi-Fi, the call gets sent to the device Wi-Fi side.

- If the dual-mode smartphone is not registered to Wi-Fi, the call gets sent to the device cellular side.

Additional Information

See the "Related Topics" section on page 14-62.

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 desk phone. A remote destination represents a phone that is designated as available for Mobile Connect answer 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 dialing methods that would be available if the user originated the call from the enterprise desk 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 gets configured in hairpin mode. (When Mobile Voice Access that is configured in hairpin mode is used, users who are calling the system do not get identified automatically by their caller ID. Instead, users must manually enter their remote destination number prior to entering their PIN number.)

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 can disconnect, and the system will lock out the user for a period of time. (The credential information for the user controls the allowed number of login attempts.)

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.

See the "Use Case Scenarios for Mobile Voice Access" section on page 14-22 for the use case scenarios that Cisco Unified Communications Manager supports with this feature.

Additional Information

See the "Related Topics" section on page 14-62.

Midcall Enterprise Feature Access Support Using DTMF

Users can leverage enterprise media resources and capabilities by invoking midcall features. DTMF digits that are relayed from the remote destination in-band in the audio path and then relayed out-of-band from the enterprise gateway to Cisco Unified Communications Manager invoke midcall features. When Cisco Unified Communications Manager receives the DTMF digits, appropriate midcall features get facilitated based on the DTMF digit sequence. Such features include adding or remove call legs for transferred or conferenced calls, as well as invoking media resources like music on hold for held calls and conference bridges as required.

The feature access codes that are configured within Cisco Unified Communications Manager under Service Parameters determine the midcall feature DTMF code sequences.

Additional Information

See the "Related Topics" section on page 14-62.

Two-Stage Dialing

The user can originate calls from the remote destination phone through the enterprise by leveraging the enterprise telephony infrastructure. Two-stage dialing provides the following benefits:

- The ability to make calls through the enterprise, which leads to centralized billing and call detail records. This ability provides the potential for cost savings by ensuring that international calls get billed to the enterprise rather than to the mobile or cellular plan. However, this capability does not eliminate normal per-minute local/long-distance charges at the mobile phone.
- The ability to mask the mobile phone number from the far-end or dialed phone. Instead of sending the mobile number to the called party, the user enterprise number gets sent to the called party during a two-stage dialed call. This method effectively masks the user mobile number and ensures that returned calls get anchored in the enterprise.

Additional Information

See the "Related Topics" section on page 14-62.

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).

Further Topics

This section includes the following topics:

- Time-of-Day Access Configuration, page 14-13
- Important Notes for Time-of-Day Access, page 14-14

The "Use Case Scenarios for Time-of-Day Access" section on page 14-22 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) or later.

Additional Information

See the "Related Topics" section on page 14-62.

Time-of-Day Access Configuration

Table 14-3 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 14-3 Time-of-Day Access Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	In Cisco Unified Communications Manager Administration, configure an end user for whom you will enable the Time-of-Day Access feature. Use the **User Management > End User** menu option. **Note** Make sure that you check the Enable Mobility check box in the End User Configuration window. **Note** Checking the Enable Mobility check box triggers licensing to consume device license units (DLUs) for Mobile Connect.	End User Configuration, *Cisco Unified Communications Manager Administration Guide* For information on how licensing works with Mobile Connect, see the "Licenses for Cisco Unified Mobility" section in the *Cisco Unified Communications Manager Features and Services Guide*.
Step 2	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. **Note** An access list must have an owner. No system access list exists. Use the **Call Routing > Class of Control > Access List** menu option.	Access List Configuration, page 14-36
Step 3	Create remote destination profiles and assign each user to a profile.	Remote Destination Profile Configuration, page 14-39.

Table 14-3 Time-of-Day Access Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 4	Configure a remote destination for a user. Remote destinations represent the mobile (or other) phones that can accept Mobile Connect calls and calls that are moved from the desk phone. Remote destinations can initiate calls by using Mobile Voice Access. Use the **Device > Remote Destination** menu option. **Note** The same configuration also applies to dual-mode phones and to Cisco Unified Mobile Communicator Mobility Identity to set up time-of-day access. For successful time-of-day access configuration, you must configure the following areas in the Remote Destination Configuration window: • Use the Ring Schedule pane to configure a ring schedule for the remote destination. • Use the *When receiving a call during the above ring schedule* pane to specify the access list for which the Ring Schedule applies. 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.	Remote Destination Configuration, page 14-43

Additional Information

See the "Related Topics" section on page 14-62.

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.

See the "Use Case Scenarios for Time-of-Day Access" section on page 14-22 for the use case scenarios that Cisco Unified Communications Manager supports with this feature.

See 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 14-62.

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, the user can park the call by transferring the parked party to the park code that the system administrator configures and assigns to the user. 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 enterprise exclusive 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 exclusive 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 Feature Access DID.

Note This same DID gets used for the Enterprise Feature Access two-stage dialing feature. Configure this DID with the **Call Routing > Mobility > Enterprise Feature Access Configuration** menu option.

4. After the call connects, dial the following field-and-digit sequence: <PIN>#*84#<Park Code>#*84#

   For example, if the PIN specifies 12345 and park code specifies 3215, the digit sequence would be 12345#*84#3215#*84#

Cisco Unified Communications Manager puts the parked party on hold.

Note The caller ID of the mobile phone must get passed to the enterprise and must match a configured remote destination when the user dials the Enterprise Feature Access DID to invoke this feature. If no caller ID exists or no caller ID match occurs, the user cannot invoke this 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 parking 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 parking party on hold with music on hold (MOH) or tone on hold. The last *84 completes the transfer of the parked party to the Cisco Unified Communications Manager generic device that associates with the selected park code. After the transfer completes, the parked party receives the MOH or tone on hold, and the parked party gets parked on this selected park code and waits for retrieval.

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

If the user-specified park code is not valid, Cisco Unified Communications Manager plays reorder tone to the parking party.

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, dial the following field-and-digit sequence to retrieve the parked call:

   <PIN>#1#<Retrieval Prefix><Park Number>#

   In our example, the full sequence specifies 12345#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 parking party by default.

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

See the "Use Case Scenarios for Directed Call Park via DTMF" section on page 14-23 for the use case scenarios that Cisco Unified Communications Manager supports with this feature.

Additional Information

See the "Related Topics" section on page 14-62.

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 14-62.

Intelligent Session Control

This feature modifies the behavior of outgoing calls placed from the enterprise directly to mobile phones and anchors such calls to the user desktop number. (Prior to the implementation of this feature, if an enterprise user made a direct call to a mobile phone, the call was treated like a normal outgoing PSTN call: the call got directed to the mobile phone only and the mobile user could not invoke any mobility features.)

An outgoing call from the enterprise to a remote destination exhibits the following behavior:

- Mobile user can use DTMF to invoke midcall features, such as Hold, Resume, Transfer, and Conference.
- Mobile user can hang up the call from the mobile phone and pick the call up from the user desk phone.
- A direct call to a remote destination from the enterprise gets anchored to the user desk phone; and the time-of-day access, Do Not Disturb, and Delay Before Ringing settings that are configured in the associated remote destination profile get ignored. The direct call goes immediately to the mobile user.
- Direct calls to remote destinations behave similarly to calls incoming to Cisco Unified Communications Manager from mobile users. Mobile users have access to the following mobility features:
  - Midcall features (Hold, Resume, Transfer, Conference)
  - Session Handoff
  - Call anchoring

Feature Configuration

Basic configuration of the Intelligent Session Control feature requires that the administrator configure the value of the Reroute Remote Destination Calls to Enterprise Number service parameter as True.

To access the service parameters in question, execute **System > Service Parameters** in Cisco Unified Communications Manager Administration**.** In the Service Parameter Configuration window that displays, specify a server and the Cisco CallManager service. The following service parameters are found in the Clusterwide Parameters (Feature - Reroute Remote Destination Calls to Enterprise Number) pane:

- Reroute Remote Destination Calls to Enterprise Number—To enable the feature, specify the value for this service parameter as True. When this parameter is enabled, all outgoing calls to a remote destination get anchored in the enterprise number with which the remote destination associates.
- Log Mobile Number in CDR for Rerouted RD Calls—This service parameter determines whether to log the mobile number or the enterprise number in the call detail record (CDR) when outgoing calls to the remote destination get anchored. If set to False, the enterprise number gets logged. If set to True, the mobile number gets logged.
- Ignore Call Forward All on Enterprise DN—This service parameter determines whether to ignore the call forward all (CFA) setting that is configured on the enterprise number when outgoing calls to the remote destination get anchored. If set to True, the CFA gets ignored; if set to False, the CFA setting gets applied.

