An Overview of Cisco Unified MobilityManager

This chapter describes Cisco Unified MobilityManager and includes these sections:

- Cisco Unified MobilityManager Solution, page 1-3
- Key Features and Benefits, page 1-3
- Use Case Examples, page 1-4
- Compatibility with Cisco Unified CallManager and Related Devices and Services, page 1-5
- Administrative Web Interface, page 1-7
- Where to Find More Information, page 1-9

Definitions

Table 1-1 lists definitions of important terms used in this guide.

Table 1-1 Terms and Definitions

Term	Definition
Caller ID	Phone number that appears on the display of the receiving phone when a call is made from the remote destination.
Group	Record that ties together a set of phone lines and remote destinations for the user. Identified by Group ID. Currently one group can be added per user.
Line appearance	Desktop phone line or extension for the user. Identified by line number. Currently one line appearance can be added per user.
Mobile Connect	Set of features that enables users to manage business calls using a single phone number and pick up in-progress calls on the desktop phone and cellular phone. Mobile Connect features are supported by Cisco Unified MobilityManager.
Mobile Voice Access	An integrated voice response (IVR) system used to initiate Mobile Connect calls and to activate or deactivate Mobile Connect capabilities.

Table 1-1 Terms and Definitions

Term	Definition
Remote destination	Cellular phones that are available for Mobile Connect responses and pickup, plus other phones that are used to reach Mobile Voice Access.
User Profile	Set of records that defines a user account, identified by Mobile Voice Access User ID. The group, line appearance, and remote destinations are part of the user profile.

Cisco Unified MobilityManager Solution

Cisco Unified MobilityManager is an enterprise application server that provides Mobile Connect functionality in conjunction with Cisco Unified CallManager, Unity, and other IP communications applications. Mobile Connect refers to the set of features that includes the ability to answer incoming calls on the desktop phone or cellular phone, to pick up in-progress calls on the desktop phone or cellular phone without losing the connection, and to originate enterprise calls from the cellular phone.

Together with Cisco Unified CallManager, Cisco Unified MobilityManager controls call routing and device mobility between enterprise desktop IP phones and cellular and other remote phones. Cisco Unified MobilityManager is provided as a software application on compatible Cisco servers. A web interface is available for administrative access and for users to administer their person profiles.

Cisco Unified MobilityManager is part of Cisco AVVID (Architecture for Voice, Video and Integrated Data) and is compatible with enterprise public service telephone network (PSTN), WAN, LAN, and wireless LAN infrastructures.

The following components are required to implement the full Cisco Unified MobilityManager solution:

- Voice-enabled IP network, including LAN and PSTN voice gateways
- Enterprise CPE-based IP telephony and messaging system, including Cisco Unified CallManager, Cisco Unity voice mail applications, and Cisco Unified IP Phone 79xx Series
- Cisco Unified MobilityManager
- Existing cellular phones devices and other remote phone endpoints

Note Existing cellular phones can be used with the Cisco Unified MobilityManager with no modification to the cellular phones or cellular network. Code Division Multiple Access (CDMA) and Global System for Mobile Communications (GSM) cellular phones are compatible with the Cisco Unified MobilityManager.

Related Topics

- Key Features and Benefits, page 1-3
- Use Case Examples, page 1-4
- Administrative Web Interface, page 1-7
- Where to Find More Information, page 1-9

Key Features and Benefits

The Cisco Unified MobilityManager enables more flexible management of enterprise and cellular telephone communications and provides these benefits:

- Simultaneous desktop ringing—Incoming calls ring simultaneously on the IP phone extension and the designated mobile handset.When the user answers one line, the unanswered line automatically stops ringing. Users can choose the preferred device each time a call comes in.
- Desktop call pickup—Users can switch between desktop phone and cellular phone during an active call without losing the connection. Based on the needs of the moment, they can take advantage of the reliability of the wired office phone or the mobility of the cellular phone.

- Single enterprise voice mailbox—The enterprise voice mail box can serve as single, consolidated voicemail box for all business, including calls to the desktop or configured remote devices. Incoming callers have a predictable means of contacting employees and less time is required for users to check multiple voice mail systems.
- System remote access—A user's cellular phone can initiate calls as if it were a local IP PBX extension. User-initiated calls can take advantage of local voice gateways and WAN trunking, and the enterprise can track employee call initiation.
- Allowed Caller and Blocked Caller filters—Users can restrict the set of callers that cause a designated remote destination to ring on an incoming call (Allowed Caller filter) or for which the remote destinations do *not* ring on an incoming call (Blocked Caller filter).
- Caller ID—Caller ID is preserved and displayed on all calls. Users can take advantage of Mobile Connect with no loss of expected IP phone features.
- Remote on/off control—Users can turn their mobility features on or off from the cellular phone using Mobile Voice Access or from the user configuration pages, assuring flexibility in how mobility is managed.
- Call tracing—Detailed Mobile Connect calls are logged, providing information to help the enterprise optimize trunk usage and debug connection problems.
- Security and privacy for Mobile Connect calls—During an active Mobile Connect call, the associated desktop IP phone is secured. Access to the call from the desktop is eliminated as soon as the cellular connection becomes active, precluding the possibility of an unauthorized person listening in on the call that is bridged to the cellular phone.

