Cloud and Hybrid Deployments for Cisco Jabber 11.5

First Published: 2015-12-22

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **Jabber Overview** 1

Purpose of this Guide 1

About Cisco Jabber 1

CHAPTER 2 **Workflows for Cloud and Hybrid Deployments** 3

Cloud Deployment Workflow 3

Hybrid Deployment Workflow 3

CHAPTER 3 **Configure Policies** 5

Configure Policies 5

CHAPTER 4 **Configure Clusters** 7

Configure Cluster Information 7

CHAPTER 5 **Create Users for Cloud Deployment** 9

Create Users for Cloud Deployments 9

CHAPTER 6 **Create Users for Hybrid Deployment** 11

Enable Synchronization 11

Specify an LDAP Attribute for the User ID 12

Specify an LDAP Attribute for the Directory URI 12

Perform Synchronization 13

Assign Roles and Groups 13

Authentication Options 14

Enable SAML SSO in the Client 14

Authenticate with the LDAP Server 15

CHAPTER 7 **Configure Deskphone Control** 17

Prerequisites 17
Configure Deskphone Control Workflow 17
Add a CTI Service 18
Apply a CTI Service 18
Enable Device for CTI 19
Desk Phone Video Configuration 19
Enable Video Rate Adaptation 21
Enable RTCP on Common Phone Profiles 21
Enable RTCP on Device Configurations 22
Configure User Associations 22
Reset Devices 24

CHAPTER 8 Configure Softphone 25
Configure Softphones Workflow 25
Create and Configure Cisco Jabber Devices 25
Add a Directory Number to the Device 28
Add a Remote Destination 29
Configure User Associations 30
Create Mobile SIP Profiles 32
Setting up System SIP Parameters 32
Configure the Phone Security Profile 33
Provide Users with Authentication Strings 34

CHAPTER 9 Configure Extend and Connect 37
Configure Extend and Connect Workflow 37
Enable User Mobility 37
Create CTI Remote Devices 38
Configure User Associations 39

CHAPTER 10 Configure Service Discovery for Remote Access 41
Service Discovery Requirements 41
DNS Requirements 41
Certificate Requirements 41
Test _collab-edge SRV Record 42

CHAPTER 11 Set Up Certificate Validation 43
Certificate Validation for Cloud Deployments 43
Update Profile Photo URLs 44

CHAPTER 12 Configure the Clients 45
Client Configuration Workflow 45
Introduction to Client Configuration 45
Create and Host Client Configuration Files 46
Specify Your TFTP Server Address 47
Specify TFTP Servers in Phone Mode 48
Create Global Configurations 48
Create Group Configurations 48
Host Configuration Files 49
Restart Your TFTP Server 50
Configuration File 50
Set Parameters on Phone Configuration for Desktop Clients 51
Parameters in Phone Configuration 51
Set Parameters on Phone Configuration for Mobile Clients 52
Parameters in Phone Configuration 52
Configure Proxy Setting 53
Configure Proxy Settings for Cisco Jabber for Windows 53
Configure Proxy Settings for Cisco Jabber for Mac 53
Configure Proxy Settings for Cisco Jabber iPhone and iPad 54
Configure Proxy Settings for Cisco Jabber for Android 54

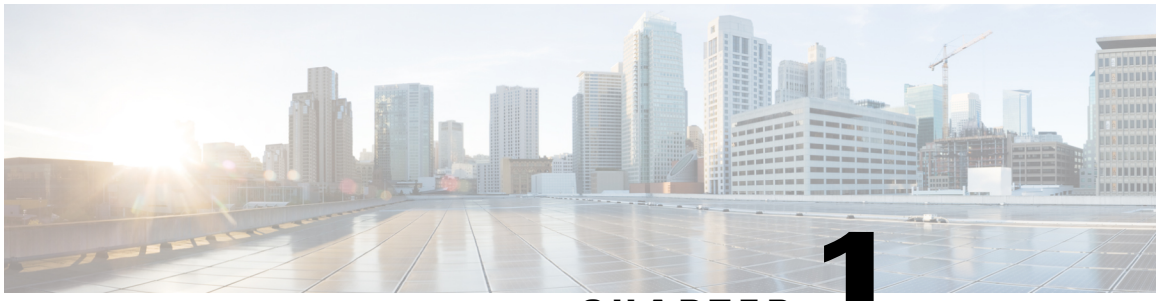
CHAPTER 13 Deploy Cisco Jabber Applications 55
Download the Cisco Jabber Clients 55
Install Cisco Jabber for Windows 55
Use the Command Line 56
Cisco Jabber for Windows for Cloud Deployment 56
Example Installation Commands 56
Command Line Arguments 57
Override Argument 57
Mode Type Argument 58

When to Set the Product Mode 58
Change Product Modes 58
Change Product Modes with Cisco Unified Communications Manager Version 9.x and Later 59
Authentication Arguments 59
TFTP Server Address 63
Common Installation Arguments 64
SSO Arguments 70
Cloud-Based SSO Arguments 70
LCID for Languages 71
Run the MSI Manually 72
Create a Custom Installer 73
Get the Default Transform File 73
Create Custom Transform Files 74
Transform the Installer 74
Installer Properties 76
Deploy with Group Policy 76
Set a Language Code 77
Deploy the Client with Group Policy 78
Cisco Media Services Interface 79
Desk Phone Video Capabilities 79
Install Cisco Media Services Interface 79
Uninstall Cisco Jabber for Windows 79
Use the Installer 79
Use the Product Code 80
Install Cisco Jabber for Mac 81
URL Configuration for Cisco Jabber for Mac 81
Install Cisco Jabber Mobile Clients 83
URL Configuration for Cisco Jabber for Android, iPhone, and iPad 83
Mobile Configuration Using Enterprise Mobility Management 86

CHAPTER 14 Remote Access 87
Service Discovery Requirements Workflow 87
Service Discovery Requirements 87
DNS Requirements 88

Certificate Requirements 88
Test _collab-edge SRV Record 88
Test SRV Records 88
Cisco Anyconnect Deployment Workflow 89
Cisco AnyConnect Deployment 89
Application Profiles 89
Automate VPN Connection 90
Set Up Trusted Network Connection 90
Set Up Connect On-Demand VPN 91
Set Up Automatic VPN Access on Cisco Unified Communications Manager 92
AnyConnect Documentation Reference 93
Session Parameters 93
Set ASA Session Parameters 94

CHAPTER 15 Troubleshooting 95
Update the SSO Certificate for the Cisco Jabber Domain 95



CHAPTER 1

Jabber Overview

- Purpose of this Guide, page 1
- About Cisco Jabber, page 1

Purpose of this Guide

This guide includes the following task-based information required to deploy and install Cisco Jabber:

- Configuration and installation workflows that outline the processes to configure and install cloud or hybrid deployments.
- How to configure the various services that the Cisco Jabber client interacts with, such as IM and Presence Service, Voice and Video Communication, Visual Voicemail, and Conferencing.
- How to configure directory integration, certificate validation, and service discovery.
- How to install the clients.

