Configuration Guide for Cisco UC Integration for Cisco WebEx Connect C7

Revised: March 7, 2011

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Configuration Guide for Cisco UC Integration for Cisco WebEx Connect C7

CONTENTS

CHAPTER 1

Getting Started

Cisco UC Integration for Cisco WebEx Connect C7 adds a phone tab to Cisco WebEx Connect. This new space turns your computer into a full-featured phone, permitting you to place, receive, and manage calls.

Cisco UC Integration for Cisco WebEx Connect C7 is built on a client services framework integration which provides call control services, call history, message waiting indicators, media, and so on.

The Cisco WebEx Connect service in the cloud provides the remaining services, including instant messaging, presence, and spaces. You can perform the following tasks from the phone tab:

- Place and receive phone calls.
- Call your voice message service.
- Display your communications history.
- Set options for the communications pane.
- Switch phone modes. You can select whether you want to control your desk phone from the computer or use the audio and microphone on your computer to handle calls. You can easily toggle between these options.

Supported Server Versions

Product	Supported Version
Cisco Unified Communications Manager	CUCM 6.1(4)
	CUCM 7.1(5) (3)
	CUCM 8.0(1)
	CUCM 8.5
Cisco Unity with Microsoft Exchange 2003 or Microsoft Exchange 2007	Unity 8.0*
Cisco Unity Connection	Unity Connection 8.0*
	Unity Connection 8.5*

Note *Cisco Unity and Cisco Unity Connection versions are only required for Visual Voicemail. For additional information, review the Cisco Unified Communications Manager compatibility matrix at: http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/compat/ccmcompmatr.html

Ports Used for Outbound Traffic by Cisco Unified Client Services Framework

Port	Protocol	Description
69	UDP	Connects to the Trivial File Transfer Protocol (TFTP) server to download the TFTP file.
2748	TCP	Connects to the CTI gateway, which is the CTIManager component of Cisco Unified Communications Manager.
5060	UDP/TCP	Provides Session Initiation Protocol (SIP) call signalling.
5061	TCP	Provides secure SIP call signalling.
8443	TCP	Connects to the Cisco Unified Communications Manager IP Phone (CCMCIP) server to get a list of currently-assigned devices.
16384-32766	UCP	Sends RTP media streams for audio.
16384-32766	UDP	Receives Real-Time Transport Protocol (RTP) media streams for audio and video. These ports are configured in Cisco Unified Communications Manager.

Client Computer Requirements

Hardware Requirements for Cisco UC Integration for Cisco WebEx Connect

Item	Description
Memory	Microsoft Windows 7: 2 GB Microsoft Windows Vista: 2 GB Microsoft Windows XP: 1 GB
Available disk space	200 MB
Connectivity	Download bandwidth: 80 Kbps Upload bandwidth: 80 Kbps
Processor	
Desktop	2.4 GHz
Laptop	1.8 GHz

Software Requirements for Cisco UC Integration for Cisco WebEx Connect

Item	Description
Operating system	Windows 7 Professional or Ultimate, 32-bit or 64-bit (in WOW mode) Windows Vista SP2 Business or Ultimate, with DirectX 10, 32-bit or 64-bit (in WOW mode) Windows XP SP3 with DirectX 9.0c, 32-bit only Minimum disk space is 80MB

Supported Cisco Unified IP Phones

The following table lists the Cisco Unified IP Phone models that are supported for Cisco UC Integration for Cisco WebEx Connect C7, and whether Skinny Call Control Protocol (SCCP) and Session Initiation Protocol (SIP) are supported:

Phone	SCCP	SIP
Cisco IP Communicator	Yes	Yes
9971 (w/ and w/o video)	No	Yes
9951	No	Yes
8961	No	Yes
7985G	Yes	No
7975G	Yes	Yes
7971G	Yes	Yes
7970G	Yes	Yes
7965G	Yes	Yes
7962G	Yes	Yes
7961G-GE	Yes	Yes
7961G	Yes	Yes
7960G	Yes	No
7945G	Yes	Yes
7942G	Yes	Yes
7941G-GE	Yes	Yes
7941G	Yes	Yes
7940G	Yes	No
7931G	Yes	No
7925G	Yes	No
7921G	Yes	No
7920G	Yes	No
7912G	Yes	No
7911G	Yes	Yes
7910G	Yes	No
7906G	Yes	Yes
7905G	Yes	No
7902G	Yes	No
6961	Yes	No
6941	Yes	No
6921	Yes	No

Tested Audio Devices

The audio headset devices tested with Cisco UC Integration for Cisco WebEx Connect are as follows:

- Polycom Speakerphone USB
- ClearOne CHAT 50 USB
- Jabra GN8110 USB
- Jabra GN8120 USB
- Jabra GN9120
- Jabra Advantage Plus
- Plantronics CS50
- Plantronics CS60
- Plantronics DA60 USB
- Plantronics DSP-400
- Plantronics DA55 USB
- Plantronics Voyager 510 Bluetooth
- Clarisys i750
- Futiro USB
- Sonic EV-87
- PLANTRONICS Blackwire C620
- Logitech USB H330
- Logitech960 USB
- SONIC DT-301
- Lenonvo
- PLANTRONICS WG200
- PLANTRONICS W430

For information about Cisco IP Phones, refer to publications that are specific to your language, phone model, and Cisco Unified Communications Manager release. Navigate from the following URL:

http://www.cisco.com/cisco/web/psa/maintain.html?mode=prod&level0=278875240

Note For 7931G phones to function correctly with Cisco UC Integration for Cisco WebEx Connect, you must set the value of the Outbound Call Rollover to field to **No Rollover** in Cisco Unified Communications Manager.

About Voice Quality

Cisco UC Integration for Cisco WebEx Connect is designed to provide premium voice quality under a variety of conditions; however, in some instances users may notice interruptions of audio transmission or temporary audio distortions ("Artifacts") which are considered a normal part of the operation of the application. These artifacts should be infrequent and temporary when using:

- Cisco UC Integration for Cisco WebEx Connect on a workstation meeting the recommended configuration requirements.
- A network that meets the recommended quality criteria in the Cisco Unified Communication Solution Reference Design Document.

We take reasonable measures to interface with the operating system in ways that decrease the likelihood that other applications running on the system will interfere with softphone audio and video quality. However, the shared nature of system environments in which these products run is very different than a closed environment like Cisco Unified IP Phones and we cannot guarantee equivalent performance.

