Cisco Mobility

- Cisco Unified Mobility, on page 1
- Cisco Jabber for Mobile, on page 66

Cisco Unified Mobility

This chapter provides information about Cisco Unified Mobility which 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 Mobility Manager, by using the Cisco Unified Communications Manager Administration windows to configure the setup for end users. End users can use Cisco Unified Communications Self Care Portal 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 Communications Self Care Portal windows.

Configure 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, on page 4.

Perform the following steps to configure Cisco Unified Mobility.

Note The CMC and FAC feature on Cisco Mobility does not support an alternative number as its DVO callback number. The DVO callback number has to be the number registered in the MI (Mobility Identity) page. For example, consider a dual-mode phone that has a registered MI of 408-555-1111. The route-pattern "9.@" is used to route the external call and has FAC enabled. The DVO callback number in Cisco Jabber on the dual-mode device must be set to 408-555-1111.

Procedure

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.

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 Cisco Unified Mobility.

Step 3 Create access lists for Cisco Unified Mobility by assigning each list to the Cisco Unified Mobility user and specifying whether the list is an allowed or blocked list.

Step 4 Create remote destination profiles and assign each user to a profile.

Step 5 Associate desktop directory numbers (DNs) for the user.

Step 6 Add remote destinations by selecting the previously-defined profile as part of the configuration.

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.

Step 8 Configure the directory number for Mobile Voice Access.

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.

Step 10 Configure mobility settings for dual-mode phone handoff.

Step 11 Configure a Mobility softkey for the phone user that uses Cisco Unified Mobility.

Step 12 Configure time-of-day access for users. Use the fields in the When Cisco Unified Mobility is Enabled pane of the Remote Destination Configuration window to do so.

Related Topics

Access List Configuration and Deletion, on page 39
Remote Destination Profile Configuration, on page 42
Associate a Directory Number with a Remote Destination Profile, on page 46
About Remote Destination Setup, on page 46
Mobile Voice Access Directory Number Configuration, on page 52
Configure Enterprise Feature Access Two-Stage Dialing, on page 59
About Handoff Mobility Setup, on page 61
Mobility Softkey Configuration, on page 66

Cisco Unified Mobility Feature

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

Terminology

The following table provides definitions of terms that are related to Cisco Unified Mobility.

Table 1: Definitions

Term	Definition
Access List	List that determines the phone numbers that the system can pass or block from being passed to remote destinations.
Session Handoff	Transfer of session/conversations such as voice, video, and meetings between various Unified Communications clients that associate with a single user.
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 Cisco Unified Mobility 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.
Cisco Unified Mobility	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.

Term	Definition
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 Cisco Unified Mobility capabilities.
Remote Destination	Phones that are available for Cisco Unified Mobility 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.

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.

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:

- Cisco Unified Mobility - 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.
- 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.
- 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.

- Mobile Voice Access - This feature extends Cisco Unified Mobility capabilities by providing an interactive voice response (IVR) system to initiate two-stage dialed calls through the enterprise and activate or deactivate Cisco Unified Mobility capabilities
- 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).

  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.
- 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 Cisco Unified Mobility feature is enabled, calls get extended to remote destinations if the associated DN is called based on time-of-day-access-based configuration.
- 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.
- SIP URI Dialing - This feature supports SIP URI as an additional type of remote destination for Cisco Unified Mobility.
- 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.
- 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.

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.

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 Cisco Unified Mobility with no loss of expected IP phone features.
- Remote on/off control - User can turn Cisco Unified Mobility feature. See Cisco Unified Mobility, on page 7 for details.
- Call tracing - The system logs detailed Cisco Unified Mobility calls and provides information to help the enterprise optimize trunk usage and debug connection problems.
- Security and privacy for Cisco Unified Mobility calls - During an active Cisco Unified Mobility call, the associated desktop IP phone remains secured. The system removes access to the call from the desktop as soon as the mobile connection becomes active, which prevents the possibility of an unauthorized person listening in on the call that is bridged to the mobile phone.
- Client Matter Codes (CMC) and Forced Authorization Codes (FAC) - You can manage call access and accounting. CMCs assist with call accounting and billing for billable clients. FACs regulate the types of calls that certain users can place and force the user to enter a valid authorization code before the call is established.
- IPv6 support - Cisco Unified Communications Manager supports IPv6 addressing from mobile phones. For information about how to configure IPv6 in Cisco Unified Communications Manager, see “IPv6 for Cisco Unified Communications Manager” in the *Cisco Unified Communications Manager Features and Services Guide*.

- Session persistency - Mobile users can roam between different networks (e.g. Wi-Fi, VPN over 3G/4G) without having to re-register with Cisco Unified Communications Manager. This feature allows users to maintain registration with Cisco Unified Communications Manager in the case of network connectivity loss, allows users to transit calls from one network to another without call drops, and prevents the loss of SIP-based subscription status while users are roaming.

Cisco Unified Mobility

Cisco Unified Mobility 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 Cisco Unified Mobility 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 About Remote Destination Setup, on page 46.

Methods for Enabling and Disabling Cisco Unified Mobility

The following methods are available for enabling and disabling the Cisco Unified Mobility 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 Cisco Unified Mobility check box (to enable Cisco Unified Mobility) or by unchecking this check box (to disable Cisco Unified Mobility).
-
- 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 Cisco Unified Mobility status. See Enable or Disable Cisco Unified Mobility From Mobile Phone, on page 70 for details.

Cisco Unified Mobility Status

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

RDNIS/Diversion Header

The RDNIS/diversion header for Cisco Unified Mobility 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 Cisco Unified Mobility calls.

For Cisco Unified Mobility 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 Cisco Unified Mobility 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 Cisco Unified Mobility

See the Use Case Scenarios for Cisco Unified Mobility, on page 20 for the use case scenarios that Cisco Unified Communications Manager supports with this feature.

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.

Send Call to Mobile Phone

Users can perform remote destination pickup on in-progress mobility calls by using the Send Call to Mobile Phone feature. To do so, users press the Mobility softkey on the desk phone and select Send Call to Mobile Phone, which generates calls to all of the remote destinations that are configured. Users 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 is sent to the device on the Wi-Fi side.
- If the dual-mode smartphone is not registered to Wi-Fi, the call is sent to the device on the cellular side.

Mobile Voice Access

Mobile Voice Access extends Cisco Unified Mobility 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 Cisco Unified Mobility 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, on page 20 for the use case scenarios that Cisco Unified Communications Manager supports with this feature.

Midcall Enterprise Feature Access Support

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.

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.

Time-of-Day Access

An access list determines whether a call should be extended to a remote destination that is enabled for the Cisco Unified Mobility 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 Communications Self Care Portal (by end users).

Use case scenarios are provided 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.

Related Topics

Use Case Scenarios for Time-of-Day Access, on page 20

Time-of-Day Access Configuration

Perform the following steps to configure the Time-of-Day Access feature for Cisco Unified Mobility.

Procedure

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 Cisco Unified Mobility.

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. Use the **Call Routing** > **Class of Control** > **Access List** menu option.

Note An access list must have an owner. No system access list exists.

