# Cisco Unified Mobility


- Cisco Unified Mobility Overview, on page 1
- Cisco Unified Mobility Prerequisites, on page 3
- Cisco Unified Mobility Configuration Task Flow, on page 4
- Cisco Unified Mobility Call Flow, on page 27
- FMC Over SIP Trunks Without Smart Client, on page 27
- Hunt Group Login and Logout for Carrier-Integrated Mobile Devices, on page 28
- Cisco Unified Mobility Interactions, on page 29
- Cisco Unified Mobility Restrictions, on page 30
- Cisco Unified Mobility Troubleshooting, on page 34


# Cisco Unified Mobility Overview

Cisco Unified Mobility offers a set of mobility-related features that allow users to interact with Unified Communications applications no matter where they may be, or which device they are using. Whether the device you are using is a home office phone, a dual-mode Cisco Jabber on iPhone or Android client over a WiFi connection, or a mobile phone from another cellular provider, you can still access Unified Communications features and have the call be anchored in the enterprise.

For example, you can answer a call that is directed to your enterprise number from any of your configured phones and then transfer the call to your mobile phone, allowing you to continue an in-progress conversation as you are leaving the office.

### Benefits of Cisco Unified Mobility

Most of the mobility features offer call anchoring within the enterprise–even if the call is placed to or from a mobile device, the call is routed through an enterprise gateway.

This provides the following benefits:

- Single enterprise phone number and voicemail for all business calls, regardless of which device you are using, and whether you are in the office or out of the office.
- Ability to extend business calls to a mobile device and have the call still be handled as if it were your office phone.
- Calls placed from mobile devices are anchored to the enterprise and routed through an enterprise gateway. This provides access to UC mid-call features, centralized billing and call detail records, and potential cost savings from avoiding expensive cellular networks.

- Ability to roam from one network to another and have the call not be dropped.

# Mobility Features

Cisco Unified Mobility offers the following mobility-related features:

| Mobility Feature | Description |
|---|---|
| Single Number Reach | Provides you with a single enterprise phone number and voicemail by which a caller can reach you, regardless of whether you are in the office or outside the office. When someone dials your enterprise number, you can answer the call from your desk phone, or from any of your configured remote destinations (for example, a home office phone, a dual-mode Cisco Jabber on iPhone or Android client, and even a mobile phone from another provider) . |
| Move to Mobile | Allows you to transfer an active call from your desk-phone to a mobile device that is configured as a remote destination by pressing the **Mobility** softkey on your Cisco IP Phone. It is associated with Single Number Reach as a part of the Remote Destination configuration.<br><br>Similar to the **Move to Mobile** option is the **Desk Pickup** option, which fits the example where you are on a mobile call and are just arriving at the office. You can hang up on the call on your mobile device and immediately resume the call by picking up your desk phone before the **Maximum Wait Time for Desk Pickup** timer expires (the default is 10 seconds). This option is enabled as part of your Single Number Reach configuration.<br><br>• Ensure that you set the **Enforce Privacy Setting on Held Calls** Service Parameter to False.<br><br>• You can also use the `Enterprise Feature Access` code and the `Session Handoff` codes to transfer calls between your remote destinations and desk phone. |
| Mobile Voice Access | Allows you to place calls from any remote phone and have the call be anchored in the enterprise and presented to the called party as if you had called from your office phone. When using this feature, you must dial in to a system interactive voice response from your mobile device. After authenticating you, and prompting you for the call destination, the system places the call as if you had called from your enterprise phone.<br><br>You can also use **Mobile Voice Access** prompts to enable or disable **Single Number Reach** for a remote destination. |
| Enterprise Feature Access<br><br>. | Provides two-stage dialing from a configured remote destination. Also, ensures that the call that is presented to the called party appears as if it originated from your desk phone. Unlike **Mobile Voice Access**, to use **Enterprise Feature Access**, you must be dialing from one of your configured remote destinations.<br><br>**Enterprise Feature Access** also allows you to access mid-call features while on a call from a remote destination. You can access mid-call features by sending DTMF digits that represent the codes for the various features such as Hold, Exclusive Hold, Transfer. |

| Mobility Feature | Description |
|---|---|
| Intelligent Session Control | Enables automatic call anchoring for enterprise-originated calls that are placed directly to configured remote destination numbers (for example, an enterprise-originated call to a cell phone number that is configured as a remote destination). By configuring a service parameter, you can have the system redirect those calls automatically to the associated enterprise number, providing cost savings and added UC functionality. |
| Dual-Mode Phones | Cisco Jabber on iPhone and Android clients can be provisioned as dual-mode devices. **Dual-Mode phones** have the capability of connecting over Wi-Fi or through cellular networks. When the client is within the enterprise network, Cisco Jabber can register to Unified Communications Manager over Wi-Fi, and has UC calling and instant messaging functionality. If you configure a mobile identity with the phone number of the mobile device, allowing the call to be transferred from Jabber to the cellular device when leaving the enterprise network.<br>**Note** An added feature that is available to Cisco Jabber mobile clients is Mobile and Remote Access, which allows Cisco Jabber clients to connect to data networks when outside of the enterprise network. For more information, see "*Configure Mobile and Remote Access*" section in Feature Configuration Guide for Cisco Unified Communications Manager. |

# Cisco Unified Mobility Prerequisites

Refer to the following prerequisites:

- Enabling Mobility features requires proper planning to ensure that your dial plan and call routing configuration can handle the deployment needs. For more information, see "*Mobile Collaboration*" section in the *Cisco Collaboration System Solution Reference Network Designs* guide.
- For information on which Cisco IP Phones support Mobility feature, see Generate a Phone Feature List.
  - For a list of Cisco IP Phones that support the Mobility softkey, run a report for the **Mobility** feature.
  - For a list of supported dual-mode phones, run a report for the **Dual-Mode** feature.
- If you are deploying Mobile Voice Access and you want to make additional locales available to your system (if you want to use non-English phone locales or country-specific tones), you can download the locale installers from cisco.com and install them through the Cisco Unified OS Administration interface. For more information on installing locales, see Installation Guide for Cisco Unified Communications Manager and the IM and Presence Service.
- Configure Self-Provisioning so that phone users can provision their own Cisco Jabber clients and remote destinations. For more information, see "*Configure Self Provisioning*" and "*Provisioning End Users*" section in the System Configuration Guide for Cisco Unified Communications Manager.

**Caution** The Cisco mobility solution is verified with only Cisco equipment. This solution may also work with other third-party PSTN gateways and Session Border Controllers (SBCs), but the features might not work as described here. If you are using this solution with third-party PSTN gateways or SBCs, Cisco technical support may not be able to resolve problems that you encounter.

