Configure Mobile and Remote Access

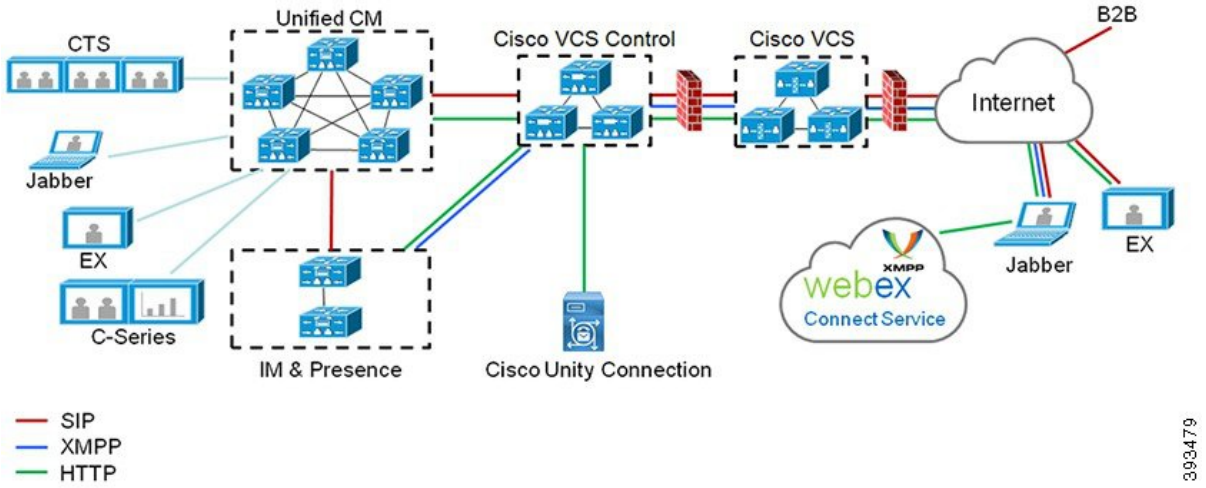
Mobile and Remote Access Overview

Unified Communications Manager Mobile and Remote Access is a core part of the Cisco Collaboration Edge Architecture. It allows endpoints such as Cisco Jabber to have their registration, call control, provisioning, messaging, and presence services that are provided by Unified Communications Manager when the endpoint is not within the enterprise network. Cisco Expressway connects the mobile endpoint to the on-premises network, providing secure firewall traversal and line-side support for Unified CM registrations.

The overall solution provides:

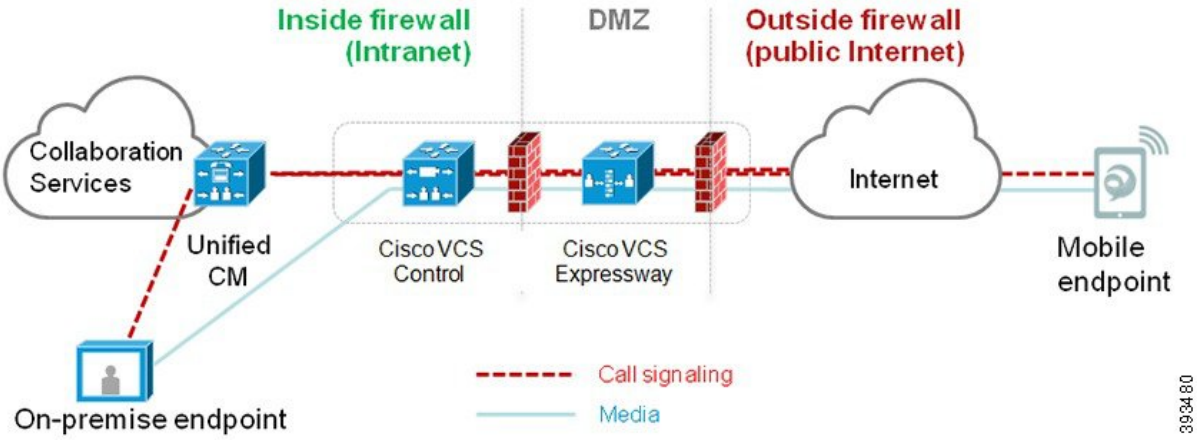
- Off-premises access: a consistent experience outside the network for Jabber and EX/MX/SX Series clients
- Security: secure business-to-business communications
- Cloud services: enterprise grade flexibility and scalable solutions providing rich Webex integration and Service Provider offerings
- Gateway and interoperability services: media and signaling normalization, and support for non-standard endpoints