Step 3 Create remote destination profiles and assign each user to a profile.

Step 4 Configure a remote destination for a user. Remote destinations represent the mobile (or other) phones that can accept Cisco Unified Mobility 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 Cisco Unified Mobility check box for the remote destination enables Cisco Unified Mobility to apply the settings in the When Cisco Unified Mobility is Enabled pane to calls that are made to this remote destination. If the Enable Cisco Unified Mobility 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.

Related Topics

Access List Configuration and Deletion, on page 39
Remote Destination Profile Configuration, on page 42
About Remote Destination Setup, on page 46

Additional Information 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, on page 20 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 Communications Self Care Portal windows.

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.

1. After the call connects, dial the following field-and-digit sequence: <PIN>#*84#<Park Code>#*84#
2. 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 throughout the system. Every Cisco Unified Communications Manager server in the system 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:
3. <PIN>#1#<Retrieval Prefix><Park Number>#
4. 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, on page 21 for the use case scenarios that Cisco Unified Communications Manager supports with this feature.

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.

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.

Note For IP Multimedia Subsystem (IMS), ensure that the Cisco Unified Mobility feature is enabled in the Remote Destination Configuration window, or by using one of the other methods prescribed for enabling Cisco Unified Mobility, before implementing Intelligent Session Control call processing.

To access the Reroute Remote Destination Calls to Enterprise Number service parameter, 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.

Use case scenarios are provided 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 topic 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 Cisco Unified Mobility feature is enabled in the Remote Destination Configuration window, or by using one of the other methods prescribed for enabling Cisco Unified Mobility, before implementing Intelligent Session Control call processing for IP Multimedia Subsystem.
- 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**).

Related Topics

Interactions, on page 26
Limitations, on page 28
Use Case Scenarios for Intelligent Session Control, on page 22

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 the Session Handoff feature entails configuration of specific service parameters and configuration of the mobile device that will hand off calls.

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.

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.

Related Topics

Limitations, on page 28
Use Case Scenarios for Session Handoff, on page 24

Session Persistency

Session Persistency enhances the mobile user experience while roaming. Session Persistency allows mobile users with supported mobile devices to do the following:

- Roam between different networks (e.g. Wi-Fi, VPN over 3G/4G) without having to re-register with Cisco Unified Communications Manager.

- Maintain the SIP-based subscription status with Cisco Unified Communications Manager while roaming between different networks.
- Maintain registration with Cisco Unified Communications Manager in the case of network connectivity loss.
- Seamlessly transit both active and held calls from one network to another without call drops.

To facilitate connectivity during roaming between networks, Session Persistency allows dynamic IP address/port change via keep-alive registration to facilitate connectivity during roaming between networks. In addition, the feature includes a configurable TCP reconnect timer, which must be enabled at the product level, to allow mobile users to remain connected in case of a temporary network connectivity loss or roaming. The timer is in effect only when the mobile device tears down the original TCP connection explicitly.

To leverage the Session Persistency feature, mobile devices must comply with Cisco-defined SIP interfaces.

TCP Reconnect Timer Configuration

If the TCP reconnect timer has been enabled at the product level, you can configure the timer by setting a value for the Time to Wait for Seamless Reconnect After TCP Drop or Roaming field from any of the following configuration windows:

- Phone Configuration window
- Common Phone Profile window
- Enterprise Phone Configuration window

NextGen Mobile Clients with QoE

If a device that shares the same user identification and is associated with a Hunt Group, signs out of the Hunt Group, then SNR calls are not sent out to the associated mobile device.

Cisco Unified Communications Manager 9.0 extends the Log Out of Hunt Groups capability onto your mobile device. This allows it to function in the same way as your desk phone. When you use the Hlog softkey via your mobile client to Log Out of the Hunt Group, you no longer receive calls placed to the Hunt Pilot.

Cisco Unified Communications Manager 9.0 provides TLS/SRTP support for dual-mode smart phones. TLS establishes the same secure and reliable data transfer mode for mobile phones as for IP phones, and SRTP encrypts voice conversations.

Use Case Scenarios for Cisco Unified Mobility Features

Use cases are provided for the following Cisco Unified Mobility features that are supported by Cisco Unified Communications Manager:

- Mobile Connect
- Mobile voice access
- Time-of-Day access
- Directed Call park via DTMF
- intelligent session control
- session handoff

Use Case Scenarios for Cisco Unified Mobility

Cisco Unified Mobility 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 Cisco Unified Mobility call, users can perform midcall functions, including hold/resume, exclusive hold, transfer, directed call park, and conference.

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.

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 Cisco Unified Mobility 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 Cisco Unified Mobility 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 Cisco Unified Mobility 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.

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.

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.

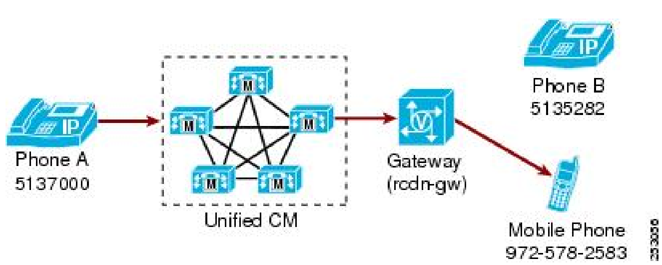
Use Case 1: Reroute Remote Destination Calls to Enterprise Number Service Parameter Is Set to False

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.

The following figure 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 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.

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:

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

Interactions and Limitations

Most standard Cisco Unified Communications Manager features are fully compatible with Cisco Unified Mobility features, except as indicated in the interactions and limitations.

The CMC and FAC feature on Cisco Mobility does not support an alternative number as its DVO callback number. The DVO callback number has to be the number registered in the MI (Mobility Identity) page.

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.

Extend and Connect

The Extend and Connect feature allows users to answer incoming calls on any of their Cisco Unified IP phones or remote destination phones under the control of Cisco Jabber for desktop. However, connected (active) calls cannot be moved between their Cisco Unified IP phone and their remote phone. So one gains application control over the remote phone, but loses mobility features such as being able to move the call back to a Cisco Unified IP phone. This feature requires configuration of CTI Remote Devices.

The Unified Mobility feature allows users to answer incoming calls to their enterprise extension on either their Cisco Unified IP phones or any remote destinations, such as a mobile phone, a home phone, or a hotel phone, etc. Users can move active calls between their Cisco Unified IP phone and their mobile phone without losing the connection. This feature requires configuration of Remote Destination Profiles.

Cisco Jabber for mobile provides telephony, availability, IM, and collaboration in a single integrated smart client. In addition, it also integrates with the native smartphone to provide the entire Cisco Unified Mobility feature set. This combination allows users to communicate seamlessly from their mobile devices when they transit between networks (Wi-Fi or cellular). The intelligence built into the mobility solution, dynamically enables different features as the network changes, eliminating the need for user intervention or preconfiguration (for example, DVO support).

Both of these mobility solutions allow users to communicate as if they are within the enterprise, increasing their reachability and providing the active user the flexibility to a move a call to another device or network once they have changed their location.