# Cisco Unified Mobility Configuration Task Flow

Complete these tasks to configure Mobility features for your deployment.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Perform one of the following:<br>• Configure a Mobility User, on page 5<br>• Configure Mobility Users Through Bulk Administration, on page 6<br>• Provision Mobility Users Through LDAP, on page 6 | Adds mobility features for an individual end user.<br>Configures Mobility features for a large number of existing end users, use the Bulk Administration Tool.<br>Provisions new users with mobility functionality, you can use a feature group template and LDAP sync. |
| **Step 2** | Configure Mobility for IP Phones, on page 7 | Configures Cisco IP Phones for Mobility including setting up the Single Number Reach (SNR) and Move to Mobile features. This allows enterprise phone users to extend enterprise calls to a wide range of mobile devices, including a home office phone or a mobile phone. |
| **Step 3** | Configure Mobile Voice Access, on page 12 | **Optional**. Provides a system IVR so that mobile users can call from any mobile device and have the call that is presented to the called party as if the caller were dialing from their enterprise desk phone. |
| **Step 4** | Configure Enterprise Feature Access, on page 19 | **Optional**. Provides two-stage dialing from a configured remote destination and have the call that is presented to the called party as if it originated from a desk phone. This feature also allows you to access mid-call features while on a call from a remote destination. |
| **Step 5** | Configure Intelligent Session Control, on page 20 | Configure the system so that inbound calls to a remote destination are rerouted to an associated enterprise, if one is available. This provides automatic call anchoring within the enterprise |

| | Command or Action | Purpose |
|---|---|---|
| | | for mobility calls, providing cost savings and added Unified Communications functionality. |
| **Step 6** | Configure Mobility Service Parameters, on page 21 | **Optional**. Configure optional mobility-related service parameters if you want to change the behavior of Cisco Unified Mobility. |
| **Step 7** | Configure Cisco Jabber Dual-Mode, on page 21 | Configure Cisco Jabber for mobility so your users can access enterprise communications features through a Jabber client on their smartphone. |
| **Step 8** | Configure Other Dual-Mode Devices, on page 22 | Complete this task flow if you want to deploy other dual-mode devices, such as FMC or IMS clients that can connect through Wi-Fi. |

# Configure a Mobility User

Use this procedure to configure an end user with the mobility feature.

### Procedure

**Step 1** From Cisco Unified CM Administration, choose **User Management** > **End User**.

**Step 2** In **Find and List Users** window, perform one of the following tasks:

- Click **Find** and select an existing user to modify the settings.
- Click **Add New** to configure a new user.

**Step 3** Configure values for the following fields:

- **User ID**
- **Last Name**

**Step 4** In the **Mobility Information** area, complete the following fields:

a) Check the **Enable Mobility** check box.

b) **Optional**. Check the **Enable Mobile Voice Access** check box to allow this user to use Mobile Voice Access.

c) In the **Maximum Wait Time for Desk Pickup** field, enter a value in milliseconds. After hanging up a call from a remote destination, this timer represents the amount of time where the user still has the option of resuming the call from a deskphone.

d) In the **Remote Destination Limit** field, enter the number of remote destinations that a user is permitted to have for single number reach (SNR) targets.

**Step 5** Complete the remaining fields in the **End User Configuration** window. For more information on the fields and their configuration options, see Online Help.

**Step 6** Click **Save**.

# Configure Mobility Users Through Bulk Administration

Use this procedure to use Bulk Administration's **Update Users** menu to add the Mobility feature to existing end users by bulk.

**Note** Bulk Administration contains other features that allow you to update existing users by bulk. For example, you can use the Export and Import functions to import a CSV file with the new Mobility settings. For more information, see the Bulk Administration Guide for Cisco Unified Communications Manager.

### Procedure

**Step 1** From Cisco Unified CM Administration, choose **Bulk Administration** > **Users** > **Update Users** > **Query**.

**Step 2** Apply the filter and click **Find** to select the users whom you want to assign as mobility users.

**Step 3** Click **Next**.

**Step 4** In the **Mobility Information** area, modify the following four fields by first checking the check box on the far left to indicate that this field is to be updated, and then configuring the setting on the right as follows:

- **Enable Mobility**—Check this check box to enable the users provisioned with this template for Mobility features.
- **Enable Mobile Voice Access**—Check this check box for provisioned users to be able to use Mobile Voice Access.
- **Maximum Wait Time for Desk Pickup**—This field represents the amount of time, after hanging up a call on a mobile phone, that you have to resume the call on your desk phone.
- **Remote Destination Limit**—This field represents the number of Remote Destinations and Mobile Identities that you can assign to users whom are provisioned through this template.

**Step 5** Under **Job Information**, check **Run Immediately**.

**Step 6** Click **Submit**.

# Provision Mobility Users Through LDAP

If you have not yet synced your LDAP directory, you can use this procedure to configure synced end users with mobility capability through the Feature Group Template configuration. Newly synced users inherit the mobility settings from the template.

**Note** This method works only if you have not yet synced your LDAP directory. You cannot assign new feature group template configurations to an LDAP directory sync after the initial sync has occurred.

### Procedure

**Step 1** From Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **Feature Group Template**.

**Step 2** In the **Find and List Feature Group Templates** window, perform one of the following:

- Click **Add New** to configure a new template.
- Click **Find** and select an existing template to configure.

**Step 3** Assign a **Name** to the template.

**Step 4** Configure the following Mobility fields:

- **Enable Mobility**—Check this check box to enable the users provisioned with this template for Mobility features.
- **Enable Mobile Voice Access**—Check this check box for provisioned users to be able to use Mobile Voice Access.
- **Maximum Wait Time for Desk Pickup**—This field represents the amount of time in milliseconds, after hanging up a call on a mobile phone, that you have to resume the call on your deskphone.
- **Remote Destination Limit**—This field represents the number of Remote Destinations and Mobile Identities that you can assign to users whom are provisioned through this template.

**Step 5** Configure the remaining fields in the **Feature Group Template Configuration** window. For more information on the fields and their configuration options, see Online Help.

**Step 6** Click **Save**.

**Note** Assign the configured Feature Group Template to an LDAP Directory that has not yet been synced. Newly synced users have Mobility enabled. For more information, on provisioning users through LDAP see "*Provisioning End Users*" chapter in System Configuration Guide for Cisco Unified Communications Manager.

# Configure Mobility for IP Phones

Complete these tasks to configure mobility features for Cisco IP Phones. This includes setting up Single Number Reach (SNR) and the Move To Mobile feature. This provides users with a single enterprise number that rings all their devices, in addition to an enterprise-level voicemail that can be reached no matter which device rings. And also, users are able to transfer active calls between their deskphone and mobile device.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Configure Softkey Template for Mobility, on page 8 | Configures a mobility softkey template for Cisco IP Phones that includes the Mobility softkey. Users can transfer calls from their deskphone to a mobile phone by pressing the softkey. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | Configure IP Phone for Mobility, on page 10 | Configures an IP phone for mobility so that incoming calls to an enterprise number are extended to remote destinations. |
| **Step 3** | Configure a Remote Destination Profile, on page 10 | Configures common settings that you want to apply to all the remote destination numbers for a user. |
| **Step 4** | Configure a Remote Destination, on page 11 | Configures a remote destination that is a virtual device that represents a mobile device where the user can be reached (for example, a home office phone, or a mobile phone on a cellular network). The remote destination carries many of the same settings as the user's desk phone. |
| **Step 5** | Configure an Access List, on page 12 | **Optional**. Controls which calls can ring which remote destinations, and at which times of day. The access list filters callers based on the Caller ID and can either allow calls or block calls from the caller during that remote destination's ring schedule. |

## Configure Softkey Template for Mobility

Use this procedure to configure a softkey template that includes the **Mobility** softkey. The softkey will be enabled for all phones that use this template.