Before you deploy and install Cisco Jabber, see the *Cisco Jabber Planning Guide* at http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html to determine the deployment options that best suit your business needs.

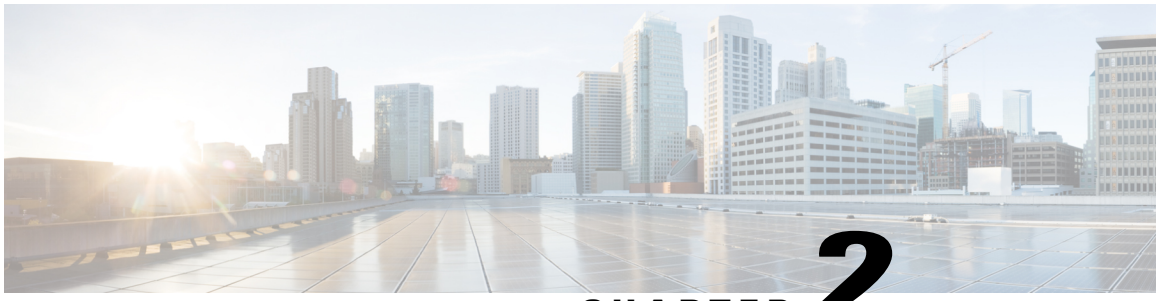
About Cisco Jabber

Cisco Jabber is a suite of Unified Communications applications that allow seamless interaction with your contacts from anywhere. Cisco Jabber offers IM, presence, audio and video calling, voicemail, and conferencing.

The applications in the Cisco Jabber family of products are:

- Cisco Jabber for Android
- Cisco Jabber for iPhone and iPad
- Cisco Jabber for Mac
- Cisco Jabber for Windows

For more information about the Cisco Jabber suite of products, see http://www.cisco.com/go/jabber.



CHAPTER 2

Workflows for Cloud and Hybrid Deployments

- Cloud Deployment Workflow, page 3
- Hybrid Deployment Workflow, page 3

Cloud Deployment Workflow

Procedure

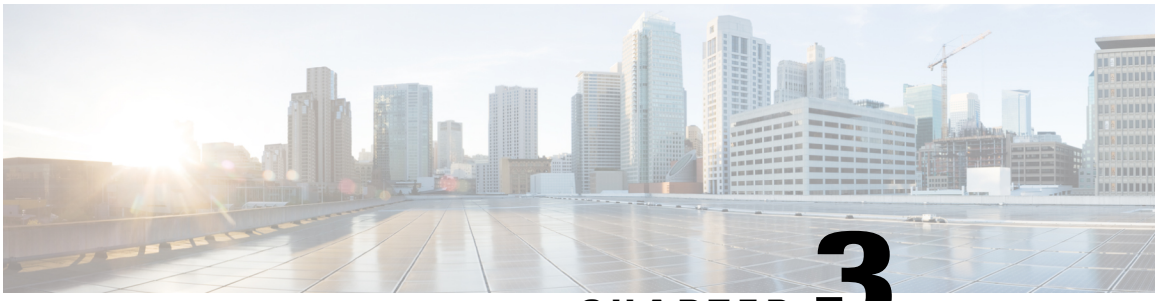
	Command or Action	Purpose
Step 1	Configure Policies, on page 5	
Step 2	Create Users for Cloud Deployment, on page 9	
Step 3	Set Up Certificate Validation, on page 43	
Step 4	Configure the Clients, on page 45	
Step 5	Deploy Cisco Jabber Applications, on page 55	

Hybrid Deployment Workflow

Procedure

	Command or Action	Purpose
Step 1	Configure Policies, on page 5	
Step 2	Configure Clusters, on page 7	
Step 3	Create Users for Hybrid Deployment, on page 11	
Step 4	Configure Deskphone Control, on page 17	
Step 5	Configure Softphone, on page 25	

	Command or Action	Purpose
Step 6	Configure Extend and Connect, on page 37	
Step 7	Configure Service Discovery for Remote Access, on page 41	
Step 8	Set Up Certificate Validation, on page 43	
Step 9	Configure the Clients, on page 45	
Step 10	Deploy Cisco Jabber Applications, on page 55	
Step 11	Remote Access, on page 87	



CHAPTER 3

Configure Policies

- Configure Policies, page 5

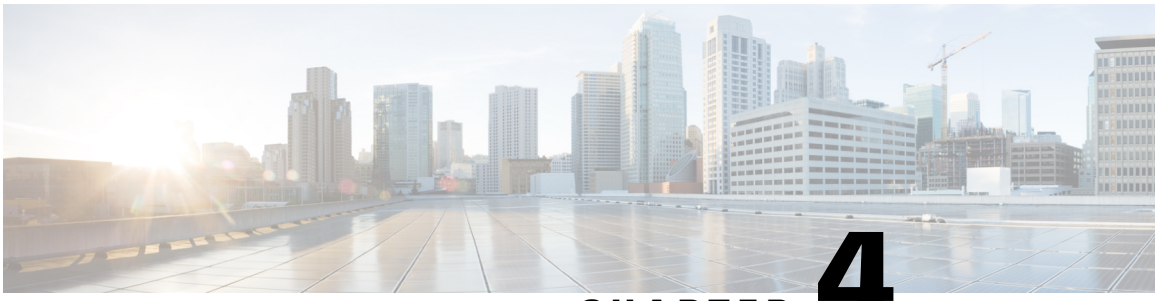
Configure Policies

Cisco WebEx provides a Policy Editor to define and apply policies to groups. You can enable and disable features for groups of users or to all the users in your Cisco WebEx organization.

Procedure

	Command or Action	Purpose
Step 1	Configure Policies for your Cisco WebEx organization.	For more information, see the *Policy Editor* section of the *Cisco WebEx Messenger Administration Guide*.
Step 2	Assign users to policy groups.	For more information, see the *Policy Group Users* section of the *Cisco WebEx Messenger Administration Guide*.