The following service parameters, found in the Clusterwide Parameters (System - Mobility) pane, also affect the behavior of the Intelligent Session Control feature:

- Matching Caller ID with Remote Destination—If this service parameter is set to Complete Match, all digits of the calling number must match for the call to connect to the remote destination. If this service parameter is set to Partial Match, partial matches are allowed and the Number of Digits for Caller ID Partial Match service parameter applies.
- Number of Digits for Caller ID Partial Match—The number of digits that this service parameter specifies applies to partial matches if the Matching Caller ID with Remote Destination service parameter is set to Partial Match.

Note For each service parameter, click the service parameter name in Cisco Unified Communications Manager Administration for a complete definition of that service parameter.

Further Topics

This section includes the following topics:

- Additional Call Processing Details for Intelligent Session Control, page 14-18
- Use Case Scenarios for Intelligent Session Control, page 14-24
- Troubleshooting the Intelligent Session Control Feature, page 14-19

The "Use Case Scenarios for Intelligent Session Control" section on page 14-24 provides use case scenarios for the Intelligent Session Control feature with Cisco Unified Mobility.

Additional Call Processing Details for Intelligent Session Control

If more than one line is configured for the matching remote destination profile for the dialed number, Cisco Unified Communications Manager uses the first matched line to route the call. Because the direct call to mobile number gets matched against the enterprise number, all enterprise number intercepts are honored, including Call Intercept on enterprise number when Call Intercept gets supported for enterprise number. The forward all intercept on enterprise number gets ignored based on the service parameter,

Ignore Forward All on Enterprise DN. If this service parameter is set to true, Cisco Unified Communications Manager ignores forward all intercept on enterprise number and still directs the call to the mobile phone. If this service parameter is set to false, Cisco Unified Communications Manager still enables CFA setting on enterprise number and, if configured, sends the call to CFA destination.

This feature does not anchor direct calls to mobile number if the call to mobile number gets sent via an overlap-sending-enabled trunk or gateway. In this case, the call to mobile number does not get anchored.

See the "Limitations" section on page 14-30 for additional restrictions that apply to this feature.

Troubleshooting the Intelligent Session Control Feature

Perform the following checks if the Intelligent Session Control feature does not function as expected:

- Ensure that the Intelligent Session Control is set to True in the Service Parameter Configuration window.
- Ensure that the caller ID matches the remote destination number as specified by the Matching Caller ID with Remote Destination setting (either complete match or partial match).
- Ensure that a trace line such as the following prints in the Cisco Unified Communications Manager SSI log after the number gets dialed:

  10/14/2008 15:09:26.507 CCM|Digit analysis: getDaRes - Remote Destination [**9725782583**]|*^*^*
- Ensure that the enterprise number Line Association check box is checked in the Remote Destination Configuration window (**Device > Remote Destination**).
- Ensure that the route pattern partition is part of the calling search space (CSS) that is configured as Rerouting CSS in the Remote Destination Profile Configuration window (**Device > Device Settings > Remote Destination Profile**).

Additional Information

See the "Related Topics" section on page 14-62.

Session Handoff

The complete Session Handoff feature can move a single call, a conference, and session collaboration among mobile phone, PC, and desk phone. Session Handoff enables a user to move conversations from user mobile phone to user desk phone. Two-touch Session Handoff uses two user inputs: one at the initiating party to hand off and the other at the terminating party to accept.

The major benefit of the Session Handoff feature over Desktop Pickup is that the original conversation can be continued until the handed off call gets answered.

Configuration of Session Handoff Feature

Configuration of the Session Handoff feature entails configuration of specific service parameters and configuration of the mobile device that will hand off calls. See the following topics:

- Session Handoff Service Parameters, page 14-20
- Mobility Device Configuration for Session Handoff Feature, page 14-20

Session Handoff Service Parameters

To configure service parameters in Cisco Unified Communications Manager Administration, choose the **System > Service Parameters** menu option. From the Server drop-down list box, choose a server. From the Service drop-down list box, choose the Cisco CallManager service.

The following service parameters must be configured to enable the Session Handoff feature:

- Session Handoff Alerting Timer—This service parameter, found in the Clusterwide Parameters (Device - General) pane, determines the length of time that the session handoff call alerts. The default value specifies 10 seconds, and valid values range from 1 to 999 seconds.
- Enterprise Feature Access Code for Session Handoff—This service parameter, found in the Clusterwide Parameters (System - Mobility) pane, specifies the DTMF feature code to trigger session handoff. The default value specifies *74.

For additional details about these service parameters, click the name of the service parameter in the Service Parameter Configuration window in Cisco Unified Communications Manager Administration, which provides a hyperlink to a complete definition of the service parameter.

Mobility Device Configuration for Session Handoff Feature

Perform the following configuration for the mobility device to enable the Session Handoff feature:

- Configure the directory number in remote destination profile and the desk phone shared line so that line-level directory number and partition match.
- Assign the same mobility user ID on the remote destination profile as the desk phone owner user ID to allow session handoff.
- To configure the Session Handoff feature for basic Cisco Unified Mobility users, the User ID field setting in the Remote Destination Configuration window should match the Owner User ID field on the (desk) phone configuration window.
- To configure the Session Handoff feature for Cisco Unified Mobile Communicator users, both the Owner User ID and the Mobility User ID fields in the Cisco Unified Mobile Communicator device configuration window must match the Owner User ID field on the desk phone configuration window.

Impact of Session Handoff on Other Features

When the user hands off a call, a new call gets presented on the desk phone. While the desk phone is flashing, the following features do not get triggered on the desk phone for the call that was handed off:

- iDivert
- Call Forward All
- DND
- Call Forwarding

If the user hands off a call and does not answer from the desk phone within the time that the Session Handoff Alerting Timer service parameter specifies, the existing Remote In Use state on the desk phone gets lost.

Thus, the desk phone loses shared-line functionality following session handoff. The user cannot perform midcall features for that call, such as Hold from Mobile (using *81) and Resume from desk, or desk pickup. The user can hand off the call again, however, to resume it from the desk phone.

Additional Topics for Session Handoff

See the following section for other topics that apply to the Session Handoff feature:

- Session Handoff Feature, page 14-34
- Use Case Scenarios for Session Handoff, page 14-26

Troubleshooting Information for Session Handoff Feature

If a call that is handed off from a mobile phone does not flash the desk phone, perform the following checks:

- Check whether Owner User ID for the desk phone matches the User ID of Remote Destination Profile.
- In service parameters, check whether Enable Enterprise Feature Access is set to True; also, check whether other DTMF features (Hold [*81], Resume [*83]) are working.
- Check the Session Handoff DTMF code (default specifies *74) and Session Handoff Alerting Timer (default specifies 10 seconds) values.

Additional Information

See the "Related Topics" section on page 14-62.

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 14-21
- Use Case Scenarios for Mobile Voice Access, page 14-22
- Use Case Scenarios for Time-of-Day Access, page 14-22
- Use Case Scenarios for Directed Call Park via DTMF, page 14-23
- Use Case Scenarios for Intelligent Session Control, page 14-24
- Use Case Scenarios for Session Handoff, page 14-26

Additional Information

See the "Related Topics" section on page 14-62.

Use Case Scenarios for Mobile Connect

Mobile Connect supports these use case scenarios:

- Receiving an outside call on desk phone or mobile phone—An outside caller dials the user desktop extension. The desk phone and mobile phone ring simultaneously. When the user answers one phone, the other phone stops ringing. The user can switch from the desk 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 desk phone—If a call was initiated to or from the desk phone and then shifted to the mobile phone, the call can get shifted back to the desk phone.
- Using midcall enterprise features—During a Mobile Connect call, users can perform midcall functions, including hold/resume, exclusive hold, transfer, directed call park, and conference.

Additional Information

See the "Related Topics" section on page 14-62.

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 desk phone.
- Moving from a mobile phone to a desk 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 desk phone during the call without losing the connection and can shift back again as needed.

Additional Information

See the "Related Topics" section on page 14-62.

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; the use case scenarios also cover 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 Do not ring this destination if 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 14-62.

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.
- Parked party disconnects while the parking party attempts to park the call.
- Parked 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 the length of the string 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 14-62.