Users who need the capabilities of both Unified Mobility and Extend and Connect may configure the same remote destination on the Remote Device Profile and CTI Remote Device types when the Owner ID of both device types is the same. This allows Cisco Mobility features to be used concurrently with Extend & Connect.

Note The ability to configure the same remote destination on both device types is supported using Cisco Unified Communications Manager Release 10 or later.

For more information, see the “Extend and Connect” chapter.

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:

- Cisco Unified Mobility
- 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.

Note For IP Multimedia Subsystem, ensure that the Cisco Unified Mobility feature is enabled in the Remote Destination Configuration window, or by using one of the other methods prescribed for enabling Cisco Unified Mobility, before implementing Intelligent Session Control call processing.

Licensing

Cisco Unified Mobility uses licensing. Checking the Enable Mobility check box in the End User Configuration window triggers licensing to consume device license units (DLUs) for Cisco Unified Mobility; 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 *Cisco Unified Communications Manager Features and Services 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.

Cisco Unified Mobility and SIP Trunks with Cisco Unified Border Element

Cisco Unified Mobility supports the Cisco Unified Mobility 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.

Limitations

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

Call Anchoring

Call anchoring, which is performed based on caller ID, is 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 is handled as part of the Cisco Unified Mobility process.

Call Queuing

Cisco Unified Communications Manager does not support Call Queuing with Cisco Unified Mobility.

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 10 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 is not 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 they 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 be 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 Dual-Tone Multifrequency (DTMF) on a mobile phone to specify the international escape character.

Cisco Unified Mobility does not support + dialing through DTMF for 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 *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 state and the call does not get anchored when:

- DND is enabled with the Call Reject option.
- DND is activated by pressing the DND softkey on the desk phone.

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 10 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 is not 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 over a SIP trunk (either intercluster trunk or gateway), check the Require DTMF Reception check box when configuring the IP phone. This allows DTMF digits to be received out of band, which is crucial for Enterprise Feature Access midcall features.

Enterprise Features in the Global System for Mobile Communications (GSM) That Is Using DTMF

Availability of enterprise features in the Global System for Mobile communications (GSM) that are using DTMF depends on the features that are supported in the third-party smartphones.

Gateways and Ports

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

Cisco Unified Mobility features do not get supported for T1 CAS, FXO, FXS and BRI.

IPv6 Support When Used with Cisco Unified Mobility Advantage

Cisco Unified Mobility does not support IPv6 for mobile clients that are using Cisco Unified Mobility Advantage to connect to Cisco Unified Communications Manager for Dial via office or midcall features. Cisco Unified Mobility Advantage does not support IPv6 addresses.

iPhone-Based Cisco Jabber VoIP Calls

Cisco Mobile devices can support Voice over IP (VoIP) and Dial via Office (DVO) calling schemes, but iPhone-based Cisco Jabber supports only VoIP calls.

Note The Android-based Cisco Jabber client supports both VoIP and DVO.

Jabber Devices are Registered Devices

When initially configured, Jabber devices count as registered devices. These devices increase the count of registered devices in a node, set by the **Maximum Number of Registered Devices** service parameter.

Maximum Wait Timer for Desktop Call Pickup Is Not Applied If User Presses Hold DTMF

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. However, the desk phone does not apply a timer for Desktop Call Pickup. The Resume key continues to display even after the timeout that is configured for the end user to pick up the call elapses and the call is not 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.)

Cisco Unified Mobility Support Restrictions

The Cisco Unified Mobility feature is supported only for Primary Rate Interface (PRI) public switched telephone network (PSTN) connections.

For SIP trunks, Cisco Unified Mobility is supported over IOS gateways or intercluster trunks.

Multilevel Precedence and Preemption (MLPP)

Cisco Unified Mobility does not work with Multilevel Precedence and Preemption (MLPP). If a call is preempted with MLPP, Cisco Unified Mobility features are 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 Cisco Unified Mobility off or on by way of Mobile Voice Access or two-stage dialing do not get saved.

Overlap Sending

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

QSIG

Mobility does not support QSIG.

QSIG Path Replacement

QSIG (Q Signaling) path replacement is not supported.

Remote Destination Profiles

When you configure 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 system 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 Cisco Unified Mobility to use either the default codes for enterprise feature access or the codes that are specified in the smartphone documentation.

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 session handoff from desk phone to mobile phone, the current Remote Destination Pickup method specifies that you must use Send Call to Mobile Phone.
- Only audio call session handoff is supported.

SIP URI and Direct Calls to Remote Destination

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

Video Calls

Cisco Unified Mobility services do not extend to video calls. A video call that is received at the desk phone cannot be picked up on the mobile phone.

System Requirements

Cisco Unified Mobility (formerly 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 Cisco Unified Mobility and Mobile Voice Access, see the applicable Cisco Unified IP Phone Administration Guide and Cisco Unified IP Phone User Guide.

HCS Supplementary Services for VoLTE IMS Mobile Device

Cisco Unified Communications Manager 9.0 supports a native way of invoking the supplementary services. The following supplementary services are supported.

- Originating Identification Presentation
- Terminating Identification Presentation
- Originating Identification Restriction
- Terminating Identification Restriction
- Communication Diversion Unconditional
- Communication Diversion on not Logged in
- Communication Diversion on Busy
- Communication Diversion on not Reachable
- Communication Diversion on No Reply
- Barring of All Incoming Calls
- Barring of All Outgoing Calls
- Barring of All Incoming Calls When Roaming
- Barring of Outgoing International Calls
- Communication Hold
- Communication Retrieve
- 3rd Party Registration
- Message Waiting Indication

- Communication Waiting
- Ad-Hoc Multi Party Conference
- Call Transfer

Originating Identification Presentation

The service control in the originating part is done by the home S-CSCF of the originator of the request. The originating S-CSCF can invoke services on behalf of the requestor.

When the initial inbound INVITE to an ISC trunk has mode set to originating, Cisco Unified Communications Manager acts as the application server for the originating DN. In this scenario, Cisco Unified Communications Manager uses the user portion of the P-Asserted-Id to find the corresponding IMS client. When no such IMS client is found, Cisco Unified Communications Manager rejects the call with a 403 forbidden error. After finding the corresponding IMS client, the call is routed through the enterprise DN configured for the IMS client.

The calling search space used for this call can either be a combination of line and IMS client’s search space or the ISC trunk's, depending on the configuration of the IMS client.

Cisco Unified Communications Manager validates the destination through its DA. If the destination is not routable in the cluster, Cisco Unified Communications Manager will reject the call. Cisco Unified Communications Manager will not alert the destination and will not provide any terminating feature. Once it is determined that the destination is routable, the call is anchored in Cisco Unified Communications Manager and then immediately routed out through the same ISC trunk, bypassing the RouteList or regular SIP trunk.

Note For unknown destinations to allow the IMS network to route to the default network, the Cisco Unified Communications Manager dial plan can have a default route through the ISC trunk for otherwise unknown destinations.

The originating call from the ISC trunk should not invoke Intelligent Session Control. If the mode is originating, CallControl does not fire intercept to Intelligent Session Control even if caller is the IMS client.