The following are some conditions that may cause artifacts:

- Spike in usage of the CPU of the personal computer - where CPU utilization is between 75 to 100% - due to launching applications, system processes or processing happening within other applications running.
- The system is running low on available physical memory.
- Other applications using large amounts of bandwidth to or from the workstation to the network.
- Other network bandwidth impairments.
- Dynamic reduction in CPU clock speed due to power management policy (for example, laptops running on battery power) or thermal protection causing the CPU to run in a more highly-loaded condition.
- Any other condition that causes the application to lose timely access to the network or audio system, for example, interference from third-party software.

Avoiding or recovering from the conditions previously listed will help minimize audio distortion artifacts.

Important Notes

Warning **IMPORTANT NOTICE - PLEASE READ: During an emergency, softphone technology may not provide the most timely or accurate location data if used for a 911 emergency call. Calls may be misdirected to the wrong emergency response center or the emergency response center may make errors when determining your location. USE A SOFTPHONE ONLY AT YOUR OWN RISK DURING AN EMERGENCY. Cisco will not be liable for resulting errors or delays.**

CHAPTER 2

Configuring the Device Type on Cisco Unified Communications Manager

Configuring Cisco Unified Communications Manager for Cisco UC Integration for Cisco WebEx Connect, involves adding the device type to Cisco Unified Communications Manager and setting up the directory number. Before you begin you must have a properly working Cisco Unified Communications configuration with the following services enabled:

- Cisco Unified Communications Manager service. For information about the Cisco Unified Communications Manager service see the documentation at the following URL:

  http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_general_information.html

- Cisco Trivial File Transfer Protocol (TFTP) service. For information about Cisco TFTP service, see the *Cisco Unified Communications Manager System Guide* at the following URL:

  http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

- Cisco CTIManager service. For information about Cisco CTIManager service, see the *Cisco Unified Communications Manager System Guide* at the following URL:

  http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

- Cisco Unified Communications Manager IP Phone (CCMCIP) service.

Note Administrators do not control the CCMCIP service. It is on by default and administrators should configure their clients to use the CUCM Subscriber for the CCMCIP Service.

Preparing Cisco Unified Communications Manager

The Cisco UC Integration for Cisco WebEx Connect requires a new Cisco Unified Communications Manager device type called Client Services Framework. Depending on which release of Cisco Unified Communications Manager is installed in your Cisco Unified Communications system, you might need to patch Cisco Unified Communications Manager with a Cisco Options Package (COP) file.

You must run the COP file if your Cisco Unified Communications Manager does not have the Client Services Framework device type. You run the COP file on the Cisco Unified Communications Manager publisher server. After you apply the COP file, you must restart the Cisco Unified Communications Manager publisher server, and all other servers.

The COP file is available from the Administration Toolkit. To access the Administration Toolkit, navigate to Cisco UC Integration for Cisco WebEx Connect from the Download Software page at the following URL:

http://www.cisco.com/cisco/software/release.html?mdfid=282811017&flowid=5464&softwareid=282888767&release=7.1(6)&rellifecycle=&relind=AVAILABLE&reltype=latest

For more information refer to the Cisco Unified Communications Manager release notes:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/rel_notes/7_0_1/cucm-rel_notes-701.html#wp684478

Creating Devices and Directory Numbers for Users

Procedure

Step 1 Select **Device > Phone** in Cisco Unified Communications Manager Administration.

Step 2 Select **Add New**.

Step 3 From the Phone Type drop down box, select **Cisco Unified Client Services Framework**.

Step 4 Select **Next**.

Step 5 Enter information for the phone in the Phone Configuration window, as follows:

Field	Description
Device Information	
Device Name	Enter a name to identify the Cisco Unified Client Services Framework device. The name contains character including alphanumeric characters, periods, hyphens, and underscores. The device name does not need to relate to the user ID of the user.
Description	(Optional) Enter a description of the device.
Device Pool	Select the device pool to which you want the phone assigned. The device pool defines sets of common characteristics for devices, such as region, date/time group, softkey template, and Multilevel Precedence and Preemption (MLPP) information.
Common Device Configuration	(Optional) Select the common device configuration to which you want this device assigned. The common device configuration includes the attributes (services or features) that are associated with a particular user.
Phone Button Template	Select the applicable phone button template. The phone button template determines the configuration of buttons on a phone and identifies which feature (line, speed dial, and so on) is used for each button.
Common Phone Profile	Select a name to identify the phone profile.
Calling Search Space	(Optional) Select from the list of partitions. A calling search space comprises a collection of partitions that are searched for numbers that are called from this directory number. The value that you select applies to all devices that are using this directory number.
Media Resource Group List	(Optional) This window lists the media resource groups. The list includes only previously defined media resource groups and are listed in order of priority highest to lowest.

Field	Description
User Hold MOH Audio Source	(Optional) Select to the sound plays when a user initiates a hold action.
Network Hold MOH Audio Source	(Optional) Select to the sound plays when the network initiates a hold action.
Location	Select a location to change the RSVP policy setting.
User Locale	(Optional) Select to identify a set of detailed information to support end users including language and font.
Network Locale	(Optional) Select the locale that is associated with the gateway. The network locale identifies a set of detailed information to support the hardware in a specific location. The network locale contains a definition of the tones and cadences that are used by the device in a specific geographic area. **Note**: Select only a network locale that is already installed and supported by the associated devices. The list contains all available network locales for this setting, but not all are necessarily installed. If the device is associated with a network locale that it does not support in the firmware, the device will fail to come up.
Device Mobility Mode	Turn the device mobility feature on or off for this device or select Default to use the default device mobility mode. The default setting uses the value for the Device Mobility Mode service parameter for the device.
Owner User ID	(Optional) Select 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. **Note**: Do not configure this field if you are using extension mobility. Extension mobility does not support device owners. **Note**: The Owner User ID and Mobility User ID can differ.
Mobility User ID	(Optional) Select the user ID of the person to whom this dual-mode phone is assigned. **Note**: The Mobility User ID configuration is used for the Mobile Connect and Mobile Voice Access features for dual-mode phones. **Note**: The Owner User ID and Mobility User ID can differ.
Primary Phone	(Optional) Select the physical phone that will be associated with the application, such as IP communicator or Cisco Unified Communications Integration. When you select a primary phone, the application consumes fewer device license units and is considered an “adjunct” license (to the primary phone).