### Procedure

**Step 1** From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Softkey Template**.

**Step 2** To create a new softkey template do the following. Otherwise, proceed to the next step.

a) Click **Add New**.
b) Select a default template and click **Copy**.
c) In the **Softkey Template Name** field, enter a new name for the template.
d) Click **Save**.

**Step 3** To add mobility softkeys to an existing template.

a) Enter search criteria and click **Find**.
b) Choose an existing template.

**Step 4** (Optional) Check the **Default Softkey Template** check box if you want to designate this softkey template as the default softkey template.

**Note** If you designate a softkey template as the default softkey template, you cannot delete it unless you first remove the default designation.

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

**Step 6** From the **Related Links** drop-down list, choose **Configure Softkey Layout** and click **Go**.

**Step 7** From the **Select a Call State to Configure** drop-down list, choose the call state for which you want to add the softkey. Typically, you will want to add the softkey for both the **OnHook** and **Connected** call states.

**Step 8** From the **Unselected Softkeys** list, choose the **Mobility** softkey and use the arrows to move the softkey to the **Selected Softkeys** list. Use the up and down arrows to change the position of the new softkey.

**Step 9** To display the softkey in additional call states, repeat the previous step.

**Step 10** Click **Save**.

**Note** If you created a new softkey template, you can assign the template to a phone through the **Phone Configuration** window or to a group of phones through Bulk Administration's **Update Phones** menu.

There are several methods to assign softkey template to phones during provisioning. For example, you can use the **Universal Device Template** configuration, or you can assign it as the default device profile for a specific model.

## Enable Mobility Within Feature Control Policy

If you have configured feature control policies to enable or disable features for Cisco IP Phones, then you will also have to enable Mobility within the policy that is used by your Cisco IP Phones. If the feature is disabled within the feature control policy configuration that is used by your phones, then the Mobility softkey will be disabled for all Cisco IP Phones that use that policy.

### Procedure

**Step 1** From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Feature Control Policy**.

**Step 2** Click **Find** and choose the applicable policy.

**Note** You can also choose **Add New** if you want to create a new feature control policy that you assign to your phones to enable mobility, along with other associated features. You can assign the policy to phones through the **Phone Configuration** window, or to a set of phones through the **Common Phone Profile Configuration**. You can also assign the policy to a universal device template to assign the policy to phones as you provision them.

**Step 3** In the **Name** field, enter a name for the feature control policy. The name can include up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that each feature control policy name is unique to the system.

**Step 4** In the **Description** field, enter a brief description for the feature control policy. The description can include up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_).

**Step 5** In the **Feature Control** area, check both the **Override Default** check box and the **Enable Setting** check box that corresponds to the Mobility softkey.

**Step 6** Click **Save**.

## Configure IP Phone for Mobility

If you have Single Number Reach or Move to Mobility configured, use this procedure to configure your desk phone with the Mobility feature so that enterprise calls can be redirected to a remote destination.

### Procedure

**Step 1** From Cisco Unified CM Administration, choose **Device** > **Phone**.

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

- Click **Find** and select an existing phone to modify the settings.
- Click **Add New** and choose a phone from the **Phone type** drop-down list to add a new phone.

**Step 3** Click **Next**.

**Step 4** From the **SoftKey Template** drop-down list, choose the mobility softkey template that you configured.

**Step 5** From the **Owner User ID** drop-down list, choose the user account on which you enabled mobility.

**Note** You can configure either the **Owner User ID** or **Mobility User ID** field. Mobility users are configured for mobility-enabled devices and Owner users are configured for Non-Mobility devices. Configuring both users for the same device is not recommended.

**Step 6** (Optional) If you are using a **Feature Control Policy** to enable features, choose the policy from the drop-down list.

**Step 7** Click **Save**.

## Configure a Remote Destination Profile

Configures common settings that you want to apply to all the remote destination numbers for a user.

### Procedure

**Step 1** From Cisco Unified CM Administration, choose **Device** > **Device Profile** > **Remote Destination Profile**.

**Step 2** Click **Add New**.

**Step 3** Enter a **Name** for the profile.

**Step 4** From the **User ID** drop-down list, choose the end user to whom this profile applies.

**Step 5** From the **Device Pool** drop-down list, select the device pool where this profile should reside.

**Step 6** Configure the remaining fields in the **Remote Destination Profile Configuration** window. For more information on the fields and their configuration options, see Online Help.

**Step 7** Click **Save**.

**Step 8** Under **Association Information**, click **Add a New DN**.

**Step 9** In the **Directory Number** field, add the directory number of the user's desk phone.

## Configure a Remote Destination

A remote destination is a virtual device that represents a mobile device where the user can be reached (for example, a home office phone, a mobile phone on a cellular network, or a PSTN phone). The remote destination carries many of the same settings as the user's desk phone.

**Note**

- When an enterprise user initiates a call from a remote destination to Cisco Jabber, Unified Communications Manager tries to establish a data call with Cisco Jabber by sending an INVITE message to Cisco TelePresence Video Communication Server (VCS). The call is established regardless of receiving a response from VCS.
- If you have Self-Provisioning enabled, your end users can provision their own phones from the Self-Care Portal. See the System Configuration Guide for Cisco Unified Communications Manager and the "*Configure Self-Provisioning*" chapter for details on configuring the system for self-provisioning and the "*Provisioning End Users*" part for details on enabling self-provisioning for users as a part of a User Profile.

### Procedure

**Step 1** From Cisco Unified CM Administration, choose **Device** > **Remote Destination**.

**Step 2** Click **Add New**.

**Step 3** In the **Destination** field, enter the number of the remote destination. For example, this could be a cellular number or PSTN number.

**Step 4** From the **Mobility User ID** field, select the mobility-enabled end user who uses this remote destination.

**Step 5** Check the **Enable Unified Mobility** features check box.

**Step 6** From the **Remote Destination Profile** drop-down list, choose the profile that you set up for the user who owns this remote destination.

**Step 7** Use the **Single Number Reach Voicemail Policy** drop-down list to configure the voicemail policy.

a) Check the **Enable Single Number Reach** check box.

b) Check the **Enable Move to Mobile** check box to include this remote destination to the list of available destinations when the user presses the **Mobility** softkey on their desk phone.

**Step 8** (Optional) If you want to limit enterprise calls to this remote destination to specific periods such as office hours, configure a **Ring Schedule**.

**Step 9** In the **When receiving a call during the above ring schedule** area, apply the list that is configured for this remote destination.

**Step 10** Configure the remaining fields on the **Remote Destination Configuration** window. For more information on the fields and their configuration options, see Online Help.

**Step 11** Click **Save**.

## Configure an Access List

An access list is an optional remote destination configuration if you want to control which calls can ring which remote destinations, and at which times of day. The access list filters callers based on the Caller ID and can either allow calls or block calls during that remote destination's ring schedule.