Terminating Identification Presentation

The service control in the terminating part is done by the home S-CSCF of the recipient of the request. The terminating S-CSCF can invoke services on behalf of the recipient.

When the initial inbound INVITE to an ISC trunk has the mode set to terminating, Cisco Unified Communications Manager acts as the application server for the terminating DN. In this scenario, Cisco Unified Communications Manager uses the user portion of the RequestURI to find the corresponding IMS client. When the IMS client is found, Cisco Unified Communications Manager will treat the caller as an internal caller. This impacts other feature interactions, such as Forwarding on Busy, Transfer to an external destination, and adhoc terminating.

Unlike when serving as the originating side, Cisco Unified Communications Manager will not reject the call, even if the caller's P-Asserted-Id does not match any IMS client. It will instead be treated as an external trunk call.

When acting as the application server for terminating DN, Cisco Unified Communications Manager will alert the destination and will provide all terminating features.

If the destination includes an IMS client, the outbound INVITE will go through the same ISC trunk logically, but could be on a different node.

Note The terminating call invokes Intelligent Session Control. It is triggered by intercept by CallControl.

Call Forward

Cisco Unified Communications Manager 9.0 supports call forward treatments for the IMS client either through configuration or after a CFA activation request is received over the ISC trunk. The supported forwarding options are:

- CFA
- CF Not Logged In
- CFB
- CF Not Reachable
- CFNA

Call Barring

Cisco Unified Communications Manager 9.0 provides call barring functionality. This feature allows you to block calls in the following ways:

- Barring of All Incoming Calls
- Barring of All Outgoing Calls
- Barring of All Incoming Calls When Roaming
- Barring of Outgoing International Calls

A new section was added to the Phone Configuration page for Call Barring Information. In this section you can select the checkbox to **Block Incoming Call while Roaming** and define the **Home Network ID**.

Note The **Home Network ID** must be defined to enable the **Block Incoming Call while Roaming** feature.

Hold

Cisco Unified Communications Manager supports hold feature invocation through Invite coming in from the ISC interface. Upon receiving the Invite, Cisco Unified Communications Manager will place the active call on hold, and allocate the necessary Music On Hold resource to stream to the held party, if configured. The IMS network triggered hold receives the same treatment as the internal user originated hold operation.

Retrieve

Cisco Unified Communications Manager now supports Retrieve requests over the ISC interface on a held call in the form of Invite with SendReceive SDP. Upon receiving such request, Cisco Unified Communications

Manager will apply its Retrieve call operations, such as remove and de-allocate any Music On Hold resources, and reconnect the media between two parties.

Third-Party Registration

Cisco Unified Communications Manager 9.0 provides a third-party registration feature.

A new checkbox for **Third-party Registration Required** was added to the Protocol Specific Information section.

Message Waiting Indication

Cisco Unified Communications Manager 9.0 supports subscription from the IMS client in the IMS core network through the SUBSCRIBE method. Upon receiving the SUBSCRIBE request from the IMS core, Cisco Unified Communications Manager determines if the requesting client is qualified to receive Message Waiting Indication (MWI) notification by checking the client provisioning data. If the client is qualified, Cisco Unified Communications Manager delivers the cached MWI data to the client upon completing the SUBSCRIBE handling, and continues to deliver the MWI notification if there is any MWI status change under the condition that the subscription is still valid.

Call Waiting

Cisco Unified Communications Manager 9.0 allows the user to select from various call waiting options. If a mobile user has an active call, and a new incoming call arrives the user has the options to:

- Ignore the new incoming call.

  When the user selects this option, the call forwarding treatment may be applied if the forward on busy configuration is set.

- Quit the incoming call.

  When the user selects this option, the call forwarding treatment may be applied if the forward on no answer configuration is set.

- Answer the incoming call.

  When the user selects this option, the original active call is put on hold first, then the new call can be answered.

IMS Client Initiated Ad-Hoc Conference Request

The single user conference initiates with an Invite with a specified conference service request URI. Upon receiving such a service request URI, the conference feature dynamically allocates a number as the conference identifier and registers that with the Cisco Unified Communications Manager internal DA service. The conference feature allocates the conference resource and creates the conference for the user that initiated the conference service request. The dynamically allocated conference identifier number is used to identify the existing conference and allow a new participant to be added to the same conference.

The conference service request URI must be provisioned through a new service parameter within Unified Communications Manager to ensure the correct behavior of the single user conference creation procedure. This provisioning of service parameter must match what is provisioned in the IMS core network. For instance, it can be configured as cucm-conference-factory@cucm1.company.com.

Additional conference participants will ride with a Refer with the existing dialog for all calls respectively. The call info in this Refer has the conference ID that the conference feature allocated during the single user conference creation. The Cisco Unified Communications Manager Refer/Replace feature picks up the task and joins the participant to the existing single user conference. The Refer feature applies the same mechanism to add all of the conference participants.

Note The new conference flows for single user conference creation as well as adding/dropping conference participant are only available when the request is sent from a Cisco Unified Communications Manager provisioned IMS client on the IMS core network. If this is not the case, the request will be rejected.

Transfer

Cisco Unified Communications Manager can handle transfer requests from the IMS core network. The transfer is done through SIP Refer/Replace method in the ISC interface.

Note Calls are put on hold before the transfer is initiated from the IMS client.

HCS Anonymous Call Rejection ISC Trunks

Cisco Unified Communications Manager 9.0 allows the administrator to block incoming calls from anonymous callers. The administrator can choose to block these calls either at the SIP trunk or at the line or DN levels. Calls that are originating from IP phones within the cluster or over other protocols with Calling Line ID Restriction (CLIR) will also get blocked.

There are three configuration options for the anonymous call rejection feature in Cisco Unified Communications Manager. One on the Directory Number page and two on the SIP Profile page.

Directory Number Configuration

To block outgoing anonymous calls for a particular line or DN, this feature can be configured on the Directory Number configuration page for the specific DN. Select the **Reject Anonymous Calls** checkbox on Directory Number page to reject all anonymous calls for the DN.

In the case of an enterprise directory number (DN) that has anonymous call rejection enabled and also has one or more single number reach destinations associated with it, Cisco Unified Communications Manager will block a call from anonymous callers to the enterprise DN and all associated remote destinations.

In the case of an enterprise directory number that has anonymous call rejection enabled and also has a Call Forward All destination, Cisco Unified Communications Manager will forward anonymous calls to the Call Forward All target.

In the case of an enterprise directory number that has anonymous call rejections enabled and also has a call forward on busy destination, Cisco Unified Communications Manager will reject the anonymous call without triggering call forward on busy.

The Call Forward No-Answer feature is not triggered for an anonymous caller.

For Call Transfer - During attended transfer, if the transfer error has CLIR and places a consult call to a transfer-target who has ACR, the consult call will be rejected. Similarly on getting a REFER from anonymous caller, if the Refer-To DN has ACR, the REFER operation will be blocked. In both cases, the consult call will be blocked when the caller has CLIR and called party has ACR.