Figure 1: Unified Communications: Mobile and Remote Access



Third-party SIP or H.323 devices can register to the Expressway-C and, if necessary, interoperate with Unified CM-registered devices over a SIP trunk.

Figure 2: Typical Call Flow: Signaling and Media Paths



- Unified CM provides call control for both mobile and on-premises endpoints.
- Signaling traverses the Expressway solution between the mobile endpoint and Unified CM.
- Media traverses the Expressway solution and is relayed between endpoints directly; all media is encrypted between the Expressway-C and the mobile endpoint.

Configuring Mobile and Remote Access

To enable Cisco Jabber users with Mobile and Remote Access functionality, set up an Mobile and Remote Access User Policy within the **User Profile Configuration** window of Unified Communications Manager. The Mobile and Remote Access User Policy is not required for non-Jabber endpoints.

In addition, you must configure Cisco Expressway with Mobile and Remote Access. For details, see Mobile and Remote Access via Cisco Expressway Deployment Guide .

Mobile and Remote Access Prerequisites

Cisco Unified Communications Manager Requirements

The following requirements apply:

- If you are deploying multiple Unified Communications Manager clusters, set up an ILS network.
- Mobile and Remote Access requires that you set up NTP servers for your deployment. Make sure that you have NTP servers deployed for your network and Phone NTP References for SIPendpoints.
- If you are deploying ICE for media path optimization, you will need to deploy a server that can provide TURN and STUN services.

DNS Requirements

For the internal connection to Cisco Expressway, configure the following locally resolvable DNS SRV that points to Unified Communications Manager:

`_cisco-uds._tcp<domain>`

You must create internal DNS records, for both forward and reverse lookups, for all Unified Communications nodes used with Mobile and Remote Access. This allows Expressway-C to find the nodes when IP addresses or hostnames are used instead of FQDNs. Make sure that the SRV record is not resolvable outside of the local network.

Cisco Expressway Requirements

This feature requires you to integrate Unified Communications Manager with Cisco Expressway. For Cisco Expressway configuration details for Mobile and Remote Access, refer to the Mobile and Remote Access Through Cisco Expressway Deployment Guide.

The minimum Expressway release for Mobile and Remote Access Access Policy support with Cisco Jabber is X8.10.

Certificate Prerequisites

You must exchange certificates between Unified Communications Manager, the IM and Presence Service, and Cisco Expressway-C. Cisco recommends that you use CA-signed certificates with the same CA for each system. In this case:

- Install the CA root certificate chain on each system (for Unified Communications Manager and the IM and Presence Service Service install the certificate chain to the tomcat-trust store).
- For Unified Communications Manager, issue a CSR to request CA-signed tomcat (for AXL and UDS traffic) and Cisco CallManager (for SIP) certificates.
- For the IM and Presence Service Service, issue a CSR to request CA-signed tomcat certificates.

Note If you use different CAs, you must install each CA's root certificate chain on Unified Communications Manager, IM and Presence Service Service, and Expressway-C.

Note You can also use self-signed certificates for both Unified Communications Manager and the IM and Presence Service Service. In this case, you must upload onto Expressway-C the tomcat and Cisco CallManager certificates for Unified Communications Manager and a tomcat certificate for the IM and Presence Service Service.

Mobile and Remote Access Configuration Task Flow

Complete these tasks in Unified Communications Manager if you want to deploy Mobile and Remote Access endpoints.