Use Case Scenarios for Intelligent Session Control

The Intelligent Session Control feature supports these use case scenarios:

- The Reroute Remote Destination Calls to Enterprise Number service parameter is set to False.
- The Reroute Remote Destination Calls to Enterprise Number service parameter is set to True.
- The Ignore Call Forward All on Enterprise DN service parameter is set to False.

The following sections discuss the configuration that takes place in order to demonstrate each user case for the Intelligent Session Control feature.

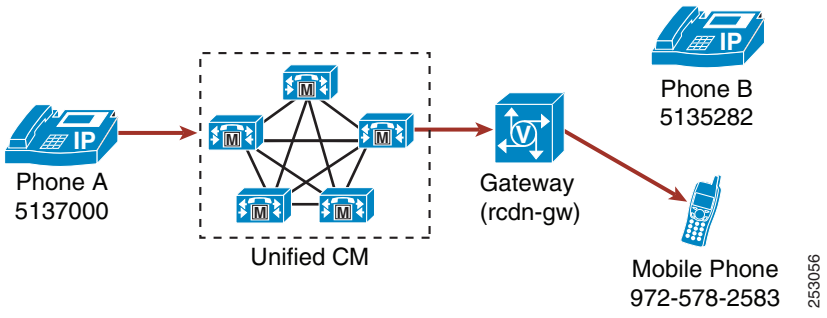
Use Case 1: Reroute Remote Destination Calls to Enterprise Number service parameter is set to False

In this use case, the following configuration takes place prior to the placement of the direct call from Cisco Unified Communications Manager to the remote destination:

1. Reroute Remote Destination Calls to Enterprise Number service parameter is set to False.
2. Number of Digits for Caller ID Partial Match service parameter specifies 7 digits for partial match.
3. Phone A DN specifies 5137000.
4. Phone B DN specifies 5135282 with owner user ID gbuser1 and remote destination (RD) specifies 9725782583.
5. Route pattern 9.XXXXXXXXXX with DDI as PreDot.
6. Route pattern points to the rcdn-gw gateway.

Figure 14-1 illustrates the setup for the direct call to the remote destination when the Reroute Remote Destination Calls to Enterprise Number service parameter is set to False.

Figure 14-1 Use Case 1: Reroute Remote Destination Calls to Enterprise Number Service Parameter Is Set to False



The following action initiates the feature behavior in this use case:

- Phone A DN 5137000 user calls the mobile phone by dialing 05782583.

The following call processing takes place:

1. The translation pattern gets matched and the called number gets transformed to 99725782583.
2. The route pattern 9.XXXXXXXXXX gets matched.

3. After the route pattern removes the leading (PreDot) 9, the number specifies 9725782583.
4. No remote destination mapping to enterprise number occurs.
5. The call extends only to the mobile user via the gateway: the call does not get anchored at the enterprise number with which this remote destination associates.

Use Case 2: Reroute Remote Destination Calls to Enterprise Number service parameter is set to True

In this use case, the following configuration takes place prior to the placement of the direct call from Cisco Unified Communications Manager to the remote destination:

1. Reroute Remote Destination Calls to Enterprise Number service parameter is set to True.
2. Number of Digits for Caller ID Partial Match service parameter specifies 7 digits for partial match.
3. Phone A DN specifies 5137000.
4. Phone B DN specifies 5135282 with owner user ID gbuser1 and remote destination (RD) specifies 9725782583.
5. Route pattern 9.XXXXXXXXXX with DDI as PreDot.
6. Translation pattern 0.XXXXXXX with DDI as PreDot and prefix digits specify 9972.
7. Route pattern points to the rcdn-gw gateway.

The following action initiates the feature behavior in this use case:

- Phone A DN 5137000 user calls the mobile phone by dialing 05782583.

The following call processing takes place:

1. The translation pattern gets matched and the called number gets transformed to 99725782583.
2. The route pattern 9.XXXXXXXXXX gets matched.
3. After the route pattern removes the leading (PreDot) 9, the number specifies 9725782583.
4. Remote destination mapping to enterprise number matches the configured remote destination for phone B.
5. The call gets anchored at the enterprise number of the called user and the call extends to the user remote destination.
6. Phone B enters Remote In Use (RIU) state after the mobile user answers the call.

Use Case 3: Ignore Call Forward All on Enterprise DN service parameter is set to False

In this use case, the following configuration takes place prior to the placement of the direct call from Cisco Unified Communications Manager to the remote destination:

1. Reroute Remote Destination Calls to Enterprise Number service parameter is set to True.
2. Ignore Call Forward All on Enterprise DN service parameter is set to False.
3. Number of Digits for Caller ID Partial Match service parameter specifies 7 digits for partial match.
4. Phone A DN specifies 5137000.
5. Phone B DN specifies 5135282 with owner user ID gbuser1 and remote destination (RD) specifies 9725782583. Call Forward All setting for phone B specifies forwarding to phone C with DN 5138000.
6. Route pattern 9.XXXXXXXXXX with DDI as PreDot.
7. Translation pattern 0.XXXXXXX with DDI as PreDot and prefix digits specify 9972.
8. Route pattern points to the rcdn-gw gateway.

The following action initiates the feature behavior in this use case:

- Phone A DN 5137000 user calls the mobile phone by dialing 05782583.

The following call processing takes place:

1. The translation pattern gets matched and the called number gets transformed to 99725782583.
2. The route pattern 9.XXXXXXXXXX gets matched.
3. After transformation, the number specifies 9725782583.
4. Remote destination mapping to enterprise number matches the configured remote destination for phone B.
5. The call gets redirected to the enterprise number of the user and goes to phone B instead of to the mobile phone.
6. Because of the setting of the Ignore Call Forward All on Enterprise DN service parameter to False, the call gets forwarded from phone B to phone C.

Additional Information

See the "Related Topics" section on page 14-62.

Use Case Scenarios for Session Handoff

The Session Handoff feature supports the following use case scenarios:

- Session Handoff using DTMF Tones (*74)
- Session Handoff using Move Softkey Event
- Session Handoff using VoIP Mode
- Session Handoff Fails or User Cancels Session Handoff

Session Handoff Using DTMF Tones (*74)

For session handoff using DTMF tones (default specifies *74), the following sequence of events takes place:

1. User A calls user B desk phone. Using the Single Number Reach feature, user B answers the call on mobile phone and his desk phone goes into Remote In Use state.
2. User B presses *74 (Session Handoff DTMF code). User B desk phone (a supported phone that is running SCCP or SIP) flashes. User B still talks with user A from user B mobile phone.
3. To move conversation to the desk phone, user B must answer the call from desk phone before the Session Handoff Alerting Timer service parameter (default 10s) expires. After the timer expires, the desk phone stops flashing. User B can still continue conversation from the mobile phone.

Session Handoff Using Move Softkey Event

For session handoff using the Move softkey event, the following sequence of events takes place:

1. Session Handoff gets triggered by using a Move softkey event message that gets embedded inside the SIP REFER message.
2. When Cisco Unified Communications Manager receives the REFER message, Cisco Unified Communications Manager triggers session handoff.

Note If user mobile device disconnects a call for which Session Handoff has been initiated, the call can still be continued by resuming the call at the desk phone prior to the expiration of the Session Handoff Alerting Timer. These cases can occur when a user moves to an area that does not have mobile connectivity, such as an elevator or dead zone/spot.

Session Handoff Using VoIP Mode With SIP Clients

For SIP clients, session handoff support exists for VoIP mode as well as for cellular mode. For this scenario, the following steps take place:

1. User that is using a SIP client on a remote destination in VoIP (Wi-Fi) mode initiates session handoff by using the Move softkey on the smartphone.
2. Cisco Unified Communications Manager flashes the shared line on the desk phone and does not break media until the desk phone answers the call.

Be aware that this function also works if the user is logged on to extension mobility.

Session Handoff Fails or User Cancels Session Handoff

If session handoff fails, the following steps take place:

1. Cisco Unified Mobile Communicator or a VoIP client initiates session handoff to a station that does not have the correct owner user ID.
2. Session handoff fails. A “Cannot move conversation” SIP message gets sent to the client.

If the user cancels session handoff, the session handoff stops. The following steps take place:

1. The user initiates session handoff from Cisco Unified Mobile Communicator or a VoIP client.
2. Before the session handoff completes, the user cancels the session handoff from the client.
3. Cisco Unified Communications Manager cancels the session handoff. Shared-line devices stop ringing.

Additional Information

See the “Related Topics” section on page 14-62.

Interactions and Limitations

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

Additional Information

See the “Related Topics” section on page 14-62.

Interactions

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

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.