SIP Trunk Configuration

Configure anonymous call rejection on Cisco Unified Communications Manager to block calls from anonymous callers at the SIP trunk using the SIP Profile page configuration settings. Select the **Reject Anonymous Incoming Calls** and **Reject Anonymous Outgoing Calls** checkboxes on the SIP Profile page. When the **Reject Anonymous Incoming Calls** checkbox is selected, all anonymous incoming calls on the SIP trunk associated this SIP Profile will be rejected. When the **Reject Anonymous Outgoing Calls** checkbox is selected, all anonymous outgoing calls on the SIP trunk associated this SIP Profile will be rejected.

Anonymous calls in SIP are identified based on the criteria described in RFC 5079. Based on RFC 5079, calls are identified to be anonymous when the incoming initial INVITE meets any of the following criteria:

- From or PAI/PPI header with display-name Anonymous
- From header host-portion = anonymous.invalid
- Privacy: id or Privacy: user or Privacy: header [associated with PAI/PPI]
- Remote-Party-ID header has a display-name Anonymous
- Remote-Party-ID header has privacy=uri/full/name

Note For calls that originate from within the Cisco Unified Communications Manager cluster, if the caller's DN or user information is present but caller name is not available or the presentation is restricted, the call is not marked as an anonymous call.

If the caller's DN is not present or the presentation is restricted, regardless of if the caller's name is presented or not, the caller is deemed to be anonymous.

When an anonymous call is rejected by Cisco Unified Communications Manager, it will send SIP error response 433 - Anonymity Disallowed to the initial INVITE. Cisco Unified Communications Manager will also include Q.850 Reason header with cause = 21 (Call Rejected) in 433 response.

Migrate From Cisco Unified Mobility Manager

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 Cisco Unified Communications Manager Bulk Administration Guide.

Cisco Unified Mobility Configuration

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.

End users use the Cisco Unified Communications Self Care Portal windows to further configure or modify the Cisco Unified Mobility settings that apply to their mobile phones.

Tip Administrators should review the summary of all the tasks necessary to configure the Cisco Unified Mobility features that are native to Cisco Unified Communications Manager before proceeding to configure Cisco Unified Mobility.

Related Topics

Configure Cisco Unified Mobility, on page 1

Access List Configuration and Deletion

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

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 *Cisco Unified Communications Manager Administration Guide*.

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 *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.
- Delete the remote destinations that are using the access list that you want to delete.

Related Topics

Access List Member Detail Configuration, on page 41
About Remote Destination Setup, on page 46

Configure Access List

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.

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

Procedure

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 Access List Member Detail Configuration, on page 41.

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:

a) 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.**
b) To delete a filter, select the filter and click **Delete.**
c) 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.
d) 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.
e) To create a new access list with the same members as the existing list, click **Copy.**

Access List Configuration Settings

The following table describes the available settings in the Access List Configuration window.

Table 2: 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.

Field	Description
Blocked	Click this radio button to block calls from member phone numbers from being passed to the remote destinations.
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.
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.

Related Topics

Access List Member Detail Configuration, on page 41

Access List Member Detail Configuration

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.**

The following table describes the available settings in the Access List Member Detail window.

Table 3: Access List Member Detail Configuration Settings

Field	Description
Filter Mask	Select an option from the drop-down list box. You can choose to enter a directory number, filter out calls that do not have caller ID (Not Available), or specify a number that will be allowed or blocked without displaying the caller ID (Private).
DN Mask	If you chose Directory Number in the Filter Mask field, enter a phone number or filter in the DN Mask field. You can use the following wild cards to define a filter: • 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.

Remote Destination Profile Configuration

This section provides information to configure remote destination profiles.

About Remote Destination Profile Setup

In Unified Communications Manager, 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 applies to all remote destinations for the user.

The remote destination profile contains the parameters that apply to all remote destinations for the user. After configuring user accounts for Cisco Unified Mobility (see the *Cisco Unified Communications Manager Administration Guide*), you can create a remote destination profile for the user.

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 *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.

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.

Remote Destination Profile Configuration Settings

The following table describes the available settings in the **Remote Destination Profile Configuration** window.

Table 4: 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.
AAR Calling Search Space	Choose the appropriate calling search space for the remote destination profile to use when automated alternate routing (AAR) is performed. The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth.
User Hold Audio Source	Choose the audio option for users on hold for Cisco Unified Mobility and Mobile Voice Access calls.

Field	Description
Network Hold MOH Audio Source	Choose the audio source from the IOS gateway that provides multicasting audio source for Cisco Unified Mobility 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.
Rerouting Calling Search Space	Choose a calling search space to be used to route Cisco Unified Mobility 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. Unified Communications Manager determines how to route calls based on the remote destination number and the Rerouting Calling Search Space. 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. Cisco Unified Mobility 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 Unified Communications Manager. Cisco Unified Mobility calls get routed to the dual-mode mobility identity number only when the device is outside the enterprise.

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. Ensure the calling search space is not null because no transformations can apply to null partitions. 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, 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. 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 Unified Communications Manager Locale Installer documentation.
Network Locale	From the drop-down list, choose the locale to associate with the remote destination profile. The network locale contains a definition of the tones and cadences that the devices tied to the remote destination profile in a specific geographic area use. Select a network locale that is supported by all of the devices that use this remote destination profile. If you do not choose a network locale, the locale that is specified in the Unified Communications Manager clusterwide parameters as Default Network Locale applies. Choose only a network locale that is already installed and supported by the associated devices. The list contains all available network locales for this setting, but not all are necessarily installed.

Field	Description
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.
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.

Associate 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 to configure a directory number in 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 re-associate it.

About Remote Destination Setup

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 Cisco Unified Mobility 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, which 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.

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.

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

Remote destinations represent phones that are available for Cisco Unified Mobility 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.

Tips About Configuring Remote Destinations

End users can create their own remote destinations in the Cisco Unified Communications Self Care Portal. For information about how to perform this task, see the user guide for the phone model.

Be aware that the appropriate timer settings in the following table 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 Cisco Unified Mobility 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.

Remote Destination Configuration Settings

Field	Description
Remote Destination Information	
Mobile Identity Information	

Field	Description
Name	Enter a name that identifies the remote destination or mobile identity.
Destination Number	Enter the PSTN 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. If the administrator configures the Incoming Calling Party settings in the 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. **Note** Add the necessary translation pattern or route patterns to route the destination number. You can also enter a directory URI in this field. Keep in mind that if you enter a directory URI in this field, you must also configure a domain-based SIP route pattern. **Note** When you place a call from a remote destination, the caller ID of the destination phone displays the directory number that is associated with the calling directory URI rather than the directory URI.
Single Number Reach Voicemail Policy	Configures how mobile device users answer calls that terminate on a remote destination (RD). This feature provides users with a single enterprise voice mail box for their enterprise mobility if the RD call reaches an external voice mail system. Available options are as follows: • Use System Default • Timer Control • User Control **Note** For User Control to work, you must set the Enable Enterprise Feature Access service parameter to TRUE.
Dial-via-Office Reverse Voicemail Policy	Configures how dual mode device users answer Dial-via-Office Reverse (DVO-R) calls that terminate on the Mobile Identity (MI). This feature provides users with a single enterprise voicemail box for their enterprise mobility if the RD call reaches an external voice mail system. Available options are as follows: • Use System Default • Timer Control • User Control

Field	Description
Answer Too Soon Timer	Enter the minimum time in milliseconds that 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, Unified Communications Manager pulls the call back to the enterprise. Range: 0 - 10,000 milliseconds Default: 1,500 milliseconds
Answer Too Late Timer	Enter the maximum time in milliseconds that Unified Communications Manager allows for the mobile phone to answer. If this value is reached, Unified Communications Manager stops ringing the mobile phone and pulls the call back to the enterprise. Range: 0 and 10,000 - 300,000 milliseconds Default: 19,000 milliseconds If the value is set to zero, the timer is not started.
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, choose the remote destination profile that you want to use for this remote destination.
Mobility Profile	From the drop-down list, 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.
Dual Mode Phone	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.