### Procedure

**Step 1** From Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **Access List**.

**Step 2** Click **Add New** to create an access list.

**Step 3** Enter a name and description to identify the new access list.

**Step 4** Associate the access list to a user by choosing an ID from the **Owner** drop-down list.

**Step 5** Choose one of the following options:

- **Allowed**—All numbers in the access list are allowed.
- **Blocked**—All numbers in the access list are blocked.

**Step 6** Click **Save**.

**Step 7** From the **Filter Mask** drop-down list, choose the filters that you want to apply to the access list:

- **Not Available**—All callers that advertise a not available status are added to the access list.
- **Private**—All callers that advertise a private status are added to the access list.
- **Directory Number**—All directory numbers or directory strings that you specify are added to the access list. If you choose this option, add a number or number string in the **DN Mask** field.

**Step 8** Choose **Save**.

**Step 9** Apply the access list to a remote destination:

a) From Cisco Unified CM Administration, choose **Device** > **Remote Destination** and reopen the remote destination that you created.

b) Configure the **Ring Schedule** for this access list and do either of the following:

- If you created an allowed access list, click the **Ring this destination only if caller is in** radio button and choose the access list that you created from the drop-down list.
- If you created a blocked access list, click the **Do not ring this destination if caller is in** radio button and choose the access list that you created from the drop-down list.

c) Click **Save**.

# Configure Mobile Voice Access

Complete the following tasks to configure the system for Mobile Voice Access, which lets users place enterprise-anchored calls from any device. Users dial a system IVR for authentication, following which the call is sent out as an enterprise call that will appear to the end user as if the call were sent from the office phone.

### Before you begin

To use Mobile Voice Access:

- Users must be enabled as mobility users with the **Enable Mobile Voice Access** option checked within **End User Configuration** For details, see Configure a Mobility User, on page 5.
- Interactive Voice Response service must be active, and included in a Media Resource Group List that the trunk uses.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Activate the Cisco Unified Mobile Voice Access Service, on page 14 | In Cisco Unified Serviceability, make sure that the Cisco Unified Mobile Voice Access feature service is activated. |
| **Step 2** | Enable Mobile Voice Access, on page 14 | Enable the Mobile Voice Access feature and specify a directory number that users can dial to reach the enterprise. |
| **Step 3** | Configure Directory Number for Mobile Voice Access, on page 15 | Configure mobile voice access (MVA) to assign sets of localized prompts for users who dial in from outside the enterprise. |
| **Step 4** | Restart Cisco CallManager Service, on page 15 | After you activate Mobile Voice Access, restart the Cisco CallManager service. |
| **Step 5** | Configure a gateway for legacy MVA or enterprise feature access (EFA) by performing one of the following tasks:<br>• Configure an Existing H.323 or SIP Gateway for Remote Access, on page 16<br>• Configure a New H.323 Gateway for Remote Access, on page 17 | **Note** Gateway configuration is no longer mandatory for Mobile Voice Access. This is an optional configuration only if you want to configure legacy Mobile Voice Access through an ISR G2 router.<br><br>Depending on your system requirements, you can add a new gateway or configure an existing gateway to handle calls that come from outside the enterprise through MVA or EFA.<br><br>If you have an existing H.323 or SIP PSTN gateway in your system, you can configure it for MVA. This function is accessed by calling a system-configured DID number that is answered and handled by an H.323 or SIP VoiceXML (VXML) gateway. After you configure your gateway, it uses a vxml script on the publisher node to pull the interactive voice response (IVR) prompts that are played to the MVA users. These prompts request user authentication and input of a number that users must dial on their phone keypad. |

| | Command or Action | Purpose |
|---|---|---|
| | | If you do not have an existing H.323 or SIP PSTN gateway and you want to configure mobile voice access, you must add a new H.323 gateway and configure it for MVA functionality by using the hairpinning method. From a technical standpoint, this method refers to using a second gateway to receive the inbound call, apply the MVA service and then the inbound call leg returns to the PSTN gateway (original source) after the system applies the MVA service. |

## Activate the Cisco Unified Mobile Voice Access Service

Use the following procedure to activate this service in your publisher node.

### Procedure

**Step 1** From Cisco Unified Serviceability, choose **Tools** > **Service Activation**.

**Step 2** From the **Server** drop-down list, choose the publisher node.

**Step 3** Click **Go**.

**Step 4** Under **CM Services**, check the **Cisco Unified Mobile Voice Access Service** check box.

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

## Enable Mobile Voice Access

Configure service parameters to enable Mobile Voice Access (MVA) and to specify the directory number or PSTN DID number that users can dial in order to reach the IVR.

### Before you begin

The Cisco Unified Mobile Voice Access feature service must be activated for Mobile Voice Access to work.

### Procedure

**Step 1** From Cisco Unified CM Administration, choose **System** > **Service Parameters**.

**Step 2** From the **Server** drop-down list, choose publisher node.

**Step 3** From the **Service** drop-down list, choose **Cisco CallManager**.

**Step 4** Configure the following service parameters:

- **Enable Mobile Voice Access**—Set this parameter to **True**.
- **Mobile Voice Access Number**—Enter the access number that you want users to dial when they access the enterprise.

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

## Configure Directory Number for Mobile Voice Access

Configure mobile voice access (MVA) to assign sets of localized prompts for users who dial in from outside the enterprise.

### Procedure

**Step 1** From Cisco Unified CM Administration, choose **Media Resources** > **Mobile Voice Access**.

**Step 2** In the **Mobile Voice Access Directory Number**, enter the internal directory number (DN) to receive Mobile Voice Access calls from the gateway.

Enter a value between 1-24 digits in length. Valid values are 0-9.

**Step 3** In the **Localization** pane, use the arrows to move the locales that you want to select to or from this pane.

**Note** Mobile Voice Access uses the first locale that appears in the Selected Locales pane in the **Mobile Voice Access** window. For example, if English United States appears first in the Selected Locales pane, the Cisco Unified Mobility user hears English when the IVR is used during a call.

**Step 4** Click **Save**.

## Restart Cisco CallManager Service

After you enable the Mobile Voice Access feature, restart the Cisco CallManager service.

### Procedure

**Step 1** From Cisco Unified Serviceability, choose **Tools** > **Control Center - Feature Services**

**Step 2** From the **Server** drop-down list, choose the Cisco Unified Communications Manager publisher node.

**Step 3** Under **CM Services**, select the radio button that corresponds to the **Cisco CallManager** service.

**Step 4** Click **Restart**.

### What to do next

You have now completed all the tasks that are required to configure Unified Communications Manager with native Mobile Voice Access support. However, if you want to configure legacy Mobile Voice Access where an ISR G2 router provides the IVR and voice prompts, you can complete either of the following two optional tasks:

- Configure an Existing H.323 or SIP Gateway for Remote Access, on page 16
- Configure a New H.323 Gateway for Remote Access, on page 17

# Configure an Existing H.323 or SIP Gateway for Remote Access

If you have an existing H.323 or SIP PSTN gateway in your system, you can configure it for MVA. This function is accessed by calling a system-configured DID number that is answered and handled by an H.323 or SIP VoiceXML (VXML) gateway. After you configure your gateway, it uses a vxml script on the publisher node to pull the interactive voice response (IVR) prompts that are played to the MVA users. These prompts request user authentication and input of a number that users must dial on their phone keypad.