Field	Description
Use Trusted Relay Point	Enable or disable whether Cisco Unified Communications Manager inserts a trusted relay point (TRP) device with this media endpoint. Select one of the following values: • Default - If you select this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates. • Off - Select this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On - Select this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point.
Always Use Prime Line	Enable or disable one of the following options: • Default - Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter, which supports the Cisco CallManager service. • Off - When the phone is idle and receives a call on any line, the phone user can answer the call from the line on which the call is received. • On - When the phone is idle (off hook) and receives a call on any line, the primary line gets selected for the call. Calls on other lines continue to ring, and the phone user must select those other lines to answer these calls.
Always Use Prime Line for Voice Message	Enable or disable one of the following options: • On - If the phone is idle, the primary line on the phone becomes the active line for retrieving voice messages when the phone user presses the Messages button on the phone. • Off - If the phone is idle, pressing the Messages button on the phone automatically dials the voice-messaging system from the line that has a voice message. Cisco Unified Communications Manager always selects the first line that has a voice message. If no line has a voice message, the primary line gets used when the phone user presses the Messages button. • Default - Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line for Voice Message service parameter, which supports the Cisco CallManager service.

Field	Description
Calling Party Transformation CSS	(Optional) This setting permits you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you select contains the calling party transformation pattern that you want to assign to this device. **Tip**: Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the Calling Party Transformation CSS as None, the transformation does not match and does not get applied. Verify that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.
Geolocation	(Optional) Select the Unspecified geolocation which designates that this device does not associate with a geolocation.
Use Device Pool Calling Party Transformation CSS	Check this box to use the Calling Party Transformation CSS that is configured in the device pool assigned to this device. If you do not select this check box, the device uses the Calling Party Transformation CSS that you selected in the Phone Configuration window.
Ignore Presentation Indicators (internal calls only)	Check this box to configure call display restrictions on a call-by-call basis. When this check box is checked, Cisco Unified Communications Manager ignores any presentation restriction that is received for internal calls.
Allow Control of Device from CTI	Select this option if you want Cisco UC Integration for Cisco WebEx Connect to control and monitor the desk phone of the user with the Computer Telephony Integration (CTI) server. Ensure that the user is added to the Standard CTI Enabled user group.
Logged Into Hunt Group	Check this box to indicate that the phone is currently logged in to a hunt list (group). When the phone is added to a hunt list, the administrator can log the user in or out by checking (and unchecking) this check box. Users use the softkey on the phone to log their phone in or out of the hunt list.
Remote Device	Check this box if you are experiencing delayed connect times over SCCP pipes to remote sites. Selecting this check box tells the Cisco Unified Communications Manager to allocate a buffer for the phone device when it registers and to bundle SCCP messages to the phone. **Tip**: Because this feature consumes resources, be sure to check this check box only when you are experiencing signaling delays for phones that are running SCCP. Most users do not require this option.
Protocol Specific Information	

Field	Description
Packet Capture Mode	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. Select one of the following options from the drop-down list box: • None - This option, which serves as the default setting, indicates that no packet capturing is occurring. After you complete packet capturing, configure this setting. • Batch Processing Mode - Cisco Unified Communications Manager writes the decrypted or non encrypted messages to a file, and the system encrypts each file. On a daily basis, the system creates a new file with a new encryption key. Cisco Unified Communications Manager, which stores the file for seven days, also stores the keys that encrypt the file in a secure location. Cisco Unified Communications Manager stores the file in the PktCap virtual directory. A single file contains the time stamp, source IP address, source IP port, destination IP address, packet protocol, message length, and the message. The TAC debugging tool uses HTTPS, administrator username and password, and the specified day to request a single encrypted file that contains the captured packets. Likewise, the tool requests the key information to decrypt the encrypted file.
Packet Capture Duration	(Optional) This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. This field specifies the maximum number of minutes that is allotted for one session of packet capturing. The default setting equals 0, although the range exists from 0 to 300 minutes. To initiate packet capturing, enter a value other than 0 in the field. After packet capturing completes, the value, 0, displays.
Presence Group	Select a Presence group for the end user. The selected group specifies the devices, end users, and application users that can monitor this directory number. The default value for Presence Group specifies Standard Presence group, configured with installation. Presence groups that are configured in Cisco Unified Communications Manager Administration also appear in the drop-down list box.
SIP Dial Rules	(Optional) Select the appropriate SIP dial rule. SIP dial rules provide local dial plans for Cisco Unified IP Phones 7905, 7912, 7940, and 7960, so users do not have to press a key or wait for a timer before the call gets processed. Leave the SIP Dial Rules field set to <None> if you do not want dial rules to apply to the IP phone that is running SIP. This means that the user must use the Dial softkey or wait for the timer to expire before the call gets processed.
MTP Preferred Originating Codec	(Optional) Select the codec to use if a media termination point is required for SIP calls.

Field	Description
Device Security Profile	Select the security profile you require for the phone. If you select Client Services Framework- Standard SIP Secure Profile, do the following: 1. Enter certification and authentication information in the Certification Authority Proxy Function (CAPF) Information section. 2. Select Generate String. 3. Email the contents of the Authentication String field to the user.
Rerouting Calling Search Space	(Optional) Select a calling search space to use for rerouting. The rerouting calling search space of the refered is used to find the route to the refer-to target. When the Refer fails due to the rerouting calling search space, the Refer Primitive rejects the request with the “405 Method Not Allowed” message. The redirection (3xx) primitive and transfer feature also uses the rerouting calling search space to find the redirect-to or transfer-to target.
SUBSCRIBE Calling Search Space	(Optional) From the drop-down list box, select the SUBSCRIBE calling search space to use for presence requests for the phone. All calling search spaces that you configure in Cisco Unified Communications Manager Administration display in the SUBSCRIBE Calling Search Space drop-down list box. If you do not select a different calling search space for the end user from the drop-down list, the SUBSCRIBE calling search space defaults to None. To configure a SUBSCRIBE calling search space specifically for this purpose, you configure a calling search space as you do all calling search spaces. Supported with the Presence feature, the SUBSCRIBE calling search space determines how Cisco Unified Communications Manager routes presence requests that come from the phone. This setting permits you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the phone.
SIP Profile	Select the default SIP profile or a specific profile that was previously created. SIP profiles provide specific SIP information for the phone such as registration and keepalive timers, media ports, and do not disturb control.
Digest User	(Optional) Select the default SIP profile or a specific profile that was previously created. SIP profiles provide specific SIP information for the phone such as registration and keepalive timers, media ports, and do not disturb control.