Related Topics

- Cisco Unified MobilityManager Solution, page 1-3
- Use Case Examples, page 1-4
- Administrative Web Interface, page 1-7
- Where to Find More Information, page 1-9

Use Case Examples

Cisco Unified MobilityManager supports these use cases:

- Receiving an outside call on desk or cellular phone—An outside caller dials the user's desktop extension. The desktop phone and cellular phone ring simultaneously. When the user answers one of the phones, the other phone stops from a desktop telephone to a cellular phone—The user can switch from the desktop phone to cellular phone during a call without losing the connection. Switching is supported for incoming and outgoing calls.
- Moving back from a cellular phone to a desktop phone—If a call was initiated to or from the desktop phone and then shifted to the cellular phone, the call can be shifted back to the desktop phone.
- Initiating a mobility call from a remote phone, such as a cellular phone—Users can use Mobile Voice Access to initiate calls from a cellular phone as if dialing from the desktop phone.
- Moving from a cellular phone to a desktop phone during a cellular-phone initiated call—If the user has initiated a call from a cellular phone using Mobile Voice Access, the user can shift to the desktop phone during the call without losing the connection, and can shift back again as needed.

Related Topics

- Cisco Unified MobilityManager Solution, page 1-3
- Key Features and Benefits, page 1-3
- Administrative Web Interface, page 1-7
- Where to Find More Information, page 1-9

Usage Limitations

Cisco Unified MobilityManager is designed to manage a maximum of one call at a time for each configured line appearance (extension). This section describes the system response based on several calling scenarios involving Extension “A,” “B,” and “C.” In each scenario, Extension A is configured for Mobile Connect services and Mobile Voice Access, and the cellular phone is configured as a remote destination.

Scenario 1

A is idle when B calls A. A can pick up the call on the cellular phone.

Scenario 2

A makes a call to C. While the call is in progress, B calls A, who answers the call on the desktop phone. A can pick up the C call on the cellular phone, but cannot pick up B’s call on the cellular phone, since Mobile Connect services are being used for the C call.

Scenario 3

B calls A, who picks the call up on the cellular phone. While the call is in progress, C calls A, who answers on the desktop phone. A now ends B’s call and continues with C. Mobile Connect services will be available for the next incoming call to A.

Scenario 4

B calls A, who picks the call up on the cellular phone. While the call is in progress, C calls A, who answers on the desktop phone. A now ends C’s call and continues with B. The B call is still using Mobile Connect services, so no other call can use the service until the B call is terminated.

Scenario 5

A uses a cellular phone to make a Mobile Voice Access call. While the call is in progress, C calls A’s extension. The call will not be extended to the cellular phone, since A was using Mobile Voice Access when the call from C came in. After A hangs up the Mobile Voice Access call, Mobile Connect services can be applied to the next incoming call.

Compatibility with Cisco Unified CallManager and Related Devices and Services

Cisco Unified MobilityManager is integrated with Cisco Unified CallManager. Most of the standard Cisco Unified CallManager features are compatible with Cisco Unified MobilityManager and related devices and services, except as indicated here:

- To use Mobile Connect features, you must first disable the Auto Call Pickup feature in Cisco Unified CallManager.

- The Cisco Unified CallManager Forced Authorization Code and Client Matter Code (FAC/CMC) feature does not work with Mobile Voice Access. JAVA telephony programming interface (JTAPI) does not support the events required for FAC/CMC.
- In order for Cisco Unified MobilityManager to support different types of codecs, a transcoder must be configured in Cisco Unified CallManager for shared line CTI ports.
- Mobile Connect does not work with Multilevel Precedence and Preemption (MLPP). If a call is preempted with MLPP, Mobile Connect features are disabled for that call.
- Mobile Connect services do not extend to video calls. A video call received at the desktop phone cannot be picked up on the cellular phone.
- Remote destinations must be Time Division Multiplex (TDM) devices. You cannot configure IP phones within a Cisco Unified CallManager cluster as remote destinations.
- Mobile Connect services are available only to directory numbers (DNs) that are in the same partition as the Shared Line CTI User. If the same DN is used in two different partitions, service is only extended to the DN in the same partition as the Shared Line CTI User.
- CDR Analysis and Reporting (CAR) support is not available with Cisco Unified MobilityManager.
- The H.323 gateway does not support failover of Cisco Unified CallManager. If the primary Cisco Unified CallManager goes out of service for some reason and the secondary takes over, the in-progress Mobile Connect calls will be dropped.
- When the outbound H.323 dial-peer is down or is unavailable and remote access calls are attempted, the CTI ports are not released after the call is completed. Although the calls are unsuccessful and are properly released, some CTI ports become unusable and are not released by Cisco Unified MobilityManager. To avoid this problem, disable the System Remote Access parameter when H.323 dial-peers are shut down or are unavailable.
- If two or more users share the same extension number, the parameters configured on the Line Appearances page correspond to the most recent update. Only one set of parameters is stored in Cisco Unified MobilityManager for each extension, whether or not the extension is shared by multiple users.
- Users cannot access Meet-Me using Mobile Voice Access.
- Cisco Unified MobilityManager does not support QSIG (Q Signaling) path replacement.
- When configuring CTI ports for outgoing calls, make sure the Media Resource group for the CTI Ports does not include Music-On-Hold (MOH) servers.
- Cisco IPT Platform Administration supports creation of remote support accounts. The Cisco Unified MobilityManager server cannot serve as the export target machine for remote access, because scp and sftp access are not permitted.
-

Administrative Web Interface

This section explains how to access the Cisco Unified MobilityManager administration application from a web browser running on your PC.