### Before you begin

Configure Directory Number for Mobile Voice Access, on page 15

### Procedure

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

**Example:**

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

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

**Example:**

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

**Step 3** Load the VXML application from the publisher node.

**Example:**

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

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

**Example:**

Sample configuration before IOS Version 12.3(12):

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

**Caution** Although VXML was added in Version12.2(11), other versions such as 12.3(8), 12.3(9), 12.3(14)T1, and 12.2(15) have VXML issues.

**Step 4** Configure the dial peer to associate the Cisco Unified Mobility application with system remote access.

**Example:**

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
```

**Example:**

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
```

(58888 represents the mobile voice access (MVA) number)

**Step 5** Add a dial peer to transfer the calls to the MVA DN.

**Example:**

Sample configuration for primary Unified Communications Manager:

```
dial-peer voice 101 voip
preference 1
destination-pattern <Mobile Voice Access DN>
session target ipv4:10.1.30.3
codec g711ulaw
dtmf-relay h245-alphanumeric
no vad
```

**Example:**

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

```
dial-peer voice 102 voip
preference 2
destination-pattern <Mobile Voice Access DN>
session target ipv4:10.1.30.4
codec g711ulaw
dtmf-relay h245-alphanumeric
no vad
```

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

**Example:**

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 a New H.323 Gateway for Remote Access

If you do not have an existing H.323 or SIP PSTN gateway and you want to configure mobile voice access, you must add a new H.323 gateway and configure it for MVA functionality by using the hairpinning method. From a technical standpoint, this method refers to using a second gateway to receive the inbound call, apply

the MVA service and then the inbound call leg returns to the PSTN gateway (original source) after the system applies the MVA service.

**Note** If you use Mobile Voice Access with hairpinning, users calling into your system will not be identified automatically by their caller ID. Instead, users must enter their remote destination number manually before they enter their PIN. The reason is that the PSTN gateway must first route the call to Unified Communications Manager to reach the hairpinned Mobile Voice Access gateway. Because of this route path, the conversion of the calling number from a mobile number to an enterprise directory number occurs before the Mobile Voice Access gateway handles the call. As a result, the gateway is unable to match the calling number with a configured remote destination, and therefore the system prompts users to enter their remote destination number.

### Before you begin

Configure Directory Number for Mobile Voice Access, on page 15

### Procedure

**Step 1** Load the VXML application from the publisher node.

**Example:**

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

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

**Example:**

Sample configuration before IOS Version 12.3(12):

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

**Caution** Although VXML was added in Version 12.2(11), other versions such as 12.3(8), 12.3(9), 12.3(14)T1, and 12.2(15) have VXML issues.

**Step 2** Configure the dial-peer to associate the Cisco Unified Mobility application with system remote access.

**Example:**

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>
```

**Example:**

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 (MVA) DN.

**Example:**

Sample configuration for primary Unified Communications Manager:

```
dial-peer voice 101 voip
preference 1
destination-pattern <Mobile Voice Access DN>
session target ipv4:10.1.30.3
voice-class h323 1
codec g711ulaw
dtmf-relay h245-alphanumeric
novad
```

**Example:**

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