Field	Description
Media Termination Point Required	Use this field to indicate whether a media termination point is used to implement features that H.323 does not support (such as hold and transfer). Select the Media Termination Point Required check box to use an MTP to implement features. Uncheck the Media Termination Point Required check box if you do not want to use an MTP to implement features. Use this check box only for H.323 clients and those H.323 devices that do not support the H.245 empty capabilities set or if you want media streaming to terminate through a single source. If you check this check box to require an MTP and this device becomes the endpoint of a video call, the call will be audio only.
Unattended Port	Check this check box to indicate an unattended port on this device.
Require DTMF Reception	Select this check box to require DTMF reception for this phone and phones that are running SIP and SCCP, **Note**: In configuring Cisco Unified Mobility features, when using intercluster DNs as remote destinations for an IP phone via SIP trunk (either intercluster trunk [ICT] or gateway), check this check box so that DTMF digits can be received out of band, which is crucial for Enterprise Feature Access midcall features.
Certification Authority Proxy Function (CAPF) Information	
Certificate Operation	From the drop-down list box, select one of the following options: • No Pending Operation - Displays when no certificate operation is occurring (default setting). • Install/Upgrade - Installs a new or upgrades an existing locally significant certificate in the phone. • Delete - Deletes the locally significant certificate that exists in the phone. • Troubleshoot - Retrieves the locally significant certificate (LSC) or the manufacture installed certificate (MIC), so you can view the certificate credentials in the CAPF trace file. If both certificate types exist in the phone, Cisco Unified Communications Manager creates two trace files, one for each certificate type. By choosing the Troubleshooting option, you can verify that an LSC or MIC exists in the phone.

Field	Description
Authentication Mode	This field permits you to select the authentication method that the phone uses during the CAPF certificate operation. From the drop-down list box, select one of the following options: • By Authentication String - Installs/upgrades, deletes, or troubleshoots a locally significant certificate only when the user enters the CAPF authentication string on the phone. • By Null String - Installs/upgrades, deletes, or troubleshoots a locally significant certificate without user intervention. This option provides no security; Cisco strongly recommends that you select this option only for closed, secure environments. • By Existing Certificate (Precedence to LSC) - Installs/upgrades, deletes, or troubleshoots a locally significant certificate if a manufacture-installed certificate (MIC) or locally significant certificate (LSC) exists in the phone. If a LSC exists in the phone, authentication occurs via the LSC, regardless whether a MIC exists in the phone. If a MIC and LSC exist in the phone, authentication occurs via the LSC. If a LSC does not exist in the phone, but a MIC does exist, authentication occurs via the MIC. Before you select this option, verify that a certificate exists in the phone. If you select this option and no certificate exists in the phone, the operation fails. At any time, the phone uses only one certificate to authenticate to CAPF even though a MIC and LSC can exist in the phone at the same time. If the primary certificate, which takes precedence, becomes compromised for any reason, or, if you want to authenticate via the other certificate, you must update the authentication mode. • By Existing Certificate (Precedence to MIC) - Installs, upgrades, deletes, or troubleshoots a locally significant certificate if a LSC or MIC exists in the phone. If a MIC exists in the phone, authentication occurs via the MIC, regardless whether a LSC exists in the phone. If a LSC exists in the phone, but a MIC does not exist, authentication occurs via the LSC. Before you select this option, verify that a certificate exists in the phone. If you select this option and no certificate exists in the phone, the operation fails. **Note**: The CAPF settings that are configured in the Phone Security Profile window interact with the CAPF parameters that are configured in the Phone Configuration window.
Authentication String	(Optional) If you select the By Authentication String option in the Authentication Mode drop-down list box, this field applies. Manually enter a string or generate a string by clicking the Generate String button. Verify the string contains 4 to 10 digits. To install, upgrade, delete, or troubleshoot a locally significant certificate, the phone user or administrator must enter the authentication string on the phone.

Field	Description
Key Size (Bits)	Select the key size for the certificate from the drop-down list box. The default setting equals 1024. Other options include 512 and 2048. If you select a higher key size than the default setting, the phones take longer to generate the entropy that is required to generate the keys. Key generation, which is set at low priority, allows the phone to function while the action occurs. Depending on the phone model, you may notice that key generation takes up to 30 or more minutes to complete. **Note**: The CAPF settings that are configured in the Phone Security Profile window interact with the CAPF parameters that are configured in the Phone Configuration window.
Operation Completes By	(Optional) This field, which supports the Install/Upgrade, Delete, and Troubleshoot Certificate Operation options, specifies the date and time in which you must complete the operation. The values that display apply to the publisher database server.
Extension Information	
Enable Extension Mobility	
Log Out Profile	(Optional)
MLPP Information	
MLPP Domain	(Optional) Select an MLPP domain from the drop-down list box for the MLPP domain that is associated with this device. If you leave the None value, this device inherits its MLPP domain from the value that was set for the device pool of the device. If the device pool does not have an MLPP domain setting, this device inherits its MLPP domain from the value that was set for the MLPP Domain Identifier enterprise parameter.
Do Not Disturb	
Do Not Disturb	Check this check box to enable Do Not Disturb on the phone.

Field	Description
DND Option	When you enable DND on the phone, this parameter permits you to specify how the DND features handle incoming calls: • Call Reject - This option specifies that no incoming call information gets presented to the user. Depending on how you configure the DND Incoming Call Alert parameter, the phone may play a beep or display a flash notification of the call. • Ringer Off - This option turns off the ringer, but incoming call information gets presented to the device, so the user can accept the call. • Use Common Phone Profile Setting - This option specifies that the DND Option setting from the Common Phone Profile window will get used for this device. **Note**: For 7940/7960 phones that are running SCCP, you can only choose the Ringer Off option. For mobile devices and dual-mode phones, you can only choose the Call Reject option. When you activate DND Call Reject on a mobile device or dual-mode phone, no call information gets presented to the device.
DND Incoming Call Alert	(Optional) When you enable the DND Ringer Off or Call Reject option, this parameter specifies how a call will be displayed. From the drop-down list, select one of the following options: • None - This option specifies that the DND Incoming Call Alert setting from the Common Phone Profile window gets used for this device. • Disable - This option disables both beep and flash notification of a call, but, for the DND Ringer Off option, incoming call information still gets displayed. For the DND Call Reject option, no call alerts display, and no information gets sent to the device. • Beep Only - For an incoming call, this option causes the phone to play a beep tone only. • Flash Only - For an incoming call, this option causes the phone to display a flash alert.

Note Cisco UC Integration for Cisco WebEx Connect does not support secure phone device configurations.

Step 6 Select **Save**.

Step 7 Click **Apply Config** to activate the settings.

Step 8 Click **OK**.

Step 9 Select the **Add a new DN** (directory number) link in the Association Information section on the Phone Configuration window.

Step 10 Enter information for the directory number in the Directory Number Configuration window.

Step 11 Select **Save**.

Step 12 Select **Associate End Users** in the Directory Number Configuration window.

Step 13 Search for the user in the Find and List Users window, select the user, then select **Add Selected**.

Step 14 Select **Save**.

Step 15 Select **User Management** > **End User** in Cisco Unified Communications Manager Administration.

Step 16 Search for the user in the Find and List Users window, then select the user.

Step 17 Associate the CSF that the device is listed for the user in the Controlled Devices list box in the Device Associations group.