Auto Call Pickup 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 call pickup.

Automatic Alternate Routing

Prior to the implementation of this interaction, if a desk phone was configured for Automatic Alternate Routing (AAR) and the desk phone was configured with a mobile phone as a remote destination, the AAR feature did not get triggered for calls to the remote destination if the out-of-bandwidth condition applied.

Cisco Unified Mobility now supports Automatic Alternate Routing (AAR) as follows:

- If a rejection occurs due to lack of bandwidth for the location-based service, the rejection triggers AAR for any device that is configured for AAR.
- If a rejection occurs based on Resource Reservation Protocol (RSVP), however, AAR does not get triggered for calls to remote destinations.

External Call Control

If external call control is configured, as described in the "External Call Control" chapter, Cisco Unified Communications Manager honors the route decision from the adjunct route server for the following Cisco Unified Mobility features:

- Mobile Connect
- Mobile Voice Access
- Enterprise Feature Access
- Dial-via-Office Reverse Callback
- Dial-via-Office Forward

Tip To invoke Mobile Voice Access or Enterprise Feature Access, the end user must dial a feature directory number that is configured in Cisco Unified Communications Manager Administration. When the Cisco Unified Communications Manager receives the call, Cisco Unified Communications Manager does not invoke external call control because the called number, in this case, is the feature DN. After the call is anchored, the Cisco Unified Communications Manager asks for user authentication, and the user enters the number for the target party. When Cisco Unified Communications Manager tries to extend the call to the target party, external call control gets invoked, and Cisco Unified Communications Manager sends a call routing query to the adjunct route server to determine how to handle the call.

Cisco Unified Communications Manager does not send a routing query for the following Cisco Unified Mobility features:

- Cell pickup
- Desk pickup
- Session handoff

Intelligent Session Control and Session Handoff

For direct calls to remote destinations that get anchored to the enterprise number, the mobile user can invoke the Session Handoff feature and mobile user can hand off the call to the desk phone.

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" in the *Cisco Unified Communications Manager Features and Services Guide*
- "Cisco Unified Mobility for End Users" in the *Cisco Unified Communications Manager System Guide*

Local Route Groups

For Single Number Reach calls to a remote destination, the device pool of the originating calling party determines the selection of the Standard Local Route Group.

Mobile Connect and SIP Trunks With Cisco Unified Border Element

Cisco Unified Mobility supports the Mobile Connect feature without midcall features over SIP trunks with Cisco Unified Border Element (CUBE).

Number of Supported Calls

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 14-62.

Limitations

Cisco Unified Mobility enforces the following limitations in operating with other Cisco Unified Communications Manager components:

- Call Anchoring, page 14-31
- Call Forwarding, page 14-31
- Cisco Unified IP Phones 7940 and 7960 That Are Running SIP, page 14-31
- Conferencing, page 14-31
- Dialing + Character From Mobile Phones, page 14-31
- DND on the Desk Phone and Direct Calls to Remote Destination, page 14-32
- Dual-Mode Handoff and Caller ID, page 14-32
- Dual-Mode Phones and Call Anchoring, page 14-32
- Dual-Mode Phones and CTI Applications, page 14-32
- Dual-Mode Phones and Desktop Call Pickup, page 14-32
- Dual-Mode Phones That Are Running SIP and Registration Period, page 14-32
- Enterprise Features From Cellular Networks, page 14-32
- Enterprise Features in GSM That Is Using DTMF, page 14-33
- Forced Authorization Code and Client Matter Code, page 14-33
- Gateways and Ports, page 14-33
- Maximum Wait Timer for Desktop Call Pickup Does Not Get Applied If Hold DTMF Is Pressed, page 14-33
- Mobile Connect Support Restrictions, page 14-33
- Multilevel Precedence and Preemption (MLPP), page 14-33
- Multiple-Node Cluster Environment, page 14-33
- Overlap Sending, page 14-33

- QSIG, page 14-33
- QSIG Path Replacement, page 14-33
- Remote Destination Profiles, page 14-34
- Remote Destinations, page 14-34
- Service Parameters, page 14-34
- Session Handoff Feature, page 14-34
- SIP URI and Direct Calls to Remote Destination, page 14-34
- Video Calls, page 14-34

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.

Cisco Unified IP Phones 7940 and 7960 That Are Running SIP

When running SIP, Cisco Unified IP Phones 7940 and 7960 do not support the Remote-in-use state and therefore cannot support desktop call pickup.

For these phones, if the mobile phone user hangs up a call that the Cisco Unified IP Phone 7940 or 7960 that is running SIP extended to the mobile phone, the calling party hears music on hold for ten seconds (as configured by the Maximum Wait Time for Desk Pickup field for the remote destination end user) and then the call drops. Because the desktop call pickup feature does not get supported for these phones when they are running as SIP devices, the user desk phone does not display the Resume softkey, so the user cannot pick up the call on the desk phone.

Cisco recommends that you configure Cisco Unified IP Phones 7940 and 7960 to run SCCP for users that are enabled for Cisco Unified Mobility.

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.

Dialing + Character From Mobile Phones

Users can dial a + sign through DTMF on a mobile phone to specify the international escape character.

Cisco Unified Mobility does not support + dialing through DTMF for interactive voice response (IVR) to make an outgoing call from a mobile phone to an enterprise IP phone for which the directory number contains the + character.

Cisco Unified Mobility does not support + dialing through DTMF for two-stage dialing to make an outgoing call from a mobile phone to an enterprise IP phone for which the directory number contains the + character.

For more information about configuring the international escape character in Cisco Unified Communications Manager Administration, see the "Using the International Escape Character +" section in the *Cisco Unified Communications Manager System Guide*.

DND on the Desk Phone and Direct Calls to Remote Destination

If Do Not Disturb (DND) is enabled on a desk phone, the desk phone cannot be placed in the Remote In Use (RIU) state and the call does not get anchored in these cases:

- DND is enabled with the call reject option—The call cannot get anchored.
- DND is activated by pressing the DND softkey on the desk phone—The call cannot get anchored.

If DND is enabled with the ring off option, however, the call does get anchored.

Dual-Mode Handoff and Caller ID

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

Dual-Mode Phones and Call Anchoring

Dual-mode phones (Cisco Unified Mobility Advantage and dual-mode phones that are running SCCP or SIP) that are configured as remote destinations cannot anchor calls.

Dual-Mode Phones and CTI Applications

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 disappear if the dual-mode phone goes out of WLAN range.

Dual-Mode Phones and Desktop Call Pickup

The desktop call pickup feature does not apply to the following mobile phone models:

- Nokia 902iL and Nokia 906iL dual-mode phones that are running SIP
- Nokia S60 dual-mode phones that are running SCCP

For these phone models, if the mobile phone user hangs up a call, the calling party hears music on hold for ten seconds (as configured by the Maximum Wait Time for Desk Pickup field for the remote destination end user) and then the call drops. Because the desktop call pickup feature does not get supported for these phone models, the user desk phone does not display the Resume softkey, so the user cannot pick up the call on the desk phone.

Dual-Mode Phones That Are Running SIP and Registration Period

For dual-mode phones that are running SIP, Cisco Unified Communications Manager determines the registration period by using the value in the Timer Register Expires (seconds) field of the SIP profile that associates with the phone, not the value that the SIP Station KeepAlive Interval service parameter specifies.

Enterprise Features From Cellular Networks

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

Note When using intercluster DNs as remote destinations for an IP phone via SIP trunk (either intercluster trunk [ICT] or gateway), check the Require DTMF Reception check box when configuring the IP phone, so DTMF digits can be received out of band, which is crucial for Enterprise Feature Access midcall features.

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.

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 nor with Enterprise Feature Access two-stage dialing.

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

Gateways and Ports

Both H.323 and SIP VoIP gateways get supported for Mobile Voice Access.

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

Maximum Wait Timer for Desktop Call Pickup Does Not Get Applied If Hold DTMF Is Pressed

If a user presses the *81 DTMF code from a remote destination (either a smartphone or any other phone) to put a call on hold, the user desk phone displays the Resume softkey. The desk phone does not apply a timer for desktop call pickup, however; the Resume key does not stop displaying after the timeout that is configured for the end user to pick up the call and the call does not get dropped.

Instead, users should hang up the call on the remote phone, which triggers the desk phone to apply the timer for desktop call pickup. (Use the Maximum Wait Time for Desk Pickup field on the End User Configuration window to change this setting.)

Mobile Connect Support Restrictions

The Mobile Connect feature gets supported only for Primary Rate Interface (PRI) public switched telephone network (PSTN) connections.