```
dial-peer voice 102 voip
preference 2
destination-pattern <Mobile Voice Access DN>
session target ipv4:10.1.30.4
voice-class h323 1
codec g711ulaw
dtmf-relay h245-alphanumeric
novad
```

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

**Step 4** Configure hairpin.

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

**Step 5** On the 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 is created.

# Configure Enterprise Feature Access

Use the following procedure to configure Enterprise Feature Access from a remote destination for:

- Two-stage dialing to place enterprise calls from a configured remote destination. Calls appear to the called party as if they were placed from an associated desk phone.
- Remote destination access to mid-call features through EFA codes that are sent using DTMF digits sent from the remote destination.

**Note** Unlike Mobile Voice Access, with Enterprise Feature Access you must be calling from a configured remote destination.

### Procedure

**Step 1** From Cisco Unified CM Administration, choose **Call Routing** > **Mobility** > **Enterprise Feature Access Number Configuration**.

**Step 2** In the **Number** field, enter the unique DID number that mobile users will dial from a remote destination in order to access the Enterprise Feature Access feature.

**Step 3** From the **Route Partition** drop-down list, choose the partition where the DID resides.

**Step 4** (Optional) Check the **Default Enterprise Feature Access Number** check box to make this EFA number the default for this system.

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

**Step 6** Configure the Enteprise Feature Access service parameters:

a) From Cisco Unified CM Administration, choose **System** > **Service Parameters**.

b) From the **Server** drop-down list, choose the publisher node.

c) From the **Service** drop-down list, choose **Cisco CallManager**.

d) Set the **Enable Enterprise Feature Access** service parameter to **True**.

e) (Optional) In the **Clusterwide Parameters (System - Mobility)** area, edit the DTMF digits that you must enter to access midcall features through Enterprise Feature Access. For example, you could edit the **Enterprise Feature Access Code for Hold** service parameter, which has a default value of ***81**. The default values are as follows:

- Hold: *81
- Exclusive Hold: *82
- Resume: *83
- Transfer: *84
- Conference: *85
- Session Handoff: *74
- Starting Selective Recording: *86
- Stopping Selective Recording: *87
- Hunt group login—enter a new code
- Hunt group logout—enter a new code

f) Click **Save**.

# Configure Intelligent Session Control

Configure the system so that inbound calls to a remote destination are rerouted to an associated enterprise number, if one is available. This provides automatic call anchoring within the enterprise for mobility calls, providing cost savings and added Unified Communications functionality.

### Procedure

**Step 1** From Cisco Unified CM Administration, choose **System** > **Service Parameters**.

**Step 2** From the **Server** drop-down list, choose a Cisco Unified Communications Manager node.

**Step 3** From the **Service** drop-down list, choose **Cisco CallManager**.

**Step 4** Under **Clusterwide Parameters (Feature - Reroute Remote Desination Calls to Enterprise Number)** set the following service parameters:

- **Reroute Remote Destination Calls to Enterprise Number**—To enable Intelligent Session Control, set this parameter to **True**.
- **Ring All Share Lines**—Set the value of the parameter to **True**. If Intelligent Session Control is enabled, and this service parameter is also enabled, the system anchor calls to remote destinations within the enterprise, and will also ring all the user's shared lines.
- **Ignore Call Forward All on Enterprise DN**—This parameter applies only to outgoing calls to a remote destination when Intelligent Session Control is enabled. By default, this parameter is set to **True**.

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

# Configure Mobility Service Parameters

Use this procedure to configure optional Mobility-related service parameters.

### Procedure

**Step 1** From Cisco Unified CM Administration, choose **System** > **Service Parameters**.

**Step 2** From the **Server** drop-down list, choose the publisher node.

**Step 3** From the **Service** drop-down list, choose **Cisco CallManager**.

**Step 4** Configure any service parameters that you want to edit. The Mobility-related parameters are listed under the following headings. For help descriptions, click the parameter name:

- **Clusterwide Parameters (System - Mobility)**
- **Clusterwide Parameters (System - Mobility Single Number Reach Voicemail)**
- **Clusterwide Parameters (Feature - Reroute Remote Destination Calls to Enterprise Number)**

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

# Configure Cisco Jabber Dual-Mode

Complete these tasks to configure Cisco Jabber on iPhone or Android as dual-mode mobile devices that can connect over WiFi. Cisco Jabber registers to Unified Communications Manager over WiFi and can be reached through an enterprise number if Single Number Reach is enabled in the user's mobile identity.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Configure a Mobility Profile, on page 23 | Configure a mobility profile to send consistent caller ID to Jabber mobile clients that are placing Dial through Office calls. |
| **Step 2** | Add a Dual-Mode Device for Cisco Jabber, on page 23 | Configure a dual-mode device type for Cisco Jabber on iPhone or Android clients. |
| **Step 3** | Configure a Mobility Identity, on page 26 | Add a Mobility Identity to the Jabber mobile client that points to the device phone number (that is, the iPhone number) to provide calling when Jabber roams out of WiFi range. Enable Single Number Reach destination for the Mobile Identity. |
| **Step 4** | Required: Configure Handoff Number, on page 26 | Configure a handoff number for dual-mode devices that are leaving enterprise. Even when the device disconnects from the enterprise WiFi network the call can be maintained without interruption by reconnecting to a remote mobile or cellular network. |

## Configure Other Dual-Mode Devices

Complete these tasks to configure other dual-mode mobile devices that can place calls over the cellular network and can also connect over WiFi. For example:

- Carrier-Integrated Mobile Devices that connect over Fixed Mobile Convergence (FMC) networks.
- IMS-integrated Mobile Devices over IP Multimedia networks

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Add a Dual-Mode Device for Cisco Jabber, on page 23 | Configure an IMS or FMC dual-mode device. |
| **Step 2** | Configure a Mobility Identity, on page 26 | Add a Mobility Identity that points to the phone number of the actual device. |
| **Step 3** | Required: Configure Handoff Number, on page 26 | Configure a handoff number for dual-mode devices that are leaving the enterprise. Even when the device disconnects from the enterprise WiFi network the call can be maintained without interruption by reconnecting to a remote mobile or cellular network. |

# Configure a Mobility Profile

Configure a mobility profile for dual-mode Cisco Jabber on iPhone and Android clients. The profile configures the client with a consistent caller ID for dial via office calls.

**Note** From a technical standpoint, this caller ID is sent during the dial via office reverse (DVO-R) callback portion of a call to the mobility identity or alternate callback number. DVO-R call feature uses enbloc dialing. If no mobility profile is assigned to the mobility identity or if the Callback Caller ID field is left blank, the system sends the default enterprise feature access number.

### Procedure

**Step 1** From Cisco Unified CM Administration, choose **Call Routing** > **Mobility** > **Mobility Profile**.

**Step 2** Click **Add New**.

**Step 3** Enter a **Name** for the profile.

**Step 4** From the **Mobile Client Calling Option** drop-down list, select Dial via Office Reverse.

**Note** Despite the field options, Dial via Office Forward is not available.

**Step 5** Configure a **Callback Caller ID** for Dial-via-Office Reverse.

**Step 6** Configure the fields in the **Mobility Profile Configuration** window. For more information on the fields and their configuration options, see Online Help.

**Step 7** Click **Save**.

# Add a Dual-Mode Device for Cisco Jabber

Use the following procedure to configure a dual-mode device type for Cisco Jabber on iPhone or Android clients.

### Before you begin

Make sure that your end users are mobility-enabled. Also, if you want to add remote destinations to your Jabber client, make sure that you have a softkey template that includes the Mobility softkey.

### Procedure

**Step 1** From Cisco Unified CM Administration, choose **Device** > **Phone**.

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

- Click **Find** to edit an existing device.
- Click **Add New** and select either **Cisco Dual Mode for Android** or **Cisco Dual Mode for iPhone** as the phone model, to add a new device. **Click Next**.

**Step 3** Configure the fields in the **Phone Configuration** window.

For detailed information about product specific configuration layout fields, see your Jabber client documentation at http://www.cisco.com/go/jabber.

**Step 4** Configure the following mandatory fields:

- Device Name
- Device Pool
- Softkey Template
- Owner User ID—The user must have mobility enabled.
- Mobility User ID—The user must have mobility enabled.
- Device Security Profile
- SIP Profile

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

**Step 6** Add a directory number:

a) In the left Association area, click **Add a New DN**.
b) Enter a new **Directory Number** and click **Save**.
c) Complete any fields that you want in the **Directory Number Configuration** window and click **Save**. For more information on the fields and their configuration options, see Online Help.