QoS Packet Marking on Windows Vista

Quality of Service (QoS) packet marking requires administrator privileges for Windows Vista computers in Active Directory 2003 domains. Therefore users must have administrator privileges to overcome this operating system limitation and enable QoS packet marking for CSF deployments on Windows Vista on Active Directory 2003 domains.

For Windows Vista computers in Active Directory 2008 Domains you can use Group Policy to overcome this limitation, as described in the following procedure.

Enabling Packet Marking for CSF with Active Directory 2008 on Windows Vista

Procedure

Step 1 Start the Group Policy Management Editor application.

Step 2 Expand the **User Configuration** node.

Step 3 In Policies > Windows Settings, right-click **Policy-based QoS**, then select **Create new policy**.

For example, create a policy called Cisco CSF UDP.

Step 4 Check **Specify DSCP Value**, and enter 46 as the value, to mark traffic as expedited forwarding (EF).

Step 5 Select **Next**.

Step 6 Select the **Only applications with this executable name** option, then enter the following executable name:

cucsf.exe

Step 7 Select **Next**.

Step 8 Specify that the QoS policy applies to any pair of source and destination IP addresses. To do this, select the following options:

- **Any source IP address**
- **Any destination IP address**

Step 9 Select **Next**.

Step 10 Select the protocol to which the QoS policy applies, then specify the port or port ranges for the source and destination of the traffic.

For example, select UDP, and select **From any source port** and **To any destination port**.

Step 11 Select **Finish**.

Step 12 Apply the group policy you created to your client computers.

The settings that are applied to the client computers from the example above are as follows:

```
[HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\QoS\Cisco CSF UDP]
"Version"="1.0"
"Application Name"="cucsf.exe"
"Protocol"="UDP"
"Local Port"="*"
"Local IP"="*"
"Local IP Prefix Length"="*"
"Remote Port"="*"
"Remote IP"="*"
"Remote IP Prefix Length"="*"
"DSCP Value"="46"
"Throttle Rate"="-1"
```

CHAPTER 3

Configuring and Installing Dialing Rules

Dialing rules provide phone number translation between the directory service and Cisco Unified Communications Manager.

Application dialing rules automatically strip numbers from or add numbers to telephone numbers that a user dials. For example, the dialing rules automatically add the digit 9 in front of a 7-digit telephone number to provide access to an outside line. Directory lookup rules transform caller identification numbers into numbers that can be looked up in the directory.

You must create a set of dialing rules for contact name resolution. You must configure and export application dialing rules and directory lookup dialing rules every time dialing rules are changed. An XML file is created that Cisco Unified CSF clients download and interpret.

Contact name resolution is required to access all functionality offered by Cisco UC Integration for Cisco WebEx Connect. Numbers entered by users in their profile settings must be synchronized with Cisco Unified Communications Manager settings. These numbers can also be set in the Cisco WebEx Connect Administration Console.

Tip Ensuring that these rules exist and are available is a requirement. Most dialing related issues are a result of non-existent rules, old rules, or invalid rules.

Configuring Dialing Rules

For detailed conceptual and task-based information on dialing rules, see the Cisco Unified Communications Manager Administration online help or the Cisco Unified Communications Manager Administration Guide and the Cisco Unified Communications Manager System Guide:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

The following rule types are required:

- Application dialing rules
- Directory lookup dialing rules

Note You may already have these rules configured for other Cisco applications. If they exist, you may skip the following procedure.

Installing Dialing Rules

If your Cisco Unified Communications Manager uses dialing rules, you must ensure that Cisco UC Integration for Cisco WebEx Connect can access these dialing rules.

You must run a Cisco Options Program (COP) file to generate copies of the dialing rules in XML format, which Cisco UC Integration for Cisco WebEx Connect can access, download and interpret. The COP file is available from the Administration Toolkit. To access the Administration Toolkit, navigate to Cisco UC Integration for Cisco WebEx Connect from the Download Software page at the following URL:

http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875240

Procedure

Step 1 Select Cisco Unified Operating System Administration from the right-side navigation drop-down box.

Step 2 Click Go.

Step 3 Select Install/Upgrade.

Step 4 Specify the Software Location criteria.

Step 5 Select Next.

Step 6 Select the appropriate COP file from the Available Software list box.

Step 7 Select **Next, Install.**

Verifying the Dialing Rules Installation

Verify that the following files are present in the /usr/local/cm/tftp/CUPC directory of the TFTP server:

- AppDialRules.xml
- DirLookupDialRules.xml

Restarting the TFTP Service

After you verify the generation of the copies of the dialing rules, restart the TFTP service. You only have to run the COP file on one server in the cluster. The files are synced across the cluster. Then restart TFTP on every server that is running TFTP to recognize these files.

For information about how to restart TFTP services, see Cisco Unified Serviceability Administration Guide at the following URL:
http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

CHAPTER 4

Adding Users to the Standard CTI User Groups

If you want Cisco UC Integration for Cisco WebEx Connect to be able to control the desk phone of the user, you must select the Allow Control of Device from CTI option when you create the device for the user. You must also ensure that the user is added to the Standard CTI Enabled user group.

If the phone of the user is a Cisco Unified IP Phone 6900, 8900 or 9900 series model, you must also add the user to the Standard CTI Allow Control of Phones supporting Connected Xfer and conf user group.

Procedure

Step 1 Select **User Management > End User** in Cisco Unified Communications Manager Administration.

Step 2 Select the user you want to add.

Step 3 Select **Add to User Group** in the Permissions Information group in the End User Configuration window.

Step 4 Search for “Standard CTI” in the Find and List User Groups window.

Step 5 Select **Standard CTI Enabled** user group.

If the phone of the user is a Cisco Unified IP Phone 6900, 8900 or 9900 series model, select the **Standard CTI Allow Control of Phones supporting Connected Xfer and conf** user group also.

Step 6 Select **Add Selected**.

Step 7 Select **Save** in the End User Configuration window.

Creating a New User

Procedure

Step 1 Select **User Management > End User** in Cisco Unified Communications Manager Administration.

Step 2 Select **Add New**.

Step 3 Enter the user credentials as applicable.