Configure Policies



CHAPTER 4

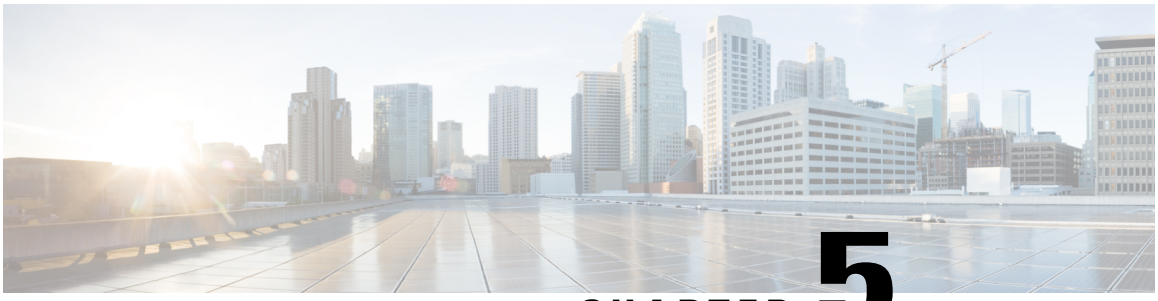
Configure Clusters

- Configure Cluster Information, page 7

Configure Cluster Information

Procedure

	Command or Action	Purpose
Step 1	Enable Visual Voicemail	For more information, see the *Configure Visual Voicemail* section of the *Cisco WebEx Messenger Administration Guide*.
Step 2	Configure Cisco Unified Communications Manager Server settings.	For more information, see the *Cisco Unified Communications Integration with Cisco WebEx* section of the *Cisco WebEx Messenger Administration Guide*.



CHAPTER 5

Create Users for Cloud Deployment

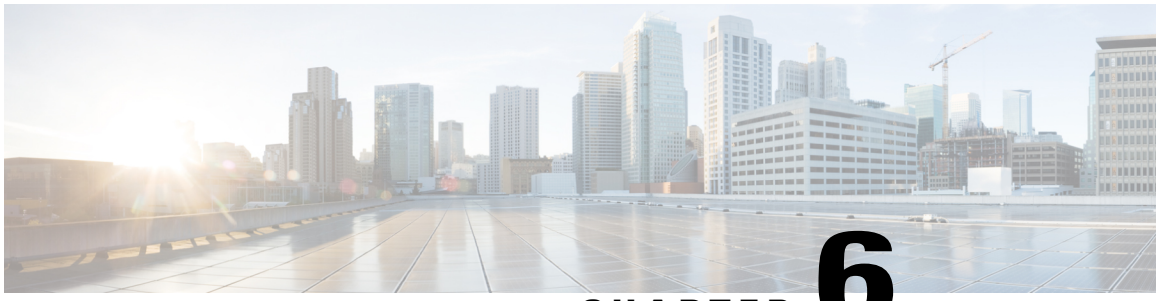
- Create Users for Cloud Deployments, page 9

Create Users for Cloud Deployments

Cisco WebEx Administration Tool provides a number of ways to create users for your organization.

Procedure

	Command or Action	Purpose
Step 1	You can add users individually using the Cisco WebEx Administration Tool.	For more information, see the *New Users* section of the *Cisco WebEx Messenger Administration Guide*.
Step 2	You can generate an email invitation for users to self register for a Cisco WebEx account.	For more information, see the *User Provisioning Information* section of the *Cisco WebEx Messenger Administration Guide*.
Step 3	Create and import a CSV file with your users information.	For more information on CSV file formats, see the *CSV File Format* section of the *Cisco WebEx Messenger Administration Guide*. For more information on Importing CSV files, see the *Import and Export Users Using the CSV File* section of the *Cisco WebEx Messenger Administration Guide*.



CHAPTER 6

Create Users for Hybrid Deployment

- Enable Synchronization, page 11
- Specify an LDAP Attribute for the User ID, page 12
- Specify an LDAP Attribute for the Directory URI, page 12
- Perform Synchronization, page 13
- Assign Roles and Groups, page 13
- Authentication Options, page 14

Enable Synchronization

To ensure that contact data in your directory server is replicated to Cisco Unified Communications Manager, you must synchronize with the directory server. Before you can synchronize with the directory server, you must enable synchronization.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **System** > **LDAP** > **LDAP System**.
The **LDAP System Configuration** window opens.

Step 3 Locate the **LDAP System Information** section.

Step 4 Select **Enable Synchronizing from LDAP Server**.

Step 5 Select the type of directory server from which you are synchronizing data from the **LDAP Server Type** drop-down list.

What to Do Next

Specify an LDAP attribute for the user ID.

Specify an LDAP Attribute for the User ID

When you synchronize from your directory source to Cisco Unified Communications Manager, you can populate the user ID from an attribute in the directory. The default attribute that holds the user ID is `sAMAccountName`.

Procedure

Step 1 Locate the **LDAP Attribute for User ID** drop-down list on the **LDAP System Configuration** window.

Step 2 Specify an attribute for the user ID as appropriate and then select **Save**.

Important If the attribute for the user ID is other than `sAMAccountName` and you are using the default IM address scheme in Cisco Unified Communications Manager IM and Presence Service, you must specify the attribute as the value for the parameter in your client configuration file as follows:

The EDI parameter is `UserAccountName`.

`<UserAccountName>`*`attribute-name`*`</UserAccountName>`

The BDI parameter is `BDIUserAccountName`.

`<BDIUserAccountName>`*`attribute-name`*`</BDIUserAccountName>`

If you do not specify the attribute in your configuration, and the attribute is other than `sAMAccountName`, the client cannot resolve contacts in your directory. As a result, users do not get presence and cannot send or receive instant messages.

Specify an LDAP Attribute for the Directory URI

On Cisco Unified Communications Manager release 9.0(1) and later, you can populate the directory URI from an attribute in the directory.

Before You Begin

Enable Synchronization.

Procedure

Step 1 Select **System** > **LDAP** > **LDAP Directory**.

Step 2 Select the appropriate LDAP directory or select **Add New** to add an LDAP directory.

Step 3 Locate the **Standard User Fields To Be Synchronized** section.

Step 4 Select one of the following LDAP attributes from the **Directory URI** drop-down list:

- **msRTCSIP-primaryuseraddress—**This attribute is populated in the AD when Microsoft Lync or Microsoft OCS are used. This is the default attribute.
- **mail**

Step 5 Select **Save**.

Perform Synchronization

After you add a directory server and specify the required parameters, you can synchronize Cisco Unified Communications Manager with the directory server.

Procedure

Step 1 Select **System** > **LDAP** > **LDAP Directory**.

Step 2 Select **Add New**.
The **LDAP Directory** window opens.

Step 3 Specify the required details on the **LDAP Directory** window.
See the Cisco Unified Communications Manager Administration Guide for more information about the values and formats you can specify.

Step 4 Create an LDAP Directory Synchronization Schedule to ensure that your information is synchronized regularly.

Step 5 Select **Save**.

Step 6 Select **Perform Full Sync Now**.

Note The amount of time it takes for the synchronization process to complete depends on the number of users that exist in your directory. If you synchronize a large directory with thousands of users, you should expect the process to take some time.

User data from your directory server is synchronized to the Cisco Unified Communications Manager database. Cisco Unified Communications Manager then synchronizes the user data to the presence server database.

Assign Roles and Groups

For all deployment types assign users to the **Standard CCM End Users** group.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **User Management** > **End User**
The **Find and List Users** window opens.

Step 3 Find and select the user from the list.
The **End User Configuration** window opens.

Step 4 Locate the **Permission Information** section.