Procedure

	Command or Action	Purpose
Step 1	Activate Cisco AXL Web Service, on page 5	Make sure that the Cisco AXL Web Service is activated on the publisher node.
Step 2	Configure Maximum Session BitRate for Video, on page 5	**Optional**. Configure Region-specific settings for your Mobile and Remote Access endpoints. For example, if you expect Mobile and Remote Access endpoints to use video, you may want to increase the **Maximum Session Bit Rate for Video Calls** setting as the default setting of 384 kbps may be too low for some video endpoints.
Step 3	Configure a Device Pool for Mobile and Remote Access, on page 6	Assign your Date/Time Group and Region configuration to the device pool that your Mobile and Remote Access endpoints use.
Step 4	Configure ICE, on page 6	**Optional**. ICE is an optional deployment that uses STUN and TURN services to analyze the available media paths for an Mobile and Remote Access call and then to select the best path. ICE adds potentially to the call setup time, but increases the reliability of Mobile and Remote Access calls.
Step 5	Configure Phone Security Profile for Mobile and Remote Access, on page 7	Use this procedure to set up a phone security profile to be used by Mobile and Remote Access endpoints.
Step 6	Configure Mobile and Remote Access Access Policy for Cisco Jabber Users, on page 8	Cisco Jabber only. Set up an Mobile and Remote Access Access Policy for Cisco Jabber users. Cisco Jabber users must be enabled with Mobile and Remote Access access within their user profiles in order to use the Mobile and Remote Access feature.

	Command or Action	Purpose
Step 7	Configure Users for Mobile and Remote Access, on page 9	For Cisco Jabber users, the User Policy that you set up must be applied to their End User Configurations.
Step 8	Configure Endpoints for Mobile and Remote Access, on page 9	Configure and provision endpoints that use the Mobile and Remote Access feature.
Step 9	Configure Cisco Expressway for Mobile and Remote Access, on page 9	Configure Cisco Expressway for Mobile and Remote Access.

Activate Cisco AXL Web Service

Make sure that the Cisco AXL Web Service is activated on the publisher node.

Procedure

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

Step 2 From the **Server** drop-down list, select the publisher node and click **Go**.

Step 3 Under **Database and Admin Services**, confirm that the **Cisco AXL Web Service** is **Activated**.

Step 4 If the service is not activated, check the corresponding check box and click **Save** to activate the service.

Configure Maximum Session BitRate for Video

Configure Region settings for your Mobile and Remote Access endpoints. The default settings may be sufficient in many cases, but if you expect Mobile and Remote Access endpoints to use video, you may want to increase the **Maximum Session Bit Rate for Video Calls** within your Region Configuration. The default setting of 384 kbps may be too low for some video endpoints, such as the DX series.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Region Information** > **Region**.

Step 2 Perform any one of the following:

- Click **Find** and select the region to edit the bit rates within an existing region.
- Click **Add New** to create a new region.

Step 3 In the **Modify Relationship to other Regions** area, configure a new setting for the **Maximum Session Bit Rate for Video Calls**. For example, 6000 kbps.

Step 4 Configure any other fields in the **Region Configuration** window. For more information on the fields and their configuration options, see Online Help..

Step 5 Click **Save**.

Configure a Device Pool for Mobile and Remote Access

When you created a new region, assign your region to the device pool that your Mobile and Remote Access endpoints use.

Procedure

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

Step 2 Do either of the following:

- Click **Find** and select the existing device pool to edit.
- Click **Add New** to create a new device pool.

Step 3 Enter a **Device Pool Name**.

Step 4 Select a redundant **Cisco Unified Communications Manager Group**.

Step 5 Assign the **Date/Time Group** that you set up. This group includes the Phone NTP references that you set up for Mobile and Remote Access endpoints.

Step 6 From the **Region** drop-down list, select the region that you configured for Mobile and Remote Access.

Step 7 Complete the remaining fields in the **Device Pool Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 8 Click **Save**.

Configure ICE

Use this procedure if you want to deploy ICE to handle call setup for Mobile and Remote Access calls. ICE is an optional deployment that uses STUN and TURN services to analyze the available media paths for an Mobile and Remote Access call and to select the best path. ICE adds potentially to the call setup time, but increases the reliability of Mobile and Remote Access calls.

Before you begin

Decide how you are going to deploy ICE. You can configure ICE for groups of phones via the Common Phone Profile Configuration, to individual Cisco Jabber desktop devices, or through system-wide defaults that apply to all phones.