Field	Description
User ID	Enter the unique end user identification name. You can enter any character, including alphanumeric and special characters. No character restrictions exist for this field.
Password	Enter alphanumeric or special characters for the end user password. You must enter at least the minimum number of characters that are specified in the assigned credential policy (1-127 characters).
Confirm Password	Enter the end user password again.
PIN	Enter numeric characters for the end user PIN. You must enter at least the minimum number of characters that are specified in the assigned credential policy (1-127 characters).
Confirm PIN	Enter the PIN again.
Last Name	Enter the end user last name.
Middle Name	Enter the end user middle name.
First Name	Enter the end user first name.
Telephone Number	Enter the end user telephone number. You may use the following special characters: (,), and -.
Mail ID	Enter the end user e-mail address.
Manager User ID	Enter the user ID of the end user manager ID. **Tip:** The manager user ID that you enter does not have to exist in the same cluster as the end user; therefore, Cisco Unified Communications Manager does not require that you enter a user ID that already exists in the database.
Department	Enter the end user department information (for example, the department number or name).
User Locale	From the drop-down list box, choose the locale that is associated with the end user. The user locale identifies a set of detailed information to support end users, including language and font. **Note:** If you do not choose an end user locale, the locale that is specified in the Cisco CallManager service parameters as Default User Locale applies.
Associated PC	This required field applies for Cisco IP Softphone users.
Digest Credentials	Enter a string of alphanumeric characters. Cisco Unified Communications Manager uses the digest credentials that you specify here to validate the credentials that the phone offers during digest authentication. The digest credentials that you enter in this field are associated with the phone when you choose a digest user in the Phone Configuration window. **Note:** For more information on digest authentication, refer to the *Cisco Unified Communications Manager Security Guide*.
Confirm Digest Credentials	To confirm that you entered the digest credentials correctly, re-enter the credentials in this field.

Step 4 Select the **Device Information** and profiles.

See the list of supported devices Supported Cisco Unified IP Phones, page 1-3

Step 5 Select the **Extension Mobility** parameters.

Field	Description
Available Profiles	This list box displays the extension mobility profiles that are available for association with this end user. To search for an extension mobility profile, click **Find**. Use the Find and List Device Profiles window that displays to search for the extension mobility profile that you want. To associate an extension mobility profile with this end user, select the profile and click the **Down** arrow below this list box.
Controlled Profiles	This field displays a list of controlled device profiles that are associated with an end user who is configured for Cisco Extension Mobility.
Default Profile	From the drop-down list box, choose a default extension mobility profile for this end user.
Presence Group	Configure this field with the Presence feature. From the drop-down list box, choose a Presence group for the end user. The selected group specifies the destinations that the end user can monitor. The default value for Presence Group specifies Standard Presence group, configured with installation. Presence groups that are configured in Cisco Unified Communications Manager Administration also appear in the drop-down list box. Presence authorization works with presence groups to allow or block presence requests between groups. Refer to the "Presence" chapter in the Cisco Unified Communications Manager Features and Services Guide for information about configuring permissions between groups and how presence works with extension mobility.
SUBSCRIBE Calling Search Space	Supported with the Presence feature, the SUBSCRIBE calling search space determines how Cisco Unified Communications Manager routes presence requests that come from the end user. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the end user. From the drop-down list box, choose the SUBSCRIBE calling search space to use for presence requests for the end user. All calling search spaces that you configure in Cisco Unified Communications Manager Administration display in the SUBSCRIBE Calling Search Space drop-down list box. If you do not select a different calling search space for the end user from the drop-down list, the SUBSCRIBE calling search space defaults to None.

Field	Description
Allow Control of Device from CTI	If this check box is checked, when the user logs in to a device, the AllowCTIControlFlag device property becomes active, which allows control of the device from CTI applications. Until the user logs in to a device, this setting has no effect. **Note:** The Allow Control of Device from CTI setting in the end user configuration overrides the AllowCTIControlFlag device property of the device to which the user logs in.
Enable Extension Mobility Cross Cluster	Check this box to enable this end user to use the Cisco Extension Mobility Cross Cluster feature.

Step 6 Select the Directory Number Associations.

Field	Description
Primary Extension	This field represents the primary directory number for the end user. End users can have multiple lines on their phones. When you associate devices to the end user, directory numbers that are configured on the associated device become available in the drop-down list box for Primary Extension. From the drop-down list box, choose a primary extension for this end user. If the system is integrated with Cisco Unity Connection, the Create Cisco Unity User link displays in the Related Links menu.
IPCC Extension	From the drop-down list box, choose an IPCC extension for this end user. **Note:** This field displays only if the IPCC Express Installed enterprise parameter is set to True.

Step 7 Select the Mobility Information.

Field	Description
Enable Mobility	Check this check box to activate Mobile Connect, which allows the user to manage calls by using a single phone number and to pick up in-progress calls on the desktop phone and cellular phone. Checking this check box, which triggers licensing to consume device license units for Mobile Connect, works in conjunction with the Primary User Device drop-down list box. If you check the Enable Mobility check box and fail to choose an adjunct device from the Primary User Device drop-down list box, four device license units (DLUs) get consumed, as indicated in the Mobility Enabled End Users row in the License Unit Calculation window. If you enable Cisco Unified Mobility and later choose an adjunct device from the Primary User Device drop-down list box, the system credits you with two DLUs, as indicated in the Mobility Enabled End Users row in the License Unit Calculation window.
Primary User Device	The Primary User Device drop-down list box, which works in conjunction with the Enable Mobility check box, controls the number of device license units that are consumed for adjunct devices for Mobile Connect. After you check the Enable Mobility check box, choose an adjunct device that you want to assign to the user specifically for Cisco Unified Mobility. For example, choose a device, such as a desktop phone, that the user uses in addition to the cell phone for Cisco Unified Mobility. Before you choose an adjunct device, consider the following information: • Only devices that consume two or more device license units (DLUs) display in the drop-down list box. • For Cisco Unified Mobility, you cannot assign the same device to multiple users, so only the devices that you can assign display in the drop-down list box. • If you check the Enable Mobility check box and choose a device from the drop-down list box, two DLUs get consumed, as indicated in the Mobility Enabled End Users (Adjunct) row in the Licensing Unit Calculation window. • If you delete the device from Cisco Unified Communications Manager Administration or remove the assignment after you enable Mobile Connect, two DLUs get consumed after you delete the device or remove the assignment, as indicated in the Mobility Enabled End Users row in the License Unit Calculation window.
Enable Mobile Voice Access	Check this check box to allow the user to access the Mobile Voice Access integrated voice response (IVR) system to initiate Mobile Connect calls and activate or deactivate Mobile Connect capabilities.
Maximum Wait Time for Desk Pickup	Enter the maximum time in milliseconds that is permitted to pass before the user must pick up a call that is transferred from the mobile phone to desktop phone.

Field	Description
Remote Destination Limit	Enter the maximum number of phones to which the user is permitted to transfer calls from the desktop phone.
Remote Destination Profiles	This field lists the remote destination profiles that have been created for this user. To view the details of a particular remote destination profile, choose a remote destination profile in the list and click the View Details link.