For SIP trunks, Mobile Connect gets supported via IOS gateways or intercluster trunks.

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.

Multiple-Node Cluster Environment

In a multiple-node cluster environment, if the Cisco Unified Communications Manager publisher server 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.

Overlap Sending

Overlap sending patterns do not get supported for the Intelligent Session Control feature.

QSIG

Mobility does not support QSIG.

QSIG Path Replacement

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

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.

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.

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.

Session Handoff Feature

The following limitations apply to the Session Handoff feature:

- Session Handoff can take place only from mobile phone to desk phone. For the other direction, the current Remote Destination Pickup method specifies using Send Call to Mobile Phone.
- Only audio call session handoff gets supported.

SIP URI and Direct Calls to Remote Destination

The Intelligent Session Control feature does not support direct URI dialing. Therefore, calls made to a SIP URI cannot be anchored to an enterprise number.

Video Calls

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

Additional Information

See the "Related Topics" section on page 14-62.

System Requirements

Mobile Connect and Mobile Voice Access 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).

To see which IP phones work with Mobile Connect and Mobile Voice Access, see the applicable Cisco Unified IP Phone Administration Guide and Cisco Unified IP Phone User Guide.

Additional Information

See the "Related Topics" section on page 14-62.

Migrating from Cisco Unified MobilityManager

Follow this process to migrate standalone Cisco Unified MobilityManager data to Cisco Unified Communications Manager:

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 and use the Bulk Administration Import/Export windows to import the CSV data files that were previously exported from Cisco Unified MobilityManager. See 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 14-62.

Configuring Cisco Unified Mobility

This section provides detailed procedures for each Cisco Unified Communications Manager Administration menu option that must be configured to provision Cisco Unified Mobility features that are native to Cisco Unified Communications Manager.

See the "Configuration Checklist for Cisco Unified Mobility" section on page 14-2 for an overview checklist of the procedures and steps that are necessary for an administrator to configure Cisco Unified Mobility features that are native to Cisco Unified Communications Manager.

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:

- Mobility Softkey Configuration, page 14-61

Tip Before you configure Cisco Unified Mobility, review the "Configuration Checklist for Cisco Unified Mobility" section on page 14-2.

Additional Information

See the "Related Topics" section on page 14-62.

Access List Configuration

You can define access lists to explicitly allow or block the extension of Mobile Connect calls to remote destinations based on the caller ID of the caller.

To configure access lists, see the following sections:

- Access List Configuration Settings, page 14-36
- Access List Member Detail Configuration Settings, page 14-38

Additional Information

See the "Related Topics" section on page 14-62.

Access List Configuration Settings

In Cisco Unified Communications Manager Administration, use the **Call Routing > Class of Control > Access List** menu path to configure access lists.

An access list, which supports Cisco Unified Mobility, specifies a list that determines the phone numbers that the system can pass or block from being passed to remote destinations. For more information on Cisco Unified Mobility, See the "Related Topics" section on page 14-62.

Tips About Configuring Access Lists

While you configure an access list, follow these additional steps to configure its members:

Step 1 If you want to configure the members of an access list, click **Add Member** and enter values for the parameters that are described in Table 14-5.

Step 2 Click **Save**.

The Access List Configuration window reopens to show the new number or filter in the Selected Filters area.

Step 3 From the Access List 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**.

Tips About Deleting Access Lists

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-2of the *Cisco Unified Communications Manager Administration Guide*. 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 14-43.
- Delete the remote destinations that are using the access list that you want to delete. See the "Remote Destination Configuration" section on page 14-43.

Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the "Navigating the Cisco Unified Communications Manager Administration Application" section in the *Cisco Unified Communications Manager Administration Guide* and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration Settings Table

Table 14-4 describes the available settings in the Access List Configuration window. For more information on Cisco Unified Mobility, see the "Related Topics" section on page 14-62.

Table 14-4 Access List Configuration Settings

Field	Description
Access List Information	
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 14-4 Access List Configuration Settings (continued)

Field	Description
Access List Member Information	
Selected Filters	This pane displays the current members of this access list. Members comprise the following types: • Private—This filter applies to calls that come from private numbers, which do not display caller ID. • Not Available—This filter applies to calls that come from numbers that do not have caller ID. • 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 #. Use the arrows below this pane to move the access list members to or from this pane. **Add Member**—Click this button to add a new member to the Selected Filters pane. The Access List Member Detail window displays. See the "Access List Member Detail Configuration Settings" section on page 14-38 for details.
Removed Filters	This pane specifies filters that have been defined for this access list but that are not currently selected. Use the arrows above this pane to move the access list members to or from this pane.

Additional Information

See the "Related Topics" section on page 14-62.

Access List Member Detail Configuration Settings

The Access List Member Detail window displays when you click the **Add Member** button on the Access List Configuration window while you configure an access list. The Access List Member Detail window allows you to configure the following settings for an access list member:

- Filter Mask
- DN Mask

After you configure a new access list member, the new access list member displays in the Access List Members pane at the bottom of the corresponding Access List Configuration window. You can click one of the access list members to view or change the settings for that access list member. To exit the Access List Member Detail window without making any changes, choose Back to Find/List from the Related Links drop-down list box and click **Go**.

Table 14-5 describes the available settings in the Access List Member Detail window.

Table 14-5 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).

Table 14-5 Access List Member Detail Configuration Settings (continued)

Field	Description
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: • X (upper or lower case)—Matches a single digit. • !—Matches any number of digits. • #—Used as a single digit for exact match. Examples: • 408! matches any number that starts with 408. • 408555123X matches any number between 4085551230 and 4085551239. **Note** If you want to filter an incoming call from a calling number that begins with a leading +, you must include the leading + in the DN Mask field unless any supported wild card precedes the directory number. For example, if an end user wants to block +14081239876, the user access list needs to include either +14081239876 or !14081239876 in the DN Mask field.

Additional Information

See the "Related Topics" section on page 14-62.

Remote Destination Profile Configuration

To configure remote destination profiles, see the following sections:

- Remote Destination Profile Configuration Settings, page 14-39
- Associating a Directory Number with a Remote Destination Profile, page 14-43

Additional Information

See the "Related Topics" section on page 14-62.

Remote Destination Profile Configuration Settings

In Cisco Unified Communications Manager Administration, use the **Device > Device Settings > Remote Destination Profile** menu path to configure remote destination profiles.

Remote destination profiles, which support Cisco Unified Mobility, specify a set of parameters that apply to all remote destinations for the user. For more information on Cisco Unified Mobility, see the "Related Topics" section on page 14-62.

Tips About Configuring Remote Destination Profiles

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

Tips About Deleting Remote Destination Profiles

You can delete remote destination profiles that associate with remote destinations. You receive a warning message that you are about to delete both a remote destination profile and the associated remote destinations.

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 of the *Cisco Unified Communications Manager Administration Guide*.

Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the "Navigating the Cisco Unified Communications Manager Administration Application" section in the *Cisco Unified Communications Manager Administration Guide* and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration Settings Table

Table 14-6 describes the available settings in the Remote Destination Profile Configuration window. For related procedures, see the "Related Topics" section on page 14-62.

Table 14-6 Remote Destination Profile Configuration Settings

Field	Description
Remote Destination Profile Information	
Name	Enter a text name for the remote destination profile. This name can comprise up to 50 characters. Valid characters include letters, numbers, dashes, dots (periods), spaces, and underscores.
Description	Enter a text description of the remote destination profile. This field can comprise up to 128 characters. You can use all characters except quotes (“), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).
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 Voice Access or Enterprise Feature Access calls. **Note** This calling search space setting applies only when you are routing calls from the remote destination, which specifies the outbound call leg to the dialed number for Mobile Voice Access and Enterprise Feature Access calls.
User Hold Audio Source	Choose the audio option for users on hold for Mobile Connect and Mobile Voice Access calls.