Step 5 Select **Add to Access Control Group**.

The **Find and List Access Control Groups** dialog box opens.

Step 6 Select the access control groups for the user.
At a minimum you should assign the user to the following access control groups:

- **Standard CCM End Users**
- **Standard CTI Enabled—**This option is used for desk phone control.

If you provision users with secure phone capabilities, do not assign the users to the **Standard CTI Secure Connection** group.

Certain phone models require additional control groups, as follows:

- Cisco Unified IP Phone 9900, 8900, or 8800 series or DX series, select **Standard CTI Allow Control of Phones supporting Connected Xfer and conf**.
- Cisco Unified IP Phone 6900 series, select **Standard CTI Allow Control of Phones supporting Rollover Mode**.

Step 7 Select **Add Selected**.
The **Find and List Access Control Groups** window closes.

Step 8 Select **Save** on the **End User Configuration** window.

Authentication Options

Enable SAML SSO in the Client

Before You Begin

- If you do not use Cisco WebEx Messenger, enable SSO on Cisco Unified Communications Applications 10.5.1 Service Update 1—For information about enabling SAML SSO on this service, read the *SAML SSO Deployment Guide for Cisco Unified Communications Applications, Release 10.5*.
- Enable SSO on Cisco Unity Connection version 10.5—For more information about enabling SAML SSO on this service, read *Managing SAML SSO in Cisco Unity Connection*.
- If you use Cisco WebEx Messenger, enable SSO on Cisco WebEx Messenger Services to support Cisco Unified Communications Applications and Cisco Unity Connection—For more information about enabling SAML SSO on this service, read about *Single Sign-On* in the *Cisco WebEx Messenger Administrator's Guide*.

  For more information about enabling SAML SSO on this service, read about `Single Sign-On` in the *Cisco WebEx Messenger Administrator's Guide*.

Procedure

Step 1 Deploy certificates on all servers so that the certificate can be validated by a web browser, otherwise users receive warning messages about invalid certificates. For more information about certificate validation, see *Certificate Validation*.

Step 2 Ensure Service Discovery of SAML SSO in the client. The client uses standard service discovery to enable SAML SSO in the client. Enable service discovery by using the following configuration parameters: ServicesDomain,VoiceServicesDomain, and ServiceDiscoveryExcludedServices. For more information about how to enable service discovery, see *Configure Service Discovery for Remote Access*.

Step 3 Define how long a session lasts.
A session is comprised of cookie and token values. A cookie usually lasts longer than a token. The life of the cookie is defined in the Identity Provider, and the duration of the token is defined in the service.

Step 4 When SSO is enabled, by default all Cisco Jabber users sign in using SSO. Administrators can change this on a per user basis so that certain users do not use SSO and instead sign in with their Cisco Jabber username and password. To disable SSO for a Cisco Jabber user, set the value of the SSO_Enabled parameter to FALSE. If you have configured Cisco Jabber not to ask users for their email address, their first sign in to Cisco Jabber may be non-SSO. In some deployments, the parameter ServicesDomainSsoEmailPrompt needs to be set to ON. This ensures that Cisco Jabber has the information required to perform a first-time SSO sign in. If users signed in to Cisco Jabber previously, this prompt is not needed because the required information is available.

Related Topics

Single Sign-On
Managing SAML SSO in Cisco Unity Connection
SAML SSO Deployment Guide for Cisco Unified Communications Applications

Authenticate with the LDAP Server

Perform this procedure if you want to enable LDAP authentication so that end user passwords are authenticated against the password that is assigned in the company LDAP directory. LDAP authentication gives system administrators the ability to assign an end user a single password for all company applications. This configuration applies to end user passwords only and does not apply to end user PINs or application user passwords. When users sign in to the client, the presence service routes that authentication to Cisco Unified Communications Manager. Cisco Unified Communications Manager then sends that authentication to the directory server.

Procedure

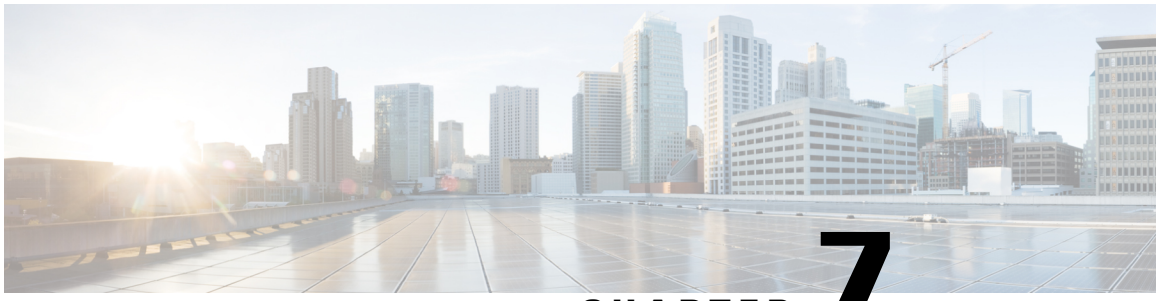
Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **System** > **LDAP** > **LDAP Authentication**.

Step 3 Select **Use LDAP Authentication for End Users**.

Step 4 Specify LDAP credentials and a user search base as appropriate.
See the *Cisco Unified Communications Manager Administration Guide* for information about the fields on the **LDAP Authentication** window.

Step 5 Select **Save**.



CHAPTER 7

Configure Deskphone Control

- Prerequisites, page 17
- Configure Deskphone Control Workflow, page 17
- Add a CTI Service, page 18
- Enable Device for CTI, page 19
- Desk Phone Video Configuration, page 19
- Enable Video Rate Adaptation, page 21
- Configure User Associations, page 22
- Reset Devices, page 24

Prerequisites

The Cisco CTIManager service must be running in the Cisco Unified Communications Manager cluster.

Configure Deskphone Control Workflow

Procedure

	Command or Action	Purpose
Step 1	Add a CTI Service, on page 18	Create a CTI UC service, the information is used by Jabber to locate the CTI Server.
Step 2	Enable Device for CTI, on page 19	Allows Cisco Jabber desktop clients to control the desk phone of the user.
Step 3	Desk Phone Video Configuration, on page 19.	Let users receive video transmitted to their desk phone devices on their computers through the client.

	Command or Action	Purpose
Step 4	Enable Video Rate Adaptation, on page 21	The client uses video rate adaptation to negotiate optimum video quality.
Step 5	Configure User Associations, on page 22	Associate users with devices and assign users to access control groups.
Step 6	Reset Devices, on page 24	You must reset devices after you configure user associations.

Add a CTI Service

The CTI service provides Jabber with the address of the UDS device service. The UDS device service provides a list of devices associated with the user.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **User Management** > **User Settings** > **UC Service**.
The **Find and List UC Services** window opens.

Step 3 Select **Add New**.
The **UC Service Configuration** window opens.