CHAPTER 5

Installing and Configuring Cisco UC Integration for Cisco WebEx Connect

Before you install Cisco UC Integration for Cisco WebEx Connect, check that your system meets all the necessary prerequisites. Ensure that you have the correct versions of all the required software, as listed in the release notes at the following URLs:

http://www.cisco.com/en/US/products/ps10627/prod_release_notes_list.html

http://www.webex.com/m/connectreleasenotes_c6.pdf

Installation Package Contents

The Cisco UC Integration for Cisco WebEx Connect installation package contains the following:

- An executable file. Users can run the executable file on their computer.
- A Microsoft Installer (MSI) file. This is used for silent installation with a push mechanism such as Active Directory Group Policy, Microsoft System Management Server (SMS), Altiris and so on.

Configuring Cisco UC Integration for Cisco WebEx Connect

There are two methods to configure Cisco WebEx Connect to work with the Cisco Unified Client Services Framework:

1. Cisco WebEx Connect Administration Console: Access the online help for the WebEx Connect Administration Console for complete information. This is the preferred configuration method. You can access the help at the following location:

   http://www.webex.com/webexconnect/orgadmin/help/index.htm

   Note Using multiple Cisco Unified CSF clients is not a supported scenario.

2. Cisco WebEx Connect, the Unified Communications tab within the Settings page: Users can input the configuration settings. It is important to note if you use this method you cannot configure the backup servers.
3. For more information about the Settings page, access the Cisco WebEx Connect help at the following location:

http://www.webex.com/webexconnect/help/wwhelp.htm

CHAPTER 6

Configuring Cisco Unity and Unity Connection Servers

Cisco Unity Servers

Cisco Unity receives calls, plays greetings, and records and encodes voicemail. When a voicemail is received, Cisco Unity adds the .wav file to an email and sends it to the configured email account. Cisco Unity creates a subscriber mailbox on the Microsoft Exchange server for use as its mailstore server for message storage.

When Cisco Unified Communications Integration for Cisco WebEx Connect users want to listen to their voicemails, they use Cisco Unified Communications Integration to retrieve them from the mailstore server through IMAP.

Cisco Unified Communications Integration supports both the Cisco Unity unified messaging and the Cisco Unity voice messaging configurations. With unified messaging, the Exchange server email account supports both voicemail and email. With voice messaging, the Exchange server email account contains only voicemail messages.

Before You Begin

- Install and configure a supported release of Cisco Unity.
- Integrate Cisco Unified Communications Manager and Cisco Unity. Both servers must be installed and running to configure voicemail ports.
- If you plan to use SSL to provide secure transmission with the mailstore server, you must set up Cisco Unity to use SSL during the installation or upgrade (or at any time after the installation or upgrade is complete). You must designate a server to act as your certificate authority, submit a certificate request, issue the certificate, and install it on the Cisco Unity server.

Procedure

Step 1 Configure the Microsoft Exchange server to use the IMAP virtual server:

To Configure This Release	Do This
Microsoft Exchange 2003	**a.** Select **Start > All Programs > Microsoft Exchange > System Manager**. **b.** In the section on the left-hand side of the System Manager, expand **Servers**. **c.** Select the server name. **d.** Select **Protocols > IMAP**. **e.** Right-click, and select **Start Server**.
Microsoft Exchange 2007	**a.** Select **Start > Run**, enter **services.msc**, and select **OK**. **b.** Select the Microsoft Exchange IMAP4 service, and select **Start**. This service is not started by default.

Step 2 Configure the port and encryption type:

To Configure This Server	Do This
Microsoft Exchange 2003	**a.** Right-click IMAP Virtual Server, and select Properties. **b.** Select **Authentication** from the Access tab. – Verify that **Requires SSL/TLS Encryption** is not checked to use TCP and SSL connection. – Verify that **Requires SSL/TLS Encryption** is checked to use SSL only. **c.** Select **OK**.
Microsoft Exchange 2007	**a.** Select **Start > Programs > Microsoft Exchange Server 2007 > Exchange Management Shell**. **b.** Specify the authentication settings for the Client Access Server that is running the IMAP4 service through the Exchange Power Shell. **Note**: Microsoft Exchange 2007 uses SSL by default. **c.** Execute one of the following commands for the appropriate setting: – For plain text login: **set-imapsettings -LoginType PlainTextLogin** – For SSL: **set-imapsettings -LoginType SecureLogin**

Step 3 Configure the user:

- If the user is an existing Cisco Unity user, add the user to the Cisco Unified Communications Manager database and to Cisco Unified Presence.
- If the user is a new user, add the user to the Cisco Unified Communications Manager database, Cisco Unity (which adds the user to Exchange and to Active Directory), and to Cisco Unified Presence.

Step 4 Create mailboxes for new and existing users. For details, see the documentation for your Exchange server.

Step 5 (Optional) Enable secure messaging as follows:

a. Select **Subscribers > Subscribers > Features** to make the change on a subscriber template.

   The change you make here is not applied to current subscriber accounts that were created by using this template. The setting applies only to subscriber accounts that are created by using this template after the change has been made.

b. Select an option from the Message Security When Sending a Message list to enable secure messages. For example, select **Encrypt All Messages**.

   This setting specifies whether messages are encrypted when subscribers send messages to other subscribers.

c. Select **Save**.

d. Repeat these steps for additional subscribers or subscriber templates, as applicable.

Step 6 (Optional) Enable secure messaging for messages from unidentified callers:

a. Select **System > Configuration > Message Security Settings**.

b. Specify whether messages from unidentified callers are encrypted. Select an option from the list.

c. Select **Save**.

Troubleshooting Tip

Cisco Unified Communications Integration users must enter their Cisco Unity credentials in the Cisco Unified Communications Integration Preferences window.

Cisco Unity Connection Servers

Cisco Unity Connection provides Cisco Unified Communications Integration for Cisco WebEx Connect users with the ability to view, play, sort, and delete voicemail messages from the Cisco Unified Communications Integration interface.

Before You Begin

- Install and configure a supported release of Cisco Unity Connection.
- Integrate Cisco Unified Communications Manager and Cisco Unity Connection. Both servers must be installed and running to configure voicemail ports.

Procedure

Step 1 Add a new user.

a. Expand **Users** in the section on the left-hand side.

b. Select **New User**.

c. Select **Edit** > **Password Settings**.

d. In the Choose Password drop down box, select **Web Application.**

e. Deselect **User Must Change at Next Sign-In**.

f. Click **Save**.

g. Select **Edit > Change Password**.

h. Set the new password.

Step 2 Configure the user:

If the users are existing Cisco Unity Connection users, add them to the Cisco Unified Communications Manager database.

If the user is a new Cisco Unified Communications Integration user, add the user to the Cisco Unified Communications Manager database and to Cisco Unity Connection.