d) Click **Associate End Users** .
e) Click **Find** and select the mobility-enabled end user whom owns this DN.
f) Click **Add Selected**.
g) Click **Save**.

### What to do next

Add a Mobility Identity that points to the phone number of the iPhone or Android device. This allows you to transfer the call to the phone if you move out of Wi-Fi range. You can also add the device as a Single Number Reach destination. For details, Configure a Mobility Identity, on page 26.

Optionally, add Remote Destinations and Single Number Reach to your Cisco Jabber client. When someone calls the Jabber client, the remote destination rings as well. Configure a Remote Destination, on page 11.

## Dual-Mode Device Configuration Fields

*Table 1: Dual-Mode Device Configuration Fields*

| Field | Description |
|---|---|
| Softkey Template | Choose the Mobility Softkey template. |
| Owner User ID | Choose the user ID of the assigned phone user. The user ID is recorded in the call detail record (CDR) for all calls made from this device. |
| Mobility User ID | Choose the user ID of the person to whom this dual-mode phone is assigned. |

| Field | Description |
|---|---|
| Device Security Profile | Choose the security profile to apply to the device.<br>You must apply a security profile to all phones that are configured in Cisco Unified Communications Manager Administration. To enable security features for a phone, you must configure a new security profile for the device type and protocol, and then apply it to the phone. |
| Rerouting Calling Search Space | Choose a calling search space for routing calls to configured remote destinations and mobility identities that are configured for this device. |
| SIP Profile | Choose **Standard SIP Profile for Mobile Device**. |

# Add Other Dual-Mode Device

Use this procedure to add another dual-mode device (for example, a **Carrier-integrated Mobile Device** for network-based FMC, or an **IMS-integrated Mobile Device**.

### Before you begin

Make sure that your end users are mobility-enabled. Refer to topics earlier in this chapter for details on how to enable mobility for users.

### Procedure

**Step 1** From Cisco Unified CM Administration, choose **Device** > **Phone**.

**Step 2** Click **Add New**.

**Step 3** From the **Phone Model** drop-down list **Carrier-integrated Mobile Device** or **IMS-integrated Mobile Device**.

**Step 4** Configure the following mandatory fields:

- Device Name
- Device Pool
- Owner User ID—The user must have mobility enabled.
- Mobility User ID—The user must have mobility enabled.

**Step 5** Configure the remaining fields in the **Phone Configuration** window. For more information on the fields and their configuration options, see Online Help.

**Step 6** Click **Save**.

**Step 7** Add a directory number:

a) In the left Association area, click **Add a New DN**.
b) Enter a new **Directory Number** and click **Save**.
c) Complete any fields that you want in the **Directory Number Configuration** window and click **Save**. For more information on the fields and their configuration options, see Online Help.
d) Click **Associate End Users**.
e) Click **Find** and select the mobility-enabled end user whom owns this DN.
f) Click **Add Selected**.

g) Click **Save**.

# Configure a Mobility Identity

Add a Mobility Identity that points to the phone number of the device if you want to enable the device as a Single Number Reach that can be reached through the enterprise number.

### Procedure

**Step 1** From Cisco Unified CM Administration, choose **Device** > **Phone**.

**Step 2** Enter search criteria if needed, click **Find**, and choose the dual-mode device that you created.

**Step 3** Click **Add New Mobility Identity**.

**Step 4** In the **Destination** field, enter the phone number of the mobile device. For example, for a Cisco Jabber on iPhone client, this would be the phone number of the iPhone.

**Step 5** Cisco Jabber only. Select the **Mobility Profile** that you configured.

**Step 6** If you want to make this Mobile Identity available from an enteprise phone number:

a) Check the **Enable Single Number Reach** check box.

b) Configure a **Single Number Reach Voicemail** policy

**Step 7** Configure a **Dial-via-Office Reverse Voicemail** policy.

**Step 8** Configure the fields on the **Mobility Identity Configuration** window. For more information on the fields and their configuration options, see Online Help.

**Step 9** Click **Save**.

**Note** If you want to apply a Ring Schedule and access list to limit calls to this mobile identity to specific times and users, Configure an Access List, on page 12.

# Configure Handoff Number

Configure handoff mobility for dual-mode phones if you want your system to preserve a call while the user moves out of the enterprise. Even when a user's device disconnects from the enterprise WiFi network and reconnects to the mobile voice or cellular network, an in-progress call is maintained without interruption.

### Procedure

**Step 1** From Cisco Unified CM Administration, choose **Call Routing** > **Mobility** > **Handoff Configuration**.

**Step 2** In the **Handoff Number** field, enter the direct inward dialing (DID) number for handoff between the Wi-Fi and mobile voice or cellular network.

For numbers that start with the international escape character (+), you must precede the + with a backslash (\). Example: \+15551234.

**Step 3** From the **Route Partition** drop-down list, choose the partition to which the handoff DID number belongs.

**Step 4** Click **Save**.

# Cisco Unified Mobility Call Flow

This section describes the incoming and outgoing call flows of Cisco Unified Mobility commonly known as Single Number Reach (SNR). Unified Communications Manager supports the separate calling party number and billing number feature when SNR is configured for users to allow desk phones to extend calls to mobile devices.

For example, User-A calls from a PSTN network to User-B whose directory number configured to SNR. If **Enable External Presentation Name and Number** check box is checked in SIP profile and **Display External Presentation Name and Number** service parameter value set to *True*, then Unified Communications Manager displays the FROM header information on both the User-B's desk phone and the configured remote destination device. In the same way, if any one option is disabled, Unified Communications Manager displays P-Asserted-Identity (PAID) header information on the called device.

Similarly, in outgoing call scenario User B (SNRD line) configured with External Presentation Information on Directory Number configuration page initiates a call to a PSTN network through a SIP trunk. If **Enable External Presentation Name and Number** is configured in its SIP profile, then, Unified Communications Manager send the External Presentation Information in the FROM header of the outgoing SIP message to display on the called device.

If **Enable External Presentation Name and Number** check box is disabled, then Unified Communications Manager sends the directory number information in the FROM and PAID to display on the called device and configured External Presentation Information in the X-Cisco-Presentation header.

If you check the **Anonymous External Presentation** check box, the configured **External Presentation Name** and **External Presentation Number** are removed from the respective fields and external presentation displayed as anonymous on the called device.

For more details on Configuring External Presentation Information, see *Configure Directory Number* chapter in the System Configuration Guide for Cisco Unified Communications Manager.

# FMC Over SIP Trunks Without Smart Client

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 through the trunk without a smart client on the mobile. Basic mobile features such as SNR, 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 Unified Communications Manager. These features can be provided by any type of trunk.

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.

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

# Hunt Group Login and Logout for Carrier-Integrated Mobile Devices

When configuring the 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. Only users with mobility enabled will appear in the **Owner User ID** drop-down on the end user page and 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.

Carrier-integrated mobile devices can be configured to support hunt group login and logout through Enterprise Feature Access codes. Make sure that you've configured the following:

- Enterprise Feature Access must be configured in **Call Routing** > **Mobility** > **Enterprise Feature Access Number Configuration**.
- Make sure you assign values for the **Enterprise Feature Access Number for Hunt Group Login** and **Enterprise Feature Access Number for Hunt Group Logout** fields in Service Parameters.

After you configure these, the user can log in or log out of Hunt groups from Carrier-Integrated Mobile devices by dialing the configured Enterprise Feature Access Number. If the user dials the given Hunt login access code number, the Carrier-Integrated Mobile device allows them to be part of the Hunt group list. If the Hunt logout access code is dialed, then the user is moved out of the Hunt group list and calls do not reach them.

**Note** Users on Carrier-Integrated Mobile devices can invoke midcall features via Enterprise Feature Access codes. For details on how to configure and use Enterprise Feature Access, see Configure Enterprise Feature Access section.

# Cisco Unified Mobility Interactions

*Table 2: Cisco Unified Mobility Interactions*

| Feature | Interaction |
|---|---|