As a fallback mechanism, ICE can use a TURN server to relay media. Make sure that you have deployed a TURN server.

Procedure

Step 1 From Cisco Unified CM Administration:

- Choose **System** > **Enterprise Phone** to configure system defaults for ICE.
- Choose **Device** > **Device Settings** > **Common Phone Profile** to configure ICE for groups of endpoints and select the profile you want to edit.
- Choose **Device** > **Phone** to configure ICE for an individual Cisco Jabber desktop endpoint and select the endpoint that you want to edit.

Step 2 Scroll down to the **Interactive Connectivity Establishment (ICE)** section.

Step 3 Set the **ICE** drop-down list to **Enabled**.

Step 4 Set the **Default Candidate Type**:

- **Host**—A candidate obtained by selecting the IP address on the host device. This is the default.
- **Server Reflexive**—An IP address and port candidate obtained by sending a STUN request. In many cases, this may represent the public IP address of the NAT.
- **Relayed**—An IP address and port candidate obtained from a TURN server. The IP address and port are resident on the TURN server such that media is relayed through the TURN server.

Step 5 From the **Server Reflexive Address** drop-down list, select whether you want to enable STUN-like services by setting this field to **Enabled** or **Disabled**. You must set this field to enabled if you configured Server Relexive as the Default Candidate.

Step 6 Enter the IP address or hostname for the Primary and Secondary TURN Servers.

Step 7 Set the **TURN Server Transport Type** to **Auto (default setting)**, **UDP**, **TCP**, or **TLS**.

Step 8 Enter the **Username** and **Password** of the TURN Server.

Step 9 Click **Save**.

Note If you configured ICE for a Common Phone Profile, you must associate phones to that Common Phone Profile for phones to be able to use the profile. You can apply the profile to a phone through the **Phone Configuration** window.

Configure Phone Security Profile for Mobile and Remote Access

Use this procedure to set up a phone security profile to be used by Mobile and Remote Access endpoints.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Security** > **Phone Security Profile**.

Step 2 Click **Add New**.

Step 3 From the **Phone Security Profile Type** drop-down list, select your device type. For example, you could select **Cisco Unified Client Service Framework** for a Jabber application.

Step 4 Click **Next**.

Step 5 Enter a **Name** for the profile. For Mobile and Remote Access, the name must be in FQDN format and must include the enterprise domain.

Step 6 From the **Device Security Mode** drop-down list, select **Encrypted**.

Note This field must be set to **Encrypted**. Otherwise, Expressway rejects communications.

Step 7 Set the **Transport Type** to **TLS**.

Step 8 Leave the **TFTP Encrypted Config** check box unchecked for the following phones as Mobile and Remote Access will not work for these phones with this option enabled: DX Series, IP Phone 7800, or IP Phone 8811, 8841, 8845, 8861 and 8865

Step 9 Complete the remaining fields in the **Phone Security Profile Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 10 Click **Save**.

Note You must apply this profile to the Phone Configuration for each of your Mobile and Remote Access endpoints.

Configure Mobile and Remote Access Access Policy for Cisco Jabber Users

Use this procedure to set up an Mobile and Remote Access Access Policy for Cisco Jabber users. Cisco Jabber users must be enabled with Mobile and Remote Access access within their user profiles in order to use the Mobile and Remote Access feature. The minimum Expressway release for Mobile and Remote Access Policy support with Cisco Jabber is X8.10.

Note The Mobile and Remote Access Policy is not required for non-Jabber users.

For more information on user profiles, see "*User Profile Overview*" section in System Configuration Guide for Cisco Unified Communications Manager.

Procedure

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

Step 2 Click **Add New**.

Step 3 Enter a **Name** and **Description** for the user profile.

Step 4 Assign a **Universal Device Template** to apply to users' **Desk Phones**, **Mobile and Desktop Devices**, and **Remote Destination/Device Profiles**.

Step 5 Assign a **Universal Line Template** to apply to the phone lines for users in this user profile.