Step 3 (Optional) Specify how to handle unidentified caller message security for your users as follows:

a. Expand **Users** in the section on the left-hand side.

b. Select **User**.

c. Select the alias of a user.

d. Select **Edit > Message Settings**.

Check **Mark Secure** in Unidentified Callers Message Security.

Procedure

Step 1 Set up a new or existing class of service in Cisco Unity Connection Administration to enable Internet Mail Access Protocol (IMAP) client access to voice messages.

a. Expand **Class of Service** in the section on the left-hand side.

b. Select **Class of Service**.

c. Select the display name of the applicable class of service in the Search Results table, in the Search Class of Service window.

d. Check **Allow Users to Use Unified Client to Access Voice Mail**, under Features.

e. Check **Allow Users to Access VoiceMail Using an IMAP Client**, under Licensed Features.

f. Select **Allow Users to Access Message Bodies**.

g. Select **Save**.

Step 2 (Optional) Enable secure messaging as follows:

a. Expand **Class of Service** in the section on the left-hand side.

b. Select **Class of Service**.

c. Select an option from Require Secure Messaging in the Message Options section to enable secure messages.

Step 3 Create a Connection user account on the Cisco Unity Connection server with a voice mailbox for each Cisco Unified Communications Integration user.

Note The user ID in Cisco Unity Connection does not need to match the user ID in Cisco Unified Presence or in the Cisco Unified Communications Integration. The Cisco Unified Communications Integration has an independent voicemail ID, which is set in the application Preference window. However, you might find it useful to have the same user IDs across your Cisco Unified Communications system.

Step 4 If one does not already exist, specify a web application password in Cisco Unity Connection for the applicable user accounts.

Troubleshooting Tips

- Users must enter their voicemail credentials, that is, their username and password, in the Cisco Unified Communications Integration application.
- If the server can be contacted and the user credentials are correct, but voicemail messages are not downloaded, do the following:
  - Check the configuration of port 7993. Make sure that Cisco Unity Connection is listening on port 7993.
  - Check the firewall configuration. Use Telnet from a remote computer to the computer running Cisco Unified Communications Integration, and make sure that you can connect to the firewall. Permit the Cisco Unified Client Services Framework executable file (connect.exe) to establish IMAP network connections using TCP, TLS, and SSL at the appropriate server and port.

Enable voicemail feature

Step 1 Open **“Class of Service” page - > “Voicemail User COS”**

Step 2 In **“Licensed Features”** section check 2 option:

Step 3 Allow Users to Access Voice Mail Using an IMAP Client and/or Single Inbox

Step 4 Allow Users to Use the Messaging Inbox and RSS Feeds

Verifying Microsoft Exchange IMAP Security Settings for Deployments with Cisco Unity

Before You Begin

Work with your Microsoft Exchange or Cisco Unity administrator if you have questions about information in this topic.

Procedure

Step 1 Determine whether IMAP is configured as secure or nonsecure.

For Microsoft Exchange 2003:

a. Select **Start > All Programs > Microsoft Exchange > System Manager**

b. Select **Administrative Groups > First Administrative Group > Servers > <your server name> >Protocols > IMAP4**

c. Right-click **Default IMAP4 Virtual Server** and select **Properties**.

d. Select **Access**, then select **Authentication** in the Access Control section.

e. Determine if **Requires SSL/TLS encryption** is selected.

For Microsoft Exchange 2007, navigate to the relevant setting in **Start > All Programs > Microsoft Exchange Server 2007 > Exchange Management Console**

Step 2 Verify the security setting for Internet Information Services (IIS)

a. Select **Start > Programs > Administrative Tools > Internet Information Services (IIS) Manager**

b. Select **<your computer name>(local computer) > > Web Sites > Default Web Site**

c. Right-click **Default Web Site** and select **Properties**.

d. Select **Directory Services**.

e. In the Secure Communications section, select **Edit**.

f. Determine if **Require secure channel (SSL)** is enabled.

What to Do Next

If your IMAP is secure, you must select TLS as the Transport Type when you configure your voicemail adapter. Otherwise, select TCP.

If you select TLS:

- Specify a security context that has Trust Policy set to Trusted Certificates.
- Exchange certificates with the Exchange server.
- For examples of certificate exchanges with Cisco Unified Mobility Advantage, see the Security documentation module at
- http://www.cisco.com/en/US/products/ps7270/products_installation_and_configuration_guides_list.html

CHAPTER 7

Settings in Cisco Unified Communications Manager and Voicemail Requirements

Important Information About DTMF Access Codes

All DTMF access codes that you configure in Cisco Unified Communications Manager must be mutually exclusive. Make sure the default mobility DTMF access codes do not overlap with other mid-call DTMF access codes.

For example, by default mobility features and Cisco Unity both use the asterisk (*) for midcall features, which prevents DTMF features in both applications from working properly.

This issue is not specific to Cisco Unified Mobility Advantage, but will affect Cisco Unified Mobile Communicator users when they access voicemail or use mid-call features.

To configure DTMF access codes, see the documentation for your release of Cisco Unified Communications Manager.

Requirements for Voicemail

The following are required for visual voicemail:

- Verify that your system will work with the supported transcoding protocols. See the Compatibility Matrix

  http://www.cisco.com/en/US/products/ps7270/products_device_support_tables_list.html

- Verify that IMAP is enabled:
  - For Cisco Unity: See the article *Using IMAP4 to Access Voice Messages in Cisco Unity System with Exchange 2007* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_configuration_example09186a00809d8c91.shtml
  - If you use Cisco Unity Connection: See “Configuring IMAP Settings” in the System Administration Guide Cisco Unity Connection Release 7.x at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.
- Make sure the DTMF code for accessing voicemail is unique in Cisco Unified Communications Manager. See Important Information About DTMF Access Codes, page 3.
- If you have users on more than one Exchange or voicemail server, create a separate voicemail adapter for each Exchange server or voicemail store.

CHAPTER 8

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the What's New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Finding Documentation

- For a complete list of documents, see the *Documentation Guide for Cisco Unified Communications Integration (TM) for Cisco WebEx Connect* at: http://www.cisco.com/en/US/docs/voice_ip_comm/cuciwebex/roadmap/cuciconnect_map.html
- Cisco WebEx Connect Administration Console:

  http://www.webex.com/webexconnect/orgadmin/help/index.htm
- Cisco Unified Communications Manager Documentation

  Refer to the Cisco Unified Communications Manager Documentation Guide and other publications specific to your Cisco Unified Communications Manager release:

  http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html
- Cisco WebEx Connect online help:

  http://www.webex.com/webexconnect/help/wwhelp.htm