| Auto Call Pickup | Cisco Unified Mobility interacts with auto call pickup depending on how you configured the service parameter. When the **Auto Call Pickup Enabled** service parameter is set to **True**, users must press only the **PickUp** softkey to pick up a call.<br><br>If the service parameter is set to **False**, users must press the **PickUp**, **GPickUp**, or **OPickUp** softkey and then the Answer softkey. |
| Automatic Alternate Routing | Cisco Unified Mobility supports automatic alternate routing (AAR) as follows:<br>• If a rejection occurs because of a lack of bandwidth for the location-based service, the rejection triggers AAR and reroutes the call through the PSTN so the caller does not need to hang up and redial.<br>• If a rejection occurs because of resource reservation protocol (RSVP), however, AAR is not triggered for calls to remote destinations and the call stops. |
| Extend and Connect | Users who need the capabilities of both Cisco Unified Mobility and Extend and Connect can 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 configuration allows Cisco Unified Mobility features to be used concurrently with Extend and Connect.<br><br>For more information, see the “Extend and Connect” chapter. |
| External Call Control | If external call control is configured, Unified Communications Manager follows the route decision from the adjunct route server for these Cisco Unified Mobility features:<br>• Cisco Unified Mobility<br>• Mobile voice access<br>• Enterprise feature access<br>• Dial via office<br><br>Unified Communications Manager does not send a routing query for the following Cisco Unified Mobility features:<br>• Cell pickup<br>• Desk pickup<br>• Session handoff |

| Feature | Interaction |
|---|---|
| Intelligent Session Control and Session Handoff | For direct calls to remote destinations that are anchored to the enterprise number, mobile users can use the session handoff feature to hand off the call to their deskphones.<br>You must enable Cisco Unified Mobility before you implement intelligent session control. |
| Licensing | Cisco Unified Mobility is included in all user-based licenses from basic to professional. |
| 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.<br>**Note** Local Route Group is not supported when the AgentGreeting with BiB (Built in Bridge) is invoked. |
| Number of Supported Calls | Each remote destination supports a maximum of six active calls. However, the number of supported calls depends on the Unified Communications Manager configuration.<br>For example, the Cisco Unified Mobility user receives a call while the user already has six calls for the remote destination or while the user is using DTMF to transfer or conference a call from the remote destination.<br>The received call is sent to the enterprise voice mail when:<br>• The number of calls with user exceeds Busy trigger configuration<br>• CFB is configured<br>• All shared lines are busy<br>**Note** The calls sent to the enterprise voice mail is not based on the maximum supported calls. |
| 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). |

# Cisco Unified Mobility Restrictions

***Table 3: Cisco Unified Mobility Interactions***

| Restriction | Description |
|---|---|
| Auto Answer | A remote destination call does not work when auto answer is enabled.<br>**Note** Auto Answer is not supported with Dual-Mode phones. |

| Restriction | Description |
|---|---|
| Call Forwarding Unregistered | Call Forward Unregistered (CFUR) support for Cisco Jabber on iPhone and Android is as follows:<br>• CFUR is supported if Cisco Jabber on iPhone or Android does not have either a mobile identity or remote destination configured.<br>• CFUR is not supported, and will not work, if a Remote Destination is configured<br>• CFUR is not supported, and will not work, if a Mobile Identity is configured with a mobile phone number and Single Number Reach is enabled.<br>If you have a mobile identity or remote destination configured, use Call Forward Busy and Call Forward No Answer instead. |
| Call Queuing | Unified Communications Manager does not support call queuing with 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.<br>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.<br>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.<br>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.<br>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. |
| Do Not Disturb 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 is not anchored in the following scenarios:<br>• DND is enabled with the call reject option.<br>• DND is activated by pressing the DND softkey on the desk phone.<br>If DND is enabled with the ring off option, however, the call is anchored. |

| Restriction | Description |
|---|---|
| Dual-Mode Phones | **Dual-Mode Handoff and Caller ID**<br>The handoff DN method of dual-mode handoff requires a caller ID in the cellular network. The mobility softkey method does not require caller ID.<br>**Dual-Mode Phones and CTI Applications**<br>While a dual-mode phone is in Wi-Fi enterprise mode, no CTI applications control it nor monitor it.<br>The **In Use Remote** indicator for dual-mode phones on a shared line call in the WLAN disappears if the dual-mode phone goes out of WLAN range.<br>**Dual-Mode Phones and SIP Registration Period**<br>For dual-mode phones, 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. The standard SIP profile for mobile devices determines the registration period as defined by the **Time Register Expires** field in that profile. |
| Enterprise Features From Cellular Networks | Enterprise features from cellular networks require out-of-band DTMF.<br>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. |
| Gateways and Ports | Both H.323 and SIP VoIP gateways are supported for mobile voice access.<br>Cisco Unified Mobility features are not supported for T1 CAS, FXO, FXS and BRI.<br>SNR(Single Number Reach) is not supported with MGCP(Media Gateway Controlled Protocol). |
| Jabber 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. |
| Locales | Cisco Unified Mobility supports a maximum of nine locales. If more than nine locales are installed, they appear in the Available Locales pane, but you can only save up to nine locales in the Selected Locales pane.<br>If you attempt to configure more than nine locales for Cisco Unified Mobility, the following message appears: “Update failed. Check constraint (informix.cc_ivruserlocale_orderindex) failed.” |

| Restriction | Description |
|---|---|
| Maximum Wait Timer for Desktop Call Pickup | 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 be displayed even after the timeout that is configured for the end user to pick up the call elapses and the call is not dropped.<br><br>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.) |
| Multilevel Precedence and Preemption | 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. |
| Overlap Sending | Overlap sending patterns are not supported for the Intelligent Session Control feature. |
| Q Signaling | Mobility does not support Q signaling (QSIG). |
| QSIG Path Replacement | QSIG path replacement is not supported. |
| 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. You 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 | The following limitations apply to the session handoff feature:<br>• 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.<br>• Only audio call session handoff is supported. |
| Single Number Reach with Hunt Groups | If you have a hunt group configured and one or more of the directory numbers that the hunt group points toward also has Single Number Reach (SNR) enabled, the call does not extend to the SNR remote destinations unless all devices in the hunt group are logged in.<br><br>For each device within the hunt group, the **Logged Into Hunt Group** check box must be checked within the **Phone Configuration** window for that device. |
| SIP Trunks | The Cisco Unified Mobility feature is supported only for primary rate interface (PRI) public switched telephone network (PSTN) connections.<br><br>For SIP trunks, Cisco Unified Mobility is supported over IOS gateways or intercluster trunks. |

| Restriction | Description |
|---|---|
| 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. |
| Unified Communications Manager publisher dependent features | In a cluster environment, the publisher must be reachable in order to enable or disable Single Number Reach. Some features may not function if the publisher is not actively running.<br>Mobile voice access is not available when the publisher node is not reachable; IVR prompts for Mobile Voice Access are stored only on the publisher. |
| 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. |
| Mobile Voice Access (MVA) | Cisco 4000 Series Integrated Services Routers do not support Voice XML (VXML). Hence, when these routers function as Unified Communications gateways with Cisco Unified Communications Manager, they do not support Mobile Voice Access (MVA) application. |

**Related Topics**

Ad Hoc Conferencing Service Parameters

# Cisco Unified Mobility Troubleshooting

## Cannot Resume Call on Desktop Phone

**Problem** When a remote destination (mobile phone) is not a smartphone and a call to this mobile phone is anchored through Cisco Unified Communications Manager, the user can hang up the mobile phone and expect to see a **Resume** softkey on the user desktop phone to resume the call. The user cannot resume this call on the user desktop phone.

**Possible Cause** If the calling party receives a busy, reorder, or disconnect tone when the mobile phone hangs up, the mobile phone provider probably did not disconnect the media. No disconnect signals came from the provider. To verify this possibility, let the calling party wait for 45 seconds. After this wait, the service provider will time out and send disconnect signals, at which time Cisco Unified Communications Manager can provide a **Resume** softkey to resume the call.

- Add the following command to the gateway:

```
voice call disc-pi-off
```

- For the Cisco CallManager service, set the **Retain Media on Disconnect with PI for Active Call** service parameter to **False**.