Step 6 If you want the users in this user profile to be able to use the self-provisioning feature to provision their own phones, do the following:

a) Check the **Allow End User to Provision their own phones** check box.

b) In the **Limit Provisioning once End User has this many phones** field, enter a maximum number of phones the user is allowed to provision. The maximum is 20.

c) Check the **Allow Provisioning of a phone already assigned to a different End User** check box to determine whether the user who is associated with this profile has the permission to migrate or reassign a device that is already owned by another user. By default, this check box is unchecked.

Step 7 If you want Cisco Jabber users who are associated with this user profile, to be able to use the Mobile and Remote Access feature, check the **Enable Mobile and Remote Access** check box.

Note

- By default, this check box is selected. When you uncheck this check box, the **Client Policies** section is disabled, and No Service client policy option is selected by default.
- This setting is mandatory only for Cisco Jabber users whom are using OAuth Refresh Logins. Non-Jabber users do not need this setting to be able to use Mobile and Remote Access. Mobile and Remote Access feature is applicable only for the Jabber Mobile and Remote Access users and not to any other endpoints or clients.

Step 8 Assign the Jabber policies for this user profile. From the **Desktop Client Policy**, and **Mobile Client Policy** drop-down list, choose one of the following options:

- No Service—This policy disables access to all Cisco Jabber services.
- IM & Presence only—This policy enables only instant messaging and presence capabilities.
- IM & Presence, Voice and Video calls—This policy enables instant messaging, presence, voicemail, and conferencing capabilities for all users with audio or video devices. This is the default option.

Note Jabber desktop client includes Cisco Jabber for Windows users and Cisco Jabber for Mac users. Jabber mobile client includes Cisco Jabber for iPad and iPhone users and Cisco Jabber for Android users.

Step 9 If you want the users in this user profile to set the maximum login time for Extension Mobility or Extension Mobility Cross Cluster through Cisco Unified Communications Self Care Portal, check the **Allow End User to set their Extension Mobility maximum login time** check box.

Note By default **Allow End User to set their Extension Mobility maximum login time** check box is unchecked.

Step 10 Click **Save**.

Configure Users for Mobile and Remote Access

For Cisco Jabber users, the Mobile and Remote Access access policy that you configured must be associated to your Cisco Jabber users during the LDAP sync. For more information on how to provision end users, see "*End User Configuration*" section in System Configuration Guide for Cisco Unified Communications Manager.

Configure Endpoints for Mobile and Remote Access

Provision and configure endpoints for Mobile and Remote Access:

- For Cisco Jabber clients, refer to "*Cisco Jabber Configuration Task Flow*" section in System Configuration Guide for Cisco Unified Communications Manager.
- For other endpoints, refer to "*Endpoint Device Configuration*" section in System Configuration Guide for Cisco Unified Communications Manager.

Configure Cisco Expressway for Mobile and Remote Access

For details on how to configure Cisco Expressway for Mobile and Remote Access, refer to the Mobile and Remote Access Through Cisco Expressway Deployment Guide.

MRA Failover with Lightweight Keepalives

Important This section is applicable from Release 14 onwards.

The MRA High-Availability for endpoint registration allows Cisco Webex and Cisco Jabber to detect any failure of network elements like Cisco Expressway-E, Cisco Expressway-C, and Cisco Unified Communications Manager Administration in the Registration path and take corrective action to reregister to the Unified CM through the next available path.

The endpoints send a lightweight STUN keepalive message to check connectivity in the registration path. When the Unified Communications Manager receives the lightweight STUN keepalive message, it validates the Cisco Expressway-C IP and responds to the message. The Unified CM discards the STUN keepalive message if it is received from any other IP.

If a node in the registration path fails, endpoints will learn the failure through the lightweight STUN keepalive response that they receive and selects a different route path for future messages. This service helps the user to have smooth and continuous incoming and outgoing calls irrespective of outages or other maintenance modes.

When Cisco Webex or Cisco Jabber registers to the Unified Communications Manager as a MRA device, the system displays the Expressway-C's IP in the Unified CM (**Device** > **Phone** > **IPv4 Address** column).

Note The Cisco IP Phones do not support registration failover.

For more information, see Mobile and Remote Access Through Cisco Expressway Deployment Guide.