Table 14-6 Remote Destination Profile Configuration Settings (continued)

Field	Description
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 remote destination profile. If you choose the Default value for this field, the setting matches the value of the Privacy Setting service parameter. **Note** If you change and save the value of the Privacy Setting service parameter, you must return to the Remote Destination Profile Configuration window for a remote destination profile that specifies Default and click **Save** for the service parameter change to take effect. **Note** You cannot transfer a call from a cell phone to a desk phone if the Remote Destination Profile Privacy specifies On, and the "Enforce Privacy Setting on Held Calls" service parameter specifies True. For more configuration information, see Barge and Privacy.
Rerouting Calling Search Space	Choose a calling search space to be used to route Mobile Connect calls. **Note** 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. **Note** The Rerouting Calling Search Space setting applies only when you are routing calls to the remote destination or mobility identity, which specifies the outbound call leg toward the remote destination or mobility identity when a call comes in to the user enterprise number. **Note** Mobile Connect calls do not get routed to the dual-mode mobility identity number that corresponds to the dual-mode mobile phone number if the device associates with the enterprise WLAN and registers with Cisco Unified Communications Manager. Mobile Connect calls get routed to the dual-mode mobility identity number only when the device is outside the enterprise.

Table 14-6 Remote Destination Profile Configuration Settings (continued)

Field	Description
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. **Note** The partitions in the calling search space should contain only calling party transformations. **Note** Ensure the calling search space is not null because no transformations can apply to null partitions. **Note** 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 **Call Routing > Class of Control > Calling Search Space**, you assign the CSS to a partition; when you configure the Calling Party Transformation CSS under **Call Routing > Transformation Pattern > Calling Party Transformation Pattern**, 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.
User Locale	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. Cisco Unified Communications Manager makes this field available only for phone models that support localization. **Note** If the users require information to display (on the phone) in any language other than English, verify that the locale installer is installed before you configure user locale. See the Cisco Unified Communications Manager Locale Installer documentation.
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.
Associated Remote Destinations	
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. See the "Remote Destination Configuration" section on page 14-43 for details.

Table 14-6 Remote Destination Profile Configuration Settings (continued)

Field	Description
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.
Do Not Disturb	
Do Not Disturb	Check this check box to enable Do Not Disturb on the phone.
DND Option	This Call Reject option specifies that no incoming call information gets presented to the user. **Note** 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.

Additional Information

See the "Related Topics" section on page 14-62.

Associating a Directory Number with a Remote Destination Profile

After creating a remote destination profile, you must associate the DN record for the desk 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 14-62.

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 represents a mobile or other phone that can be configured to perform remote destination pickup (accept transfers from the desk phone of the user) and accept incoming Mobile Connect calls that come from the system as a result of the line that is shared with the desk phone.

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 "Directory Number Configuration Settings" in the *Cisco Unified Communications Manager Administration Guide*.

Note This section describes how to access remote destination records by opening the Remote Destination Configuration window. You can also open an existing or new record in the Remote Destination Profile Configuration window by clicking the Add a New Remote Destination link at the bottom of the remote destination profile. See the "Remote Destination Profile Configuration" section on page 14-39 for instructions on displaying a remote destination profile.

To configure remote destinations, see the following section:

- Remote Destination Configuration Settings, page 14-44

Additional Information

See the "Related Topics" section on page 14-62.

Remote Destination Configuration Settings

In Cisco Unified Communications Manager Administration, use the **Device > Remote Destination** menu path to configure remote destinations.

Remote destinations represent phones that are available for Mobile Connect answer and pickup, plus locations that are used to reach Mobile Voice Access. Remote destinations may include any of the following devices:

- Single-mode mobile (cellular) phones
- Smartphones
- Dual-mode phones
- Enterprise IP phones that are not in the same cluster as the desk phone
- Home phone numbers in the PSTN.

For more information on Cisco Unified Mobility, see the "Related Topics" section on page 14-62.

Tips About Configuring Remote Destinations

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

Be aware that the appropriate timer settings in Table 14-7 may be service-provider-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 service provider for the remote destination phone.

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

Note This step requires that a directory number has already been configured on the remote destination profile with which the remote destination associates.

Tips About Deleting Remote Destinations

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 of the *Cisco Unified Communications Manager Administration Guide*.

Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the "Navigating the Cisco Unified Communications Manager Administration Application" section in the *Cisco Unified Communications Manager Administration Guide* and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration Settings Table

Table 14-7 describes the available settings in the Remote Destination Configuration window. For related procedures, see the "Related Topics" section on page 14-62.

Table 14-7 Remote Destination Configuration Settings

Field	Description
Remote Destination Information	
Mobile Identity Information	
Name	Enter a name that identifies the remote destination or mobile identity.
Destination Number	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. **Note** Add the necessary translation pattern or route patterns to route the destination number. For the SIP URI feature, you can also enter a Universal Resource Indicator (URI) in this field, such as *user@corporation.com*, up to 126 characters in length. Keep in mind that a SIP route pattern must also be configured. If the administrator configures the Incoming Calling Party settings in the Cisco Unified Communications Manager gateway, trunk, or device pool to globalize the incoming calling party number, configure the Destination Number of the remote destination in the E.164 format. Example: For a remote destination with US area code 408 and destination number 5552222, configure the Destination Number as +14085552222. Additionally, if globalized destination numbers are in use, set the Matching Caller ID with Remote Destination service parameter to Complete Match.
Answer Too Soon Timer	Enter the minimum time in milliseconds that Cisco Unified Communications Manager requires the mobile phone to ring before answering the call. This setting accounts for situations where the mobile phone is switched off or is not reachable, in which case the network may immediately divert the call to the mobile phone voice mail. If the mobile phone is answered before this timer expires, Cisco Unified Communications Manager pulls the call back to the enterprise. Range: 0 - 10,000 milliseconds Default: 1,500 milliseconds

Table 14-7 Remote Destination Configuration Settings (continued)

Field	Description
Answer Too Late Timer	Enter the maximum time in milliseconds that Cisco Unified Communications Manager allows for the mobile phone to answer. If this value is reached, Cisco Unified Communications Manager stops ringing the mobile phone and pulls the call back to the enterprise. Range: 10,000 - 300,000 milliseconds Default: 19,000 milliseconds
Delay Before Ringing Timer	Enter the time that elapses before the mobile phone rings when a call is extended to the remote destination. Range: 0 - 30,000 milliseconds Default: 4,000 milliseconds **Tip** When a hunt group is in use, the lines ring only for a short period of time. You may need to manipulate the Delay Before Ringing Timer setting and make it zero to allow a remote destination call to be established, ring, and answer, before the hunt list timer expires and pulls the call back.
Remote Destination Profile	From the drop-down list box, choose the remote destination profile that you want to use for this remote destination.
Mobility Profile	From the drop-down list box, choose the mobility profile that you want to use for this remote destination. To configure a mobility profile, use the **Call Routing > Mobility > Mobility Profile** menu option. See the "Mobility Profile Configuration" section on page 14-58 for details.
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.
Mobile Phone	Check the check box if you want calls that the desk phone answers to be sent to your mobile phone as the remote destination. Checking this check box ensures that, if Send Call to Mobile Phone is specified (by using the Mobility softkey for remote destination pickup), the call gets extended to this remote destination. **Note** This check box does not apply to dual-mode phones that are running SIP, such as DoCoMo N902iL and DoCoMo N906i, nor to dual-mode phones that are running SCCP, such as Nokia S60.
Enable Mobile Connect	Check the check box to allow an incoming call to ring your desk phone and remote destination at the same time.

Table 14-7 Remote Destination Configuration Settings (continued)

Field	Description
When Mobile Connect Is Enabled	
Ring Schedule	
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 *When receiving a call during the above ring schedule* 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 *When receiving a call during the above ring schedule* pane below.
(day of week)	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. **(day of the week)**—Check the check box for a day of the week, such as Monday, to specify the ring schedule for that day. **All Day**—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 *When receiving a call during the above ring schedule* pane below. **(drop-down list box) to (drop-down list box)**—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 **to** and specify the ending time by choosing a value in the drop-down list box that follows **to**. For a particular day, the default ring schedule specifies *No Office Hours*. The values that you specify in the drop-down list boxes relate to the time zone that you specify in the **Time Zone** field for the remote destination or mobile identity.
Time Zone	From the drop-down list box, choose a time zone to use for this remote destination or mobile identity. **Note** The time-of-day access feature uses the time zone that you choose for this remote destination or mobile identity to allow or to block calls to this remote destination or mobile identity.
When receiving a call during the above ring schedule	
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.

Table 14-7 Remote Destination Configuration Settings (continued)

Field	Description
Ring this destination only if caller is in	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. 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 **Call Routing > Class of Control > Access List** menu option.) Choosing an access list that contains no members equates to choosing to never ring this destination.
Do not ring this destination if caller is in	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. 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 **Call Routing > Class of Control > Access List** menu option.) Choosing an access list that contains no members equates to choosing the Always ring this destination radio button.
Association Information	
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. You must check a line association check box for Mobile Connect to work for this remote destination. **Note** Be aware that the line association check box of a line must be checked for Mobile Connect calls to ring this remote destination when a call comes into the directory number that is assigned to that line.