Field	Description
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 nor to dual-mode phones that are running SCCP, such as the 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. For more information, see the "Cisco Mobility" and "Extend and Connect" chapters in the Feature Configuration Guide for Cisco Unified Communications Manager
When Cisco Unified Mobility Is Enabled	
Ring Schedule	
All the time	If the Enable Cisco Unified Mobility 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 Cisco Unified Mobility 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 Cisco Unified Mobility 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.

Field	Description
Time Zone	From the drop-down list, 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 Cisco Unified Mobility check box is checked for this remote destination.
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 Cisco Unified Mobility check box is checked for this remote destination. From the drop-down list, 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 Cisco Unified Mobility 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 Cisco Unified Mobility to work for this remote destination. **Note** Be aware that the line association check box of a line must be checked for Cisco Unified Mobility calls to ring this remote destination when a call comes into the directory number that is assigned to that line.

FMC Over SIP Trunks Without Smart Client

Cisco Unified Communications Manager allows service providers to provide base PBX-extension features such as enterprise dialing, SNR, single VM, call move, and mid-call features via the trunk without a smart client on the mobile. Basic mobile features such as Single Number Reach, Deskphone pickup, Send Call to Mobile, Mobile Voice Access and Mid-call DTMF features are supported. Extension dialing is supported if it is implemented in the network and the network is integrated with Cisco Unified Communications Manager. These features can be provided by any type of trunk.

With previous versions of Cisco Unified Communications Manager, service providers used the Remote Destination feature to deliver network-based FMC including the enterprise dialing/DVO feature without a client. This version allows for a new device type called Carrier-Integrated Mobile to deliver network-based FMC via the trunk or gateway.

When configuring the new device type Carrier-Integrated Mobile, set the Owner User ID value to the mobile user identity. The mobile user identity does not appear on the configuration page. Only end users with mobility enabled will appear in the Owner User ID drop-down on the end user page. Only one line (DN) can be associated with an FMC device. Users should associate a mobile identity with the FMC. This can be done on the FMC device configuration page after the device has been added. For calls to be extended to the number of the mobile identity, users must enable Cisco Unified Mobility on the Mobile Identity window.

Cisco Unified Communications Manager can be configured in the Ring All Shared Lines service parameter so that the shared-line is rung when mobile DN is dialed.

Note The Reroute Remote Destination Calls to Enterprise Number feature must be enabled for Ring All Shared Lines to take effect. Reroute Remote Destination Calls to Enterprise Number is disabled by default.

IMS shared lines will ring solely based on the value of the Ring All Shared Lines parameter. In previous versions of Cisco Unified Communications Manager, IMS shared lines rang based on the value of Reroute Remote Destination Calls to Enterprise Number.

You can also migrate from the Remote Destination feature used in previous versions to this new device type.

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 Mobile Voice Access Configuration, on page 53.

Step 3 Click **Save.**

Mobile Voice Access Configuration

The following table describes the available settings in the Mobile Voice Access window.

Table 5: 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. **Note** The Mobile Voice Access Directory Number field is required only for legacy Mobile Voice Access where the gateway provides the IVR resource. For native Mobile Voice Access, Cisco Unified Communications Manager provides the IVR. In this case, you do not need to configure a Mobile Voice Access Directory Number.
Mobile Voice Access Partition	From the drop-down list, 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 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 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>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Selected Locales</td><td>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.</td></tr>
</table>

Gateway Configuration for Enterprise Feature Access

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

Configure an H.323 or SIP Gateway

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 *Cisco Unified Communications Manager Administration Guide*.

Note When a Cisco Unified Mobility 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 Cisco Unified Mobility application with system remote access.

Sample configuration for IOS 12.3(13) and later:

- dial-peer voice 58888 pots
- service CCM (Cisco Unified Mobility VXML application)
- incoming called-number 58888

Sample configuration for IOS 12.3(12) and earlier:

- dial-peer voice 100 pots
- application CCM (Cisco Unified Mobility 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, on page 52.

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

Configure an H.323 Gateway for System Remote Access

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 *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 the Cisco Unified Mobility 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, on page 52.

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.

Configure Enterprise Feature Access Two-Stage Dialing

Use this procedure to configure enterprise feature access two-stage dialing.

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.

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:

a) Set the Enable Enterprise Feature Access service parameter to True.
b) 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.
c) 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.

Mobility Enterprise Feature Configuration

This section provides information about mobility enterprise feature configuration.

About Mobility Enterprise Feature Setup

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.

Mobility Enterprise Feature Configuration Settings

The following table describes the available settings in the Mobility Enterprise Feature Configuration window.

Table 6: 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.

Field	Description
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.

Handoff Mobility Configuration

This section provides information about handoff mobility configuration.

About Handoff Mobility Setup

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.

Handoff Mobility Settings

The following table describes the available settings in the Handoff Mobility Configuration window.

Table 7: 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.

Mobility Profile Configuration

This section provides information about mobility profile configuration.

About Mobility Profile Setup

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 mobile identity or with a dual-mode mobile identity. Standard, single-mode remote destinations cannot associate with a mobility profile.

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 You 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:

3. Default EFA DN
4. Default service access number

Also consider the following requirements when you configure mobility profiles:

- You must 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 are retrieved from the mobility profile and must match in the mobility profile, or both default values are retrieved and the default values must match.

Mobility Profile Configuration Settings

The following table describes the available settings in the Mobility Profile Configuration window.

Table 8: 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	

Field	Description
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.
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.

Toll Bypass Optimization for Handoff

The Least Cost Routing (LCR) and Dialed Number Identification Service (DNIS) pool features were introduced as part of the Cisco Unified Communications Manager 8.5 release. These features led to reduced costs for Dial Via Office (DVO) calls by providing call routing based on the area, location, and region. Cisco Unified Communications Manager release 8.6.(1) leverages the LCR-DNIS feature to invoke Handoff. Toll Bypass Optimization for Handoff uses the Enterprise Feature Access Number configured in the Mobility Profile associated with the Mobile Identity. Using this feature eliminates the need for a separate Handoff DID to be configured, which can also result in cost savings. When a user needs to invoke legacy Handoff, the client must dial the administrator configured Handoff DID number, which would be an international call placed to the Handoff DID number in roaming scenarios, which incurs additional costs to the enterprise.