Step 4 In the **Add a UC Service** section, select **CTI** from the **UC Service Type** drop-down list.

Step 5 Select **Next**.

Step 6 Provide details for the instant messaging and presence service as follows:

a) Specify a name for the service in the **Name** field.
The name you specify displays when you add services to profiles. Ensure the name you specify is unique, meaningful, and easy to identify.

b) Specify the CTI service address in the **Host Name/IP Address** field.

c) Specify the port number for the CTI service in the **Port** field.

Step 7 Select **Save**.

What to Do Next

Add the CTI service to your service profile.

Apply a CTI Service

After you add a CTI service on Cisco Unified Communications Manager, you must apply it to a service profile so that the client can retrieve the settings.

Before You Begin

- Create a service profile if none already exists or if you require a separate service profile for CTI.
- Add a CTI service.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **User Management** > **User Settings** > **Service Profile**.
Find and List Service Profiles window opens.

Step 3 Find and select your service profile.
Service Profile Configuration window opens.

Step 4 Navigate to **CTI Profile** section, and select up to three services from the following drop-down lists:

- **Primary**
- **Secondary**
- **Tertiary**

Step 5 Select **Save**.

Enable Device for CTI

If you want Cisco Jabber desktop clients 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.

Procedure

Step 1 In Cisco Unified CM Administration, click **Device** > **Phone** and search for the phone.

Step 2 In the **Device Information** section, check **Allow Control of Device from CTI**.

Step 3 Click **Save**.

Desk Phone Video Configuration

Desk phone video capabilities let users receive video transmitted to their desk phone devices on their computers through the client.

Set Up Desk Phone Video

To set up desk phone video, you must complete the following steps:

1 Physically connect the computer to the computer port on the desk phone device.

You must physically connect the computer to the desk phone device through the computer port so that the client can establish a connection to the device. You cannot use desk phone video capabilities with wireless connections to desk phone devices.

Tip If users have both wireless and wired connections available, they should configure Microsoft Windows so that wireless connections do not take priority over wired connections. See the following Microsoft documentation for more information: *An explanation of the Automatic Metric feature for Internet Protocol routes*.

2 Enable the desk phone device for video in Cisco Unified Communications Manager.

3 Install Cisco Media Services Interface on the computer.

Cisco Media Services Interface provides the Cisco Discover Protocol (CDP) driver that enables the client to do the following:

- Discover the desk phone device.
- Establish and maintain a connection to the desk phone device using the CAST protocol.

Note Download the **Cisco Media Services Interface** installation program from the download site on `cisco.com`.

Desk Phone Video Considerations

Review the following considerations and limitations before you provision desk phone video capabilities to users:

- You cannot use desk phone video capabilities on devices if video cameras are attached to the devices, such as a Cisco Unified IP Phone 9971. You can use desk phone video capabilities if you remove video cameras from the devices.
- You cannot use desk phone video capabilities with devices that do not support CTI.
- Video desktop sharing, using the BFCP protocol, is not supported with desk phone video.
- It is not possible for endpoints that use SCCP to receive video only. SCCP endpoints must send and receive video. Instances where SCCP endpoints do not send video result in audio only calls.
- 7900 series phones must use SCCP for desk phone video capabilities. 7900 series phones cannot use SIP for desk phone video capabilities.
- If a user initiates a call from the keypad on a desk phone device, the call starts as an audio call on the desk phone device. The client then escalates the call to video. For this reason, you cannot make video calls to devices that do not support escalation, such as H.323 endpoints. To use desk phone video capabilities with devices that do not support escalation, users should initiate calls from the client.
- A compatibility issue exists with Cisco Unified IP Phones that use firmware version SCCP45.9-2-1S. You must upgrade your firmware to version SCCP45.9-3-1 to use desk phone video capabilities.

- Some antivirus or firewall applications, such as Symantec EndPoint Protection, block inbound CDP packets, which disables desk phone video capabilities. You should configure your antivirus or firewall application to allow inbound CDP packets.

  See the following Symantec technical document for additional details about this issue: *Cisco IP Phone version 7970 and Cisco Unified Video Advantage is Blocked by Network Threat Protection*.

- You must not select the **Media Termination Point Required** checkbox on the SIP trunk configuration for Cisco Unified Communications Manager. Desk phone video capabilities are not available if you select this checkbox.

Desk Phone Video Troubleshooting

If you encounter an error that indicates desk phone video capabilities are unavailable or the desk phone device is unknown, do the following:

1. Ensure you enable the desk phone device for video in Cisco Unified Communications Manager.
2. Reset the physical desk phone.
3. Exit the client.
4. Run services.msc on the computer where you installed the client.
5. Restart Cisco Media Services Interface.
6. Restart the client.

Enable Video Rate Adaptation

The client uses video rate adaptation to negotiate optimum video quality. Video rate adaptation dynamically increases or decreases video quality based on network conditions.

To use video rate adaptation, you must enable Real-Time Transport Control Protocol (RTCP) on Cisco Unified Communications Manager.

Note RTCP is enabled on software phone devices by default. However, you must enable RTCP on desk phone devices.

Enable RTCP on Common Phone Profiles

You can enable RTCP on a common phone profile to enable video rate adaptation on all devices that use the profile.

Note RTCP is an integral component of Jabber Telephony services. Jabber will continue to send RTCP packets even when disabled.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **Device** > **Device Settings** > **Common Phone Profile**.
The **Find and List Common Phone Profiles** window opens.

Step 3 Specify the appropriate filters in the **Find Common Phone Profile where** field and then select **Find** to retrieve a list of profiles.

Step 4 Select the appropriate profile from the list.
The **Common Phone Profile Configuration** window opens.

Step 5 Locate the **Product Specific Configuration Layout** section.

Step 6 Select **Enabled** from the **RTCP** drop-down list.

Step 7 Select **Save**.

Enable RTCP on Device Configurations

You can enable RTCP on specific device configurations instead of a common phone profile. The specific device configuration overrides any settings you specify on the common phone profile.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **Device** > **Phone**.
The **Find and List Phones** window opens.

Step 3 Specify the appropriate filters in the **Find Phone where** field and then select **Find** to retrieve a list of phones.

Step 4 Select the appropriate phone from the list.
The **Phone Configuration** window opens.

Step 5 Locate the **Product Specific Configuration Layout** section.

Step 6 Select **Enabled** from the **RTCP** drop-down list.

Step 7 Select **Save**.

Configure User Associations

When you associate a user with a device, you provision that device to the user.

Before You Begin

Create and configure Cisco Jabber devices.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **User Management** > **End User**.
The **Find and List Users** window opens.

Step 3 Specify the appropriate filters in the **Find User where** field and then select **Find** to retrieve a list of users.

Step 4 Select the appropriate user from the list.
The **End User Configuration** window opens.

Step 5 Locate the **Service Settings** section.

Step 6 Select **Home Cluster**.