Additional Information

See the "Related Topics" section on page 14-62.

Mobile Voice Access Directory Number Configuration

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

This configuration is required for making calls with the Mobile Voice Access feature. After the gateway collects the required digits from the user to make a call, the call gets transferred to the DN that is configured in this window. This DN can be an internal DN to Cisco Unified Communications Manager and the end user does not need to know the DN. The administrator must configure a dial-peer so that the MVA service can transfer the call from the gateway to this DN. This DN should be also be placed in a

partition where the inbound calling search space (CSS) of the gateway or the remote destination profile CSS can reach the DN, as configured in the Inbound Calling Search Space for Remote Destination service parameter in the Clusterwide Parameters (System - Mobility) pane.

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 14-8.

Step 3 Click **Save**.

Additional Information

See the "Related Topics" section on page 14-62.

Mobile Voice Access Configuration Settings

Table 14-8 describes the available settings in the Mobile Voice Access window. For more information on Cisco Unified Mobility, see the "Related Topics" section on page 14-62.

Table 14-8 Mobile Voice Access Configuration Settings

Field	Description
Mobile Voice Access Information	
Mobile Voice Access Directory Number	Enter the internal DN to receive Mobile Voice Access calls from the gateway. Enter a value between 1 and 24 digits in length. You may use the following characters: 0 to 9.
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.
Mobile Voice Access Localization	
Available Locales	This pane displays the locales that have been configured. See the Cisco Unified Communications Manager Locale Installer documentation for details. Use the Down Arrow key to move the locales that you select to the Selected Locales pane. **Note** 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."

Table 14-8 Mobile Voice Access Configuration Settings (continued)

Field	Description
Selected Locales	Use the arrows above this pane to move the locales that you want to select to or from this pane. **Note** Remember that you can select a maximum of nine locales, even if more locales are available in the system. 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. **Note** 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.

Additional Information

See the "Related Topics" section on page 14-62.

Gateway Configuration for Enterprise Feature Access

To configure H.323 or SIP gateways for Enterprise Feature Access, two options are available:

- Configuring an H.323 or SIP Gateway for System Remote Access, page 14-50
- Configuring an H.323 Gateway for System Remote Access by Using Hairpinning, page 14-53

Additional Information

See the "Related Topics" section on page 14-62.

Configuring an H.323 or SIP Gateway for System Remote Access

If you already have an H.323 or SIP 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 or SIP gateway, you must add and configure one. For more information, see 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 or SIP 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 Publisher IP Addr>:8080/ccmivr/pages/IVRMainpage.vxml

Sample configuration before IOS Version 12.3(12):

- call application voice Unified CCM
- http://<Unified CM 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 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

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)*

Step 5 Add a dial-peer to transfer the calls to the Mobile Voice Access DN that is configured in the "Mobile Voice Access Directory Number Configuration" section on page 14-48.

Sample configuration for primary Cisco Unified Communications Manager:

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

Note This specifies the Mobile Voice Access DN that is configured with the **Media Resources > Mobile Voice Access** menu option. 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 This specifies the Mobile Voice Access DN that is configured with the **Media Resources > Mobile Voice Access** menu option. 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

Sample configuration for SIP gateway voip dial-peer:

- dial-peer voice 80 voip
- destination-pattern <Mobile Voice Access DN>
- rtp payload-type nse 99
- session protocol sipv2
- session target ipv4:10.194.107.80
- incoming called-number .T

- dtmf-relay rtp-nte
- codec g711ulaw

Additional Information

See the "Related Topics" section on page 14-62.

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

If you do not have an H.323 gateway but want to use a H.323 gateway only to support System Remote Access, you must add and configure the gateway. For more information, see the "Adding a Cisco IOS H.323 Gateway" section in the *Cisco Unified Communications Manager Administration Guide*.

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 Publisher IP Addr>:8080/ccmivr/pages/IVRMainpage.vxml

Sample configuration before IOS Version 12.3(12):

- call application voice Unified CCM
- http://<Unified CM 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 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 that is configured in the "Mobile Voice Access Directory Number Configuration" section on page 14-48.

Sample configuration for primary Cisco Communications Manager:

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

Note This specifies the Mobile Voice Access DN that is configured with the **Media Resources > Mobile Voice Access** menu option. 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 This specifies the Mobile Voice Access DN that is configured with the **Media Resources > Mobile Voice Access** menu option. 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

Step 5 On the Cisco Unified Communications Manager, create a new route pattern to redirect the incoming MVA number to the H.323 gateway that has the vxml script loaded. Ensure that the Incoming CSS of the gateway can access the partition in which the new route pattern gets created.

Additional Information

See the "Related Topics" section on page 14-62.

Enterprise Feature Access Two-Stage Dialing

To configure enterprise feature access two-stage dialing, 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 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 > Enterprise Feature Access Configuration**.

Step 5 In the Mobility Enterprise Feature Access Configuration window, configure the Enterprise Feature Access DID by specifying a value in the (Access Number Information) Number field. (This field specifies the same DID that is called to invoke midcall features like Transfer and Conference.)

Step 6 Specify the partition by choosing a value for the Route Partition.

Step 7 To save the Mobility Enterprise Feature Access Configuration settings, click **Save**.

Step 8 Ensure that the outbound VOIP dial-peer that is used on the gateway for the initial call leg over to the remote destination (mobile phone) has DTMF-relay configuration in it, so the DTMF codes can get passed through to Cisco Unified Communications Manager.

Step 9 Configure dial-peers on the gateway that receives the second-stage inbound call to the Enterprise Feature Access DID, so the call gets forwarded to the Cisco Unified Communications Manager. Ensure that the VOIP dial-peer has the DTMF-relay configuration in it.

Note If a generic dial-peer is already configured to forward the calls to Cisco Unified Communications Manager and is consistent with the EFA DN, you do not need to perform this step. Ensure that the VOIP dial-peer for this call leg also has a configured DTMF-relay command.

See the *Cisco Unified Communications Solution Reference Network Design (SRND) Based on Cisco Unified Communications Manager* for the list of steps that you need to configure Enterprise Feature Access.

When a caller calls the Enterprise Feature Access 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

inserts 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.

See the User Guide of the remote phone model for the steps that users perform to make outbound calls and to use Mobile Voice Access. Keep in mind that, when you use Enterprise Feature Access, each entry must end with the # (octothorpe) character.

Note When calling the Mobile Voice Access DN or Enterprise Feature Access DN, the gateway device must present the exact number of digits that are configured as the Mobile Voice Access DN or Enterprise Feature Access DN. Translation patterns or other called number modification cannot be used to match the MVA or EFA numbers either by stripping digits or by adding digits to the number that the gateway presents. Because Cisco Unified Mobility intercepts the call at the gateway layer, the feature behaves thus by design.

Note Unlike Mobile Voice Access (MVA), Enterprise Feature Access (EFA) identifies the user based solely on caller ID. If the system receives no inbound caller ID or receives a value that does not match a remote destination, the EFA call fails. With MVA, if the caller ID does not match, the user gets prompted to enter the user remote destination number. EFA does not provide this capability because no IVR prompts exist. In both cases, after the user is identified, the user authenticates by using the same PIN number.

Additional Information

See the "Related Topics" section on page 14-62.

Mobility Enterprise Feature Configuration

To configure mobility enterprise feature configuration, see the following section:

- Mobility Enterprise Feature Configuration Settings, page 14-56

Additional Information

See the "Related Topics" section on page 14-62.

Mobility Enterprise Feature Configuration Settings

In Cisco Unified Communications Manager Administration, use the **Call Routing > Mobility > Enterprise Feature Access Configuration** menu path to configure mobility enterprise feature configuration.

The Mobility Enterprise Feature Configuration window allows you to configure mobility enterprise feature access (EFA) numbers. These numbers can then associate with mobility profile(s) for use.

Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the "Navigating the Cisco Unified Communications Manager Administration Application" section in the *Cisco Unified Communications Manager Administration Guide* and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration Settings Table

Table 14-9 describes the available settings in the Mobility Enterprise Feature Configuration window. For more information on Cisco Unified Mobility, see the "Related Topics" section on page 14-62.