Cisco Mobile Clients that are registered with a release previous to 8.6.(1) of Cisco Unified Communications Manager will continue to have the legacy Handoff invocation. For more information see, Session Handoff, on page 17.

Toll Bypass Optimization for Handoff Dial Via Office - Forward (DVO-F)

Enable DVO-F for all handoff calls between cellular and WiFi to leverage LCR policies for cost savings. Mid-call features can be triggered after handoff.

To configure LCR enabled handoff for DVO-F, perform the following procedures:

1. Configure an Enterprise Feature Access Number. For more information, see About Mobility Enterprise Feature Setup, on page 60.
2. Configure a Handoff DN. For more information, see Handoff Mobility Configuration, on page 61.
3. Create a Mobility Profile Associated with the Mobile Identity with the Mobile Client Calling Option set to DVO-F. For more information, see Mobility Profile Configuration, on page 61.

Toll Bypass Optimization for Handoff Dial Via Office - Reverse (DVO-R)

Enable DVO-R for all handoff calls between cellular and WiFi to leverage LCR policies for cost savings. Mid-call features can be triggered after handoff.

To configure LCR enabled handoff for DVO-R, perform the following procedures:

1. Configure an Enterprise Feature Access Number. For more information, see About Mobility Enterprise Feature Setup, on page 60.
2. Create a Mobility Profile Associated with the Mobile Identity the Mobile Client Calling Option set to DVO-R. For more information, see Mobility Profile Configuration, on page 61.

Unified Application Dial Rule Configuration for Mobility

Cisco Unified Communications Manager 8.5 and earlier versions, required that Application Dial Rules be configured locally on the client side for VoIP calls and separately in Cisco Unified Communications Manager for DVO calls. To simplify configuration for both VoIP and DVO calls, Cisco Unified Communications Manager 8.6(1) allows Application Dial Rule configuration to apply to DVO as well as VoIP calls, so that there is no separate client configuration required. This allows mobile users to make calls with both the enterprise dial plan or service provider dial plan regardless of the transports and provides a consistent way to manage dial plans. When a client makes a call in either VOIP or DVO mode, the same rule applies. Mobility uses the Application Dial Rules in such a way that the client can dial a 10-digit number in VoIP mode to call an external number as it does in DVO mode.

Note VoIP mode is applicable to only SIP based mobile clients using enbloc dialing and cannot be applied to SCCP based mobile clients using overlap dialing.

This feature uses existing Application Dial Rule configuration and Mobility is treated as an application. For more information about Dial Rules, see the Cisco Unified Communications Manager System Guide. For more information about Application Dial Rule configuration, see the Cisco Unified Communications Manager Administration Guide.

Application Dial rules are shared by all applications. Ensure that the Application Dial rules you configure for Mobility do not conflict with Application Dial rules shared among other applications.

Mobility Softkey Configuration

Note Do not configure the Mobility softkey and the MOVE softkey together.

Follow this procedure to configure a Mobility softkey for the phone user that uses Cisco Unified Mobility.

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 the Cisco Unified Communications Manager Administration Guide.

Step 11 Choose the Owner User ID for the Cisco Unified Mobility phone user.

Step 12 Click **Save**.

Cisco Jabber for Mobile

This chapter provides information about functionality for Cisco Mobile VoiP Clients which connect directly with Cisco Unified Communications Manager. This chapter discusses the features and the required configurations.

Cisco Mobile VoiP Clients register directly with Cisco Unified Communications Manager

Cisco Mobile is the name given to a family of clients that run on mobile devices. Different Cisco Mobile clients offer different features. Features may include the following:

- Direct connection from Cisco Unified Communications Manager to mobile client without proxy server

- Dial-via-Office (DVO) optimization settings for toll reduction
- Enable/disable Cisco Unified Mobility from mobile phone
- Dial-via-Office Reverse Callback
- Dial-via-Office Forward
- Ability to transfer active Dial-via-Office calls between the mobile device and the desktop phone

See the following documentation for details about configuring Cisco Unified Mobility and Cisco Mobile VoiP Clients:

- End-user guides for Cisco Mobile VoiP Clients.
- End-user guide for a particular Cisco Unified IP Phone for procedures that end users follow to configure the Cisco Unified Mobility settings for their phones by using the Cisco Unified Communications Self Care Portal windows.

Configuration for Cisco Mobile VoiP Clients

See the Cisco Mobility installation guide for complete configuration instructions for Cisco Mobile VoiP Clients.

For more information on Cisco Unified Mobility features that are available upon configuration of the Cisco Unified Mobility Advantage server, see the List of Cisco Mobile VoiP Client Features, on page 68.

Cisco Mobile VoIP Clients

This section provides information about Cisco Mobile VoIP clients.

Be aware that special configuration in Cisco Unified Communications Manager Administration is required for features that Cisco Mobile VoIP Clients provide.

Terminology

The following table provides definitions of terms that are related to Cisco Unified Mobility with Cisco Mobile VoiP Clients.

Table 9: Definitions

Term	Definition
Cisco Mobile 8.x	These direct-connect dual-mode clients support voice-over-Wi-Fi (for costing savings) in addition to cellular. They connect to Cisco Unified Communications Manager directly without the need of a proxy server.

List of Cisco Mobile VoiP Client Features

This section provides a list of Cisco Unified Mobility features that are available to mobile phone users when the Cisco Mobile VoiP Client has been configured. This material discusses configuration within Cisco Unified Communications Manager Administration.

The following entities and features require configuration of Cisco Unified Mobility in Cisco Unified Communications Manager Administration:

- Direct connection from Cisco Unified Communications Manager to mobile client without proxy server - This feature provides server-side support for Cisco Mobile VoiP Clients to connect to Cisco Unified Communications Manager directly and thus eliminate Cisco Unified Mobility Advantage in the deployment. Cisco Unified Communications Manager adjusts to support direct connection with the Cisco Mobile VoiP Client.
- DVO Optimization Settings for Toll Reduction - This feature supports a pre-configured policy to determine which mobile origination call (DVO-R or DVO-F) yields the least cost to the enterprise; this determination is typically based on locations. Administrators assign a profile based on the user location and any other available information. Least cost routing negotiates with Cisco Unified Communications Manager to determine whether DVO-R or DVO-F generates the least cost, then chooses the less costly method for making the call.
- Enable/Disable Cisco Unified Mobility From Mobile Phone - This feature allows the Cisco Mobile VoiP Client to change the Cisco Unified Mobility status dynamically and keep the Cisco Unified Mobility Status between Cisco Unified Communications Manager and the client in sync. This feature provides the flexibility to the end user: the end user can change the user Cisco Unified Mobility status from the user mobile phone, not just from the GUI website.

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

- Cisco Unified Mobility
- Desktop Call Pickup
- Access List

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

- Midcall Enterprise Feature Support Using DTMF
- Dual-mode Phone Support
- Manual Handoff of Calls on a Dual-mode Phone
- Time-of-Day Access
- Directed Call Park via DTMF
- SIP URI Dialing

See topics related to the benefits of Cisco Unified Mobility features for a discussion of other benefits of Cisco Unified Mobility features, such as simultaneous desktop ringing, single enterprise voice mailbox, system remote access, caller ID, remote on/off control, call tracing, security and privacy for Cisco Unified Mobility calls, and smartphone support.