- Cisco Unified MobilityManager Solution, page 1-3
- Web Browsers, page 1-7
- Using Internet Explorer with Cisco Unified MobilityManager Administration, page 1-7

Web Browsers

The Cisco Unified MobilityManager administration application supports the following Microsoft Windows operating system browsers:

- Microsoft Internet Explorer, version 6.0 or later
- Netscape Navigator version, 7.2 or later

The administrative interface can be reached from any user PC in your network. For instructions on logging in, see the "Accessing Cisco Unified MobilityManager Administration" section on page 2-2.

Related Topics

- Cisco Unified MobilityManager Solution, page 1-3
- Using Internet Explorer with Cisco Unified MobilityManager Administration, page 1-7
- Using Netscape with Cisco Unified MobilityManager Administration, page 1-8

Using Internet Explorer with Cisco Unified MobilityManager Administration

You can save the certificate authority (CA) root certificate in the trusted folder so that the Security Alert dialog box does not display each time that you access the web application. The first time that you or a user accesses Cisco Unified MobilityManager Administration, a Security Alert dialog box asks whether you trust the server. You must select *one* of the these options:

- Click **Yes** to trust the certificate for the current web session only. If you trust the certificate for the current session only, the Security Alert dialog box opens each time that you access the application, unless you install the certificate in the trusted folder.
- Choose **View Certificate** > **Install Certificate** to perform certificate installation tasks. If you install the certificate in the trusted folder, the Security Alert dialog box does not display each time that you access the web application.
- Click **No** to cancel the action. No authentication occurs, and you cannot access the web application.

To save the security certificate, follow these steps:

Procedure

Step 1 Browse to the Cisco Unified MobilityManager Administration web page (see "Accessing Cisco Unified MobilityManager Administration" section on page 2-2).

Step 2 When the Security Alert dialog box displays, click **View Certificate**.

Step 3 In the Certificate pane, click **Install Certificate**.

Step 4 Click **Next**.

Step 5 Click the **Place all certificates in the following store** radio button; click **Browse**.

Step 6 Browse to **Trusted Root Certification Authorities**.

Step 7 Click **Next**.

Step 8 Click **Finish**.

Step 9 To install the certificate, click **Yes**.

A message states that the import was successful.

Step 10 Click **OK**.

Step 11 In the lower, right corner of the dialog box, click **OK**.

Step 12 To trust the certificate so you do not receive the dialog box again, click **Yes**.

Note If you use the localhost, the IP address, or the hostname in the URL to access the application that supports HTTPS, you must save the certificate in the trusted folder for each of type of URL (with the local host, IP address, and so on); otherwise, the Security Alert dialog box displays for each type.

Related Topics

- Cisco Unified MobilityManager Solution, page 1-3
- Using Netscape with Cisco Unified MobilityManager Administration, page 1-8

Using Netscape with Cisco Unified MobilityManager Administration

Using Netscape, you can view the certificate credentials, trust the certificate for one session, trust the certificate until it expires, or not trust the certificate at all.

Tip If you trust the certificate for one session only, you must repeat the following procedure each time that you access the HTTPS-supported application. If you do not trust the certificate, you cannot access the application.

To save the certificate to the trusted folder, follow these steps:

Procedure

Step 1 Access the application through Netscape.

Step 2 After the New Site Certificate window displays, click **Next**.

Step 3 After the next New Site Certificate window displays, click **Next**.

Tip To view the certificate credentials before you click Next, click **More Info**. Review the credentials, and click **OK**.; then, click **Next** in the New Site Certificate window.

Step 4 Click one of the following radio buttons:

- Accept this certificate for this session
- Do not accept this certificate and do not connect
- Accept this certificate forever (until it expires)

Step 5 Click **Next**.

Step 6 If you clicked the Do not accept this certificate... radio button, go to Step 8.

Step 7 If you want Netscape to warn you before sending information to other sites, check the **Warn me before I send information to this site** check box; then, click **Next**.

Step 8 Click **Finish**.

Related Topics

- Cisco Unified MobilityManager Solution, page 1-3
- Using Internet Explorer with Cisco Unified MobilityManager Administration, page 1-7

Where to Find More Information

See the following documents for additional information on web interfaces to Cisco Unified MobilityManager and Cisco Unified CallManager.

- *Cisco Unified CallManager System Guide*
- *Cisco IP Telephony Solution Reference Network Design Guide*
- *Cisco Unified MobilityManager Installation Guide*