Table 14-9 Mobility Enterprise Feature Configuration Settings

Field	Description
Access Number Information	
Number	Enter the DID number that is required for enterprise feature access. This number supports transfer, conference, resume, and two-stage dialing from smartphones. **Note** Ensure that each DID number is unique.
Route Partition	From the drop-down list box, choose the partition of the DID that is required for enterprise feature access.
Description	Enter a description of the Mobility Enterprise Feature Access number.
Default Enterprise Feature Access Number	Check this box to make this Enterprise Feature Access number the default for this system.

Additional Information

See the "Related Topics" section on page 14-62.

Handoff Mobility Configuration

To configure handoff mobility configuration, see the following section:

- Handoff Mobility Configuration Settings, page 14-57

Additional Information

See the "Related Topics" section on page 14-62.

Handoff Mobility Configuration Settings

In Cisco Unified Communications Manager Administration, use the **Call Routing > Mobility > Handoff Configuration** menu path to configure handoff mobility configuration.

The Handoff Mobility Configuration window allows you to configure a handoff number and/or partition for dual-mode phones between the Wi-Fi and Global System for Mobile communication (GSM) or Code Division Multiple Access (CDMA) networks.

Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the "Navigating the Cisco Unified Communications Manager Administration Application" section in the *Cisco Unified Communications Manager Administration Guide* and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration Settings Table

Table 14-10 describes the available settings in the Handoff Mobility Configuration window. For more information on Cisco Unified Mobility, see the "Related Topics" section on page 14-62.

Table 14-10 Handoff Mobility Configuration Settings

Field	Description
Handoff Configuration Information	
Handoff Number	Enter the DID number for handoff between the Wi-Fi and GSM or CDMA networks. The handoff feature requires this number. For numbers that start with the international escape character +, you must precede the + with a backslash (\). Example: \+15551234.
Route Partition	From the drop-down list box, choose the partition to which the handoff direct inward dial (DID) number belongs.

Additional Information

See the "Related Topics" section on page 14-62.

Mobility Profile Configuration

To configure mobility profiles, see the following section:

- Mobility Profile Configuration Settings, page 14-58

Additional Information

See the "Related Topics" section on page 14-62.

Mobility Profile Configuration Settings

In Cisco Unified Communications Manager Administration, use the **Call Routing > Mobility > Mobility Profile** menu path to configure mobility profiles.

Mobility profiles specify profiles where you can configure Dial-via-Office Forward or Dial-via-Office Reverse settings for a mobile client. After you configure a mobility profile, you can assign it to a user or to a group of users, such as the users in a region or location. You specify either DVO-F or DVO-R for a particular mobility profile, but you configure both the DVO-F and DVO-R settings for the mobility profile.

Mobility profiles can associate with a standalone Cisco Unified Mobile Communicator mobile identity or with a Cisco Unified Mobile Communicator-enabled dual-mode mobile identity. Standard, single-mode remote destinations cannot associate with a mobility profile.

Mobility profiles settings can be changed only by administrators: users cannot change the settings in a mobility profile.

Note If no mobility profile exists for a client and the client opts to let the server choose, the default DVO call type specifies Dial-via-Office Reverse (DVO-R).

Tips About Configuring Mobility Profiles

Before you start to configure mobility profiles, consider the design issues that follow.

If a client associates with a mobility profile and a DVO-R call is configured, the caller ID value in the 183 SIP message gets retrieved according to the following preference order:

1. DVO-R caller ID from the mobility profile (if this value is configured in the mobility profile)
2. EFA DN from mobility profile (if this value is configured in the mobility profile)
3. Default EFA DN

Note The administrator must configure the caller ID value in at least one of the preceding settings for the DVO-R call to succeed.

If a client associates with a mobility profile and a DVO-F call is configured, the DID value in the 183 SIP message gets retrieved according to the following preference order:

1. DVO-F service access number from mobility profile (if this value is configured in the mobility profile)
2. DVO-F EFA DN from mobility profile (if this value is configured in the mobility profile)
3. Default service access number, which is configured in the Service Parameter Configuration window
4. Default EFA DN

Note For a DVO-F call, the client needs to make an incoming call to Cisco Unified Communications Manager that terminates at a particular DID. The administrator must configure this DID in at least one of the preceding settings for the DVO-F call to succeed.

Cisco Unified Communications Manager identifies an incoming PSTN call (made by the client) as DVO-F by matching the called number (that is, the DID number that was sent in the 183 SIP message) in the following priority order:

If a mobility profile associates with the client

1. DVO-F EFT DN from mobility profile (if this value is configured)
2. DVO-F service access number from mobility profile (if this value is configured)

If no mobility profile associates with the client:

1. Default EFA DN
2. Default service access number

Also consider the following requirements when you configure mobility profiles:

- Administrator should configure the PSTN gateway so that matching of the called party can take place.
- EFA DN and service access number always comprise a pair: both of these values get retrieved from the mobility profile and must match in the mobility profile, or both default values get retrieved and the default values must match.

Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the "Navigating the Cisco Unified Communications Manager Administration Application" section in the *Cisco Unified Communications Manager Administration Guide* and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration Settings Table

Table 14-11 describes the available settings in the Mobility Profile Configuration window. For more information on Cisco Unified Mobility, see the "Related Topics" section on page 14-62.\

Table 14-11 Mobility Profile Configuration Settings

Field	Description
Mobility Profile Information	
Name	Enter a unique name for this mobility profile, up to 50 characters in length. Valid values specify upper- and lowercase letters, numeric digits (0 through 9), periods (.), dashes (-), underscores (_) and spaces ( ).
Description	Enter a description for this mobility profile.
Mobile Client Calling Option	From the drop-down list box, choose a mobile client calling option: • **Dial via Office Reverse**—Choose this option for the mobile client to make Dial-via-Office Reverse calls. • **Dial via Office Forward**—Choose this option for the mobile client to make Dial-via-Office Forward calls. **Note** The administrator configures either DVO-R or DVO-F for automatic selection by the client for any DVO calls that the user makes. Users can make the opposite type of DVO call than what the administrator has configured by explicitly choosing their DVO call type on their mobile devices.
Dial-via-Office Forward Configuration	
Service Access Number	Enter the DID number that is required for Dial-via-Office Forward feature access. This number supports transfer, conference, resume, and two-stage dialing from smartphones. This number gets returned in the 183 SIP message that Cisco Unified Communications Manager sends to the client. The client uses this value as a dial-in DID. Cisco Unified Communications Manager uses this value as the first preference to search when completing a DVO-F call. If this value is not configured, Cisco Unified Communications Manager uses the value in the Enterprise Feature Access Number/Partition field. **Note** Ensure that each DID number is unique.

Table 14-11 Mobility Profile Configuration Settings (continued)

Field	Description
Enterprise Feature Access Number/Partition	From the drop-down list box, choose the number or number and partition of the DID that is required for Dial-via-Office Forward call completion. After the client dials the Service Access Number, the gateways compare this value with the stripped digits that Cisco Unified Communications Manager sends. If the number is configured with a partition, both the number and the partition display in the drop-down list box. Cisco Unified Communications Manager uses this value as the second preference to search when completing a DVO-F call.
Dial-via-Office Reverse Callback Configuration	
Callback Caller ID	Enter a callback caller ID for dial-via-office reverse callback completion. If the client makes a DVO-R call, Cisco Unified Communications Manager send this value in the 183 SIP message, and this value becomes the caller ID value for the callback call that the client receives. This value displays in the client screen for DVO-R.

Additional Information

See the "Related Topics" section on page 14-62.

Mobility Softkey Configuration

To configure a Mobility softkey for the phone user that uses 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 Softkey 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 14-62.

Related Topics

- Mobility Profile Configuration, page 14-58
- Mobility Softkey Configuration, page 14-61
- End User Configuration, *Cisco Unified Communications Manager Administration Guide*
- Service Parameter Configuration, *Cisco Unified Communications Manager Administration Guide*
- Licenses for Cisco Unified Mobility, *Cisco Unified Communications Manager Features and Services Guide*
- Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator Integration, page 15-1

Additional Cisco Documentation

- *Cisco Unified Serviceability Administration Guide*
- *Cisco Unified Communications Manager Security Guide*
- *Troubleshooting Guide for Cisco Unified Communications Manager*
- Applicable Cisco Unified IP Phone User Guides
- Applicable Cisco Unified IP Phone Administration Guides
- "Cisco Mobility Applications" chapter in *Cisco Unified Communications Solution Reference Network Design (SRND) Based on Cisco Unified Communications Manager*
- "Configuring Cisco Unified Communications Manager for Use With Cisco Unified Mobility Advantage" chapter in the *Installation and Administration Guide for Cisco Unified Mobility Advantage*