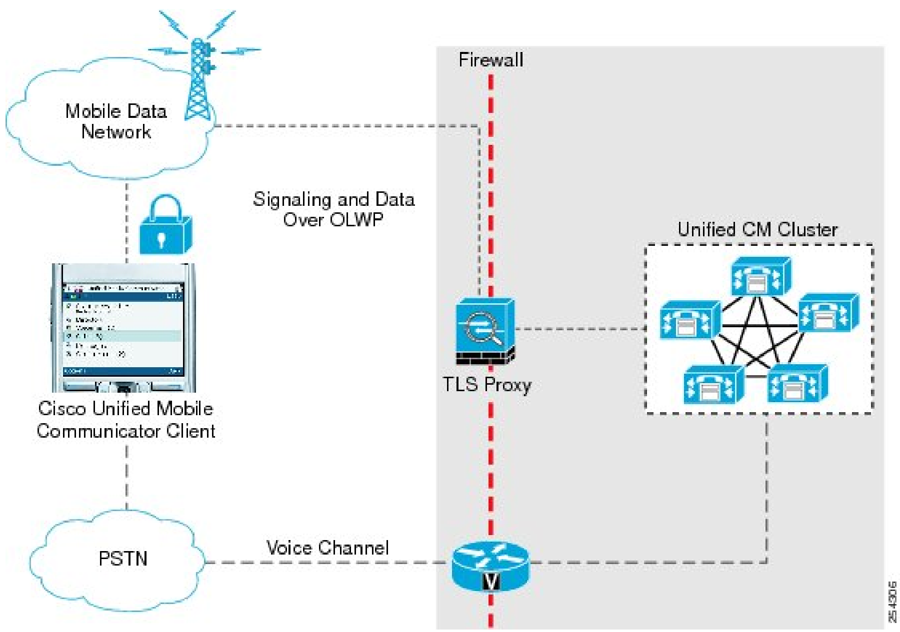
Related Topics

Benefits of Cisco Unified Mobility Features, on page 6
Cisco Unified Mobility, on page 1
Direct Connection From CUCM to Mobile Client, on page 69
DVO Optimization Settings, on page 70
Enable or Disable Cisco Unified Mobility From Mobile Phone, on page 70
Cisco Unified Mobility, on page 7

Direct Connection From CUCM to Mobile Client

Registration between the Cisco Mobile VoiP Client and Cisco Unified Communications Manager takes place over a separate TCP port. (The shared or pooled connection that was used by the Cisco Unified Mobility Advantage server is not used.) Keepalive messages between the Cisco Mobile VoiP Client and Cisco Unified Communications Manager remain the same as those passed between Cisco Unified Communications Manager and Cisco Unified Mobility Advantage. Cisco Mobile VoiP Client registration with Cisco Unified Communications Manager introduces no new alarms, and registration takes place over the SIP channel.

Figure 2: Cisco Mobile VoiP Client Registration with Cisco Unified Communications Manager



If the client is running on the iPhone and the Cisco Mobile VoiP Client is unable to complete the SIP dialog, the Cisco Unified Communications Manager retains the PSTN call. (The PSTN call does not drop even if the SIP stat times out.) For example, if Cisco Unified Communications Manager does not receive an ACK message after it sends a 200 OK message, the PSTN call gets retained.

Limitation for Direct Connection From Cisco Unified Communications Manager to Mobile Client

This feature specifies the following limitation:

- If the SIP dialog between Cisco Unified Communications Manager and the Cisco Mobile VoiP Client is not complete, the dialog cannot be used for further midcall feature invocations. The user can, however, invoke midcall features through the DTMF interface.

DVO Optimization Settings

This feature supports a pre-configured policy to determine which mobile origination call (DVO-R or DVO-F) yields the least cost to the enterprise; this determination is typically based on locations. This feature benefits the mobile user by allowing the user to find the least cost when making a mobile call. The DNIS pool provides a list of Direct Inward Dialing (DID) numbers so that the user, if roaming, can choose a non-international number for the mobile call. Least cost routing negotiates with Cisco Unified Communications Manager to determine whether DVO-R or DVO-F generates the least cost, then chooses the less costly method for making the call.

Reasons for Least Cost Routing and DNIS Pool

The following reasons make this feature desirable:

- Administrator can decide upon the DVO call type, DVO-F or DVO-R, for least cost call routing. In certain regions and with certain service providers, DVO-F can be more economical for mobile users; in other regions, DVO-R can be more economical. For example, in regions where incoming calls are free for mobile phone users, configuring a DVO-R call for mobile phone users achieves least cost call routing.
- Scalability - Multiple users in a given region can use a single mobility profile, which comprises region, service provider, location, and so forth. Here, “users” refers to the clients under actual end users. The administrator does not need to create a mobility profile for each end user.
- Single DID within a cluster for all DVO-F calls - For such DVO-F calls, the client makes an incoming call to Cisco Unified Communications Manager by using a particular DID.
- Multisite cluster - For a multisite cluster, a client in cluster A (such as the UK) uses the DID of cluster B (such as San Jose) for DVO-F calls, which incurs costs.
- DVO-R - Trunk allows calls that originate from a local DID. At times, when a client makes an outgoing DVO-R call, the client trunk may not allow an outgoing call if the caller ID does not lie in a specific range. For example, if a UK client invokes DVO-R, the callback call from the trunk at the San Jose cluster shows 408. When this call reaches the UK, the service provider trunk may not recognize the 408 and therefore not allow the call. Therefore, the caller IDs need to specify the local identifiable values.

Characteristics of DVO Optimization Settings for Toll Reduction

This feature involves the use of mobility profiles, which the administrator configures by using the Call Routing > Mobility > Mobility Profile menu path in Cisco Unified Communications Manager Administration. See the Mobility Profile Configuration, on page 61 for additional details about mobility profiles.

The DVO Optimization Settings for Toll Reduction feature does not change the alternate callback mechanism that DVO-R calls use: the client continues to control alternate callback.

Limitation of DVO Optimization Settings for Toll Reduction

The DVO Optimization Settings for Toll Reduction feature specifies the following limitation:

- Least Cost Routing (LCR) rules are applied after application dial rules. Called party transformations and call forward scenarios do not get considered for LCR.

Enable or Disable Cisco Unified Mobility From Mobile Phone

The Cisco Mobile VoiP Client can update its Cisco Unified Mobility status directly.

Interactions and Limitations

Be aware that most standard Cisco Unified Communications Manager features are fully compatible with Cisco Unified Mobility features. See the chapter for Cisco Unified Mobility for details of any exceptions.

Related Topics

Cisco Unified Mobility, on page 1
Interactions, on page 26
Limitations, on page 28

System Requirements

See the Cisco Mobile release notes for detailed system requirements.

Configure Cisco Mobile VoiP Clients

For details about configuring the Cisco Mobile VoiP Clients, see the configuration guides for Cisco Mobile VoiP Clients.