Step 7 Select the appropriate service profile for the user from the **UC Service Profile** drop-down list.

Step 8 Locate the **Device Information** section.

Step 9 Select **Device Association**.
The **User Device Association** window opens.

Step 10 Select the devices to which you want to associate the user. Jabber only supports a single softphone association per device type. For example, only one TCT, BOT, CSF, and TAB device can be associated with a user.

Step 11 Select **Save Selected/Changes**.

Step 12 Select **User Management** > **End User** and return to the **Find and List Users** window.

Step 13 Find and select the same user from the list.
The **End User Configuration** window opens.

Step 14 Locate the **Permissions Information** section.

Step 15 Select **Add to Access Control Group**.
The **Find and List Access Control Groups** dialog box opens.

Step 16 Select the access control groups to which you want to assign the user.
At a minimum you should assign the user to the following access control groups:

- **Standard CCM End Users**
- **Standard CTI Enabled**

Remember If you are provisioning users with secure phone capabilities, do not assign the users to the **Standard CTI Secure Connection** group.

Certain phone models require additional control groups, as follows:

- Cisco Unified IP Phone 9900, 8900, or 8800 series or DX series, select **Standard CTI Allow Control of Phones supporting Connected Xfer and conf**.
- Cisco Unified IP Phone 6900 series, select **Standard CTI Allow Control of Phones supporting Rollover Mode**.

Step 17 Select **Add Selected**.
The **Find and List Access Control Groups** window closes.

Step 18 Select **Save** on the **End User Configuration** window.

Reset Devices

After you create and associate users with devices, you should reset those devices.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **Device** > **Phone**.
The **Find and List Phones** window opens.

Step 3 Specify the appropriate filters in the **Find Phone where** field and then select **Find** to retrieve a list of devices.

Step 4 Select the appropriate device from the list.
The **Phone Configuration** window opens.

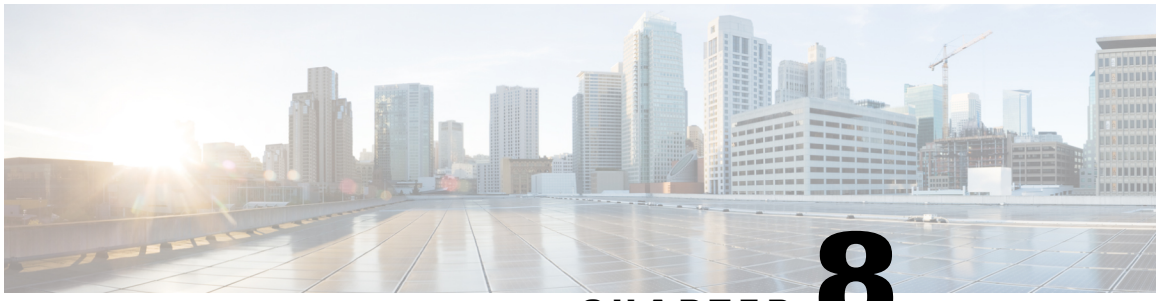
Step 5 Locate the **Association Information** section.

Step 6 Select the appropriate directory number configuration.
The **Directory Number Configuration** window opens.

Step 7 Select **Reset**.
The **Device Reset** dialog box opens.

Step 8 Select **Reset**.

Step 9 Select **Close** to close the **Device Reset** dialog box.



CHAPTER 8

Configure Softphone

- Configure Softphones Workflow, page 25

Configure Softphones Workflow

Procedure

	Command or Action	Purpose
Step 1	Create and Configure Cisco Jabber Devices, on page 25	Create at least one device for every user that will access Cisco Jabber.
Step 2	Configure User Associations, on page 22	
Step 3	Create Mobile SIP Profiles, on page 32.	Complete this task if you have Cisco Unified Communications Manager release 9 and plan to configure devices for mobile clients.
Step 4	Configure the Phone Security Profile, on page 33	Complete this task to set up secure phone capabilities for all devices.
Step 5	Provide Users with Authentication Strings, on page 34	

Create and Configure Cisco Jabber Devices

Create at least one device for every user that accesses Cisco Jabber. A user can have multiple devices.

Note Users can only remove participants from a conference call when using the softphone(CSF) device for calls.

Before You Begin

- Install COP files.
- Enable mobility for each user for whom you plan to assign to a CTI remote device.
- Create SIP profiles if you have Cisco Unified Communications Manager release 9 or earlier and plan to configure devices for mobile clients.
- Create the Phone Security Profile if you plan to set up secure phone capabilities for all devices.
- For Cisco Unified Communications Manager release 10 or later, ensure that the Cisco Certificate Authority Proxy Function (CAPF) service parameters value for **Certificate Issuer to Endpoint** is **Cisco Certificate Authority Proxy Function**, this is the only option supported by Cisco Jabber. For information on configuring the CAPF service parameter see the *Update CAPF Service Parameters* topic in the Cisco Unified Communications Manager Security Guides.
- Before you create TCT devices, BOT devices, or TAB devices for Cisco Jabber for mobile users, specify the organization top domain name to support registration between Cisco Jabber and the Cisco Unified Communications Manager. In Unified CM Administration interface, select **System** > **Enterprise Parameters**. Under the Clusterwide Domain Configuration section, enter the organization top domain name. For example, cisco.com. This top domain name is used by Jabber as the DNS domain of the Cisco Unified Communications Manager servers for phone registration. For example, CUCMServer1@cisco.com.

Procedure

Step 1 Log in to the **Cisco Unified CM Administration** interface.

Step 2 Select **Device** > **Phone**.
Find and List Phones window opens.

Step 3 Select **Add New**.

Step 4 From the **Phone Type** drop-down list, select the option that is applicable to the device type you are configuring and then select **Next**.
For Jabber users, you can only create one type of device per user although you can create multiple devices for each user. For example, you can create one tablet device and one CSF device but not two CSF devices.

- **Cisco Unified Client Services Framework—**Select this option to create a CSF device for Cisco Jabber for Mac or Cisco Jabber for Windows.
- **Cisco Dual Mode for iPhone—**Select this option to create a TCT device for an iPhone.
- **Cisco Jabber for Tablet—**Select this option to create a TAB device for an iPad or an Android tablet.
- **Cisco Dual Mode for Android—**Select this option to create a BOT device for an Android device.
- **CTI Remote Device—**Select this option to create a CTI remote device.
  CTI remote devices are virtual devices that monitor and have call control over a user's remote destination.

Step 5 From the **Owner User ID** drop-down list, select the user for whom you want to create the device.
For the **Cisco Unified Client Services Framework** option in a Phone mode deployment, ensure that **User** is selected.

Step 6 In the **Device Name** field, use the applicable format to specify a name for the device:

If You Select	Required Format
CTI Remote Device	• When you select **Owner User ID**, the device name field populates with *CTIRD<owner user ID>*. You can change this value. The device name does not have to begin with *CTIRD*. • Valid characters: a–z, A–Z, 0–9, period (.), underscore (_), hyphen (-). • 15-character limit.
Cisco Unified Client Services Framework	• Valid characters: a–z, A–Z, 0–9. • 15-character limit.
Cisco Dual Mode for iPhone	• The device name must begin with *TCT*. For example, if you create a TCT device for user, Tanya Adams, whose username is tadams, enter TCTTADAMS. • Must be uppercase. • Valid characters: A–Z, 0–9, period (.), underscore (_), hyphen (-). • 15-character limit.
Cisco Jabber for Tablet	• The device name must begin with *TAB*. For example, if you create a TAB device for user, Tanya Adams, whose username is tadams, enter TABTADAMS. • Must be uppercase. • Valid characters: A–Z, 0–9, period (.), underscore (_), hyphen (-). • 15-character limit.

If You Select	Required Format
Cisco Dual Mode for Android	• The device name must begin with *BOT*. For example, if you create a BOT device for user, Tanya Adams, whose username is tadams, enter BOTTADAMS. • Must be uppercase. • Valid characters: A–Z, 0–9, period (.), underscore (_), hyphen (-). • 15-character limit.

Step 7 If you are creating a CTI Remote Device, in the **Protocol Specific Information** section, select an appropriate option from the **Rerouting Calling Search Space** drop-down list.
The Rerouting Calling Search Space defines the calling search space for rerouting and ensures that users can send and receive calls from the CTI remote device.

Step 8 To generate an authentication string that you can provide to end users to access their devices and securely register to Cisco Unified Communications Manager, navigate to the **Certification Authority Proxy Function (CAPF) Information** section.

Step 9 From the **Certificate Operation** drop-down list, select **Install/Upgrade**.

Step 10 From the **Authentication Mode** drop-down list, select **By Authentication String** or **By Null String**.

Note Using the CAPF Authentication mode **By Null String** with VXME and Jabber for Windows CSF devices is not supported. It causes Jabber registration with Cisco Unified Communications Manager (CUCM) to fail.

Step 11 Click **Generate String**.
The Authentication String autopopulates with a string value. This is the string that you will provide to end users.

Step 12 From the **Key Size (Bits)** drop-down list, select the same key size that you set in the phone security profile.

Step 13 In the **Operation Completes By** fields, specify an expiration value for the authentication string or leave as default.

Step 14 If you are using a group configuration file, specify it in the **Cisco Support Field** of the **Desktop Client Settings.** Cisco Jabber does not use any other settings that are available on the **Desktop Client Settings**.

Step 15 Select **Save**.

Step 16 Click **Apply Config**.

What to Do Next

Add a Directory Number to the device.

Add a Directory Number to the Device

After you create and configure each device, you must add a directory number to the device. This topic provides instructions on adding directory numbers using the **Device** > **Phone** menu option.

Before You Begin

Create a device.

Procedure

Step 1 Locate the **Association Information** section on the **Phone Configuration** window.
Step 2 Click **Add a new DN**.
Step 3 In the **Directory Number** field, specify a directory number.
Step 4 In the **Users Associated with Line** section, click **Associate End Users**.
Step 5 In the **Find User where** field, specify the appropriate filters and then click **Find**.
Step 6 From the list that appears, select the applicable users and click **Add Selected**.
Step 7 Specify all other required configuration settings as appropriate.
Step 8 Select **Apply Config**.
Step 9 Select **Save**.

Add a Remote Destination

Remote destinations represent the CTI controllable devices that are available to users.

You should add a remote destination through the **Cisco Unified CM Administration** interface if you plan to provision users with dedicated CTI remote devices. This task ensures that users can automatically control their phones and place calls when they start the client.

If you plan to provision users with CTI remote devices along with software phone devices and desk phone devices, you should not add a remote destination through the **Cisco Unified CM Administration** interface. Users can enter remote destinations through the client interface.

Note

- You should create only one remote destination per user. Do not add two or more remote destinations for a user.
- Cisco Unified Communications Manager does not verify if it can route remote destinations that you add through the **Cisco Unified CM Administration** interface. For this reason, you must ensure that Cisco Unified Communications Manager can route the remote destinations you add.
- Cisco Unified Communications Manager automatically applies application dial rules to all remote destination numbers for CTI remote devices.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.
Step 2 Select **Device** > **Phone**.

The **Find and List Phones** window opens.

Step 3 Specify the appropriate filters in the **Find Phone where** field to and then select **Find** to retrieve a list of phones.

Step 4 Select the CTI remote device from the list.
The **Phone Configuration** window opens.

Step 5 Locate the **Associated Remote Destinations** section.

Step 6 Select **Add a New Remote Destination**.
The **Remote Destination Information** window opens.

Step 7 Specify JabberRD in the **Name** field.

Restriction You must specify JabberRD in the **Name** field. The client uses only the JabberRD remote destination. If you specify a name other than JabberRD, users cannot access that remote destination.

The client automatically sets the JabberRD name when users add remote destinations through the client interface.

Step 8 Enter the destination number in the **Destination Number** field.

Step 9 Specify all other values as appropriate.

Step 10 Select **Save**.

What to Do Next

Complete the following steps to verify the remote destination and apply the configuration to the CTI remote device:

1. Repeat the steps to open the **Phone Configuration** window for the CTI remote device.
2. Locate the **Associated Remote Destinations** section.
3. Verify the remote destination is available.
4. Select **Apply Config**.

Note The **Device Information** section on the **Phone Configuration** window contains a **Active Remote Destination** field.

When users select a remote destination in the client, it displays as the value of **Active Remote Destination**.

none displays as the value of **Active Remote Destination** if:

- Users do not select a remote destination in the client.
- Users exit or are not signed in to the client.

Configure User Associations

When you associate a user with a device, you provision that device to the user.

Before You Begin

Create and configure Cisco Jabber devices.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **User Management** > **End User**.
The **Find and List Users** window opens.

Step 3 Specify the appropriate filters in the **Find User where** field and then select **Find** to retrieve a list of users.

Step 4 Select the appropriate user from the list.
The **End User Configuration** window opens.

Step 5 Locate the **Service Settings** section.

Step 6 Select **Home Cluster**.

Step 7 Select the appropriate service profile for the user from the **UC Service Profile** drop-down list.

Step 8 Locate the **Device Information** section.

Step 9 Select **Device Association**.
The **User Device Association** window opens.

Step 10 Select the devices to which you want to associate the user. Jabber only supports a single softphone association per device type. For example, only one TCT, BOT, CSF, and TAB device can be associated with a user.

Step 11 Select **Save Selected/Changes**.

Step 12 Select **User Management** > **End User** and return to the **Find and List Users** window.

Step 13 Find and select the same user from the list.
The **End User Configuration** window opens.

Step 14 Locate the **Permissions Information** section.

Step 15 Select **Add to Access Control Group**.
The **Find and List Access Control Groups** dialog box opens.

Step 16 Select the access control groups to which you want to assign the user.
At a minimum you should assign the user to the following access control groups:

- **Standard CCM End Users**
- **Standard CTI Enabled**

Remember If you are provisioning users with secure phone capabilities, do not assign the users to the **Standard CTI Secure Connection** group.

Certain phone models require additional control groups, as follows:

- Cisco Unified IP Phone 9900, 8900, or 8800 series or DX series, select **Standard CTI Allow Control of Phones supporting Connected Xfer and conf**.
- Cisco Unified IP Phone 6900 series, select **Standard CTI Allow Control of Phones supporting Rollover Mode**.

Step 17 Select **Add Selected**.

The **Find and List Access Control Groups** window closes.

Step 18 Select **Save** on the **End User Configuration** window.

Create Mobile SIP Profiles

This procedure is required only when you use Cisco Unified Communication Manager release 9 and are configuring devices for mobile clients. Use the default SIP profile provided for desktop clients. Before you create and configure devices for mobile clients, you must create a SIP profile that allows Cisco Jabber to stay connected to Cisco Unified Communication Manager while Cisco Jabber runs in the background.

If you use Cisco Unified Communication Manager Release 10, choose the **Standard SIP Profile for Mobile Device** default profile when you create and configure devices for mobile clients.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **Device** > **Device Settings** > **SIP Profile**.
The **Find and List SIP Profiles** window opens.

Step 3 Do one of the following to create a new SIP profile:

- Find the default SIP profile and create a copy that you can edit.
- Select **Add New** and create a new SIP profile.

Step 4 In the new SIP profile, set the following values:

- **Timer Register Delta** = 120
- **Timer Register Expires** = 720
- **Timer Keep Alive Expires** = 720
- **Timer Subscribe Expires** = 21600
- **Timer Subscribe Delta** = 15

Step 5 Select **Save**.

Setting up System SIP Parameters

If you are connected to a low-bandwidth network and finding it difficult to take an incoming call on your mobile device, you can set the system SIP parameters to improve the condition. Increase the SIP Dual Mode Alert Timer value to ensure that calls to the Cisco Jabber extension are not prematurely routed to the mobile-network phone number.

Before You Begin

This configuration is only for mobile clients.

Cisco Jabber must be running to receive work calls.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **System** > **Service Parameters**.

Step 3 Select the node.

Step 4 Select the **Cisco CallManager (Active)** service.

Step 5 Scroll to the **Clusterwide Parameters (System - Mobility)** section.

Step 6 Increase the **SIP Dual Mode Alert Timer** value to 10000 milliseconds.

Step 7 Select **Save**.

Note If, after you increase the SIP Dual Mode Alert Timer value, incoming calls that arrive in Cisco Jabber are still terminated and diverted using Mobile Connect, you can increase the SIP Dual Mode Alert Timer value again in increments of 500 milliseconds.

Configure the Phone Security Profile

You can optionally set up secure phone capabilities for all devices. Secure phone capabilities provide secure SIP signaling, secure media streams, and encrypted device configuration files.

If you enable secure phone capabilities for users, device connections to Cisco Unified Communications Manager are secure. However, calls with other devices are secure only if both devices have a secure connection.

Before You Begin

- Configure the Cisco Unified Communications Manager security mode using the Cisco CTL Client. At minimum, select mixed mode security.

  For instructions on how to configure mixed mode with the Cisco CTL Client, see the Cisco Unified Communications Manager Security Guide.

- For conference calls, ensure that the conferencing bridge supports secure phone capabilities. If the conferencing bridge does not support secure phone capabilities, calls to that bridge are not secure. Likewise, all parties must support a common encryption algorithm for the client to encrypt media on conference calls.

Procedure

Step 1 In **Cisco Unified Communications Manager**, select **System** > **Security** > **Phone Security Profile**.

Step 2 Select **Add New**.

Step 3 From the **Phone Type** drop-down list, select the option that is applicable to the device type you are configuring and then select **Next**.

- **Cisco Unified Client Services Framework—**Select this option to create a CSF device for Cisco Jabber for Mac or Cisco Jabber for Windows.
- **Cisco Dual Mode for iPhone—**Select this option to create a TFT device for an iPhone.
- **Cisco Jabber for Tablet—**Select this option to create a TAB device for an iPad or an Android tablet.
- **Cisco Dual Mode for Android—**Select this option to create a BOT device for an Android device.
- **CTI Remote Device—**Select this option to create a CTI remote device.
  CTI remote devices are virtual devices that monitor and have call control over a user's remote destination.

Step 4 In the **Name** field of the **Phone Security Profile Configuration** window, specify a name for the phone security profile.

Step 5 For **Device Security Mode**, select one of the following options:

- **Authenticated—**The SIP connection is over TLS using NULL-SHA encryption.
- **Encrypted—**The SIP connection is over TLS using AES 128/SHA encryption. The client uses Secure Real-time Transport Protocol (SRTP) to offer encrypted media streams.

Step 6 For **Transport Type**, leave the default value of **TLS**.

Step 7 Select the **TFTP Encrypted Config** check box to encrypt the device configuration file that resides on the TFTP server.

Note For a TCT/BOT/Tablet device, do not select the TFTP Encrypted Config check box here. For Authentication Mode, select By Authentication String or Null String.

Step 8 For **Authentication Mode**, select **By Authentication String** or **By Null String**.

Note Using the CAPF Authentication mode **By Null String** with VXME and Jabber for Windows CSF devices is not supported. It causes Jabber registration with Cisco Unified Communications Manager (CUCM) to fail.

Step 9 For **Key Size (Bits)**, select the appropriate key size for the certificate. Key size refers to the bit length of the public and private keys that the client generates during the CAPF enrollment process.
The Cisco Jabber clients were tested using authentication strings with 1024-bit length keys. The Cisco Jabber clients require more time to generate 2048-bit length keys than 1024-bit length keys. As a result, if you select 2048, expect it to take longer to complete the CAPF enrollment process.

Step 10 For **SIP Phone Port**, leave the default value.
The port that you specify in this field takes effect only if you select **Non Secure** as the value for **Device Security Mode**.

Step 11 Click **Save**.

Provide Users with Authentication Strings

Users must specify the authentication string in the client interface to access their devices and securely register with Cisco Unified Communications Manager.

When users enter the authentication string in the client interface, the CAPF enrollment process begins.

Note The time it takes for the enrollment process to complete can vary depending on the user's computer or mobile device and the current load for Cisco Unified Communications Manager. It can take up to one minute for the client to complete the CAPF enrollment process.

The client displays an error if:

- Users enter an incorrect authentication string.

  Users can attempt to enter authentication strings again to complete the CAPF enrollment. However, if a user continually enters an incorrect authentication string, the client might reject any string the user enters, even if the string is correct. In this case, you must generate a new authentication string on the user's device and then provide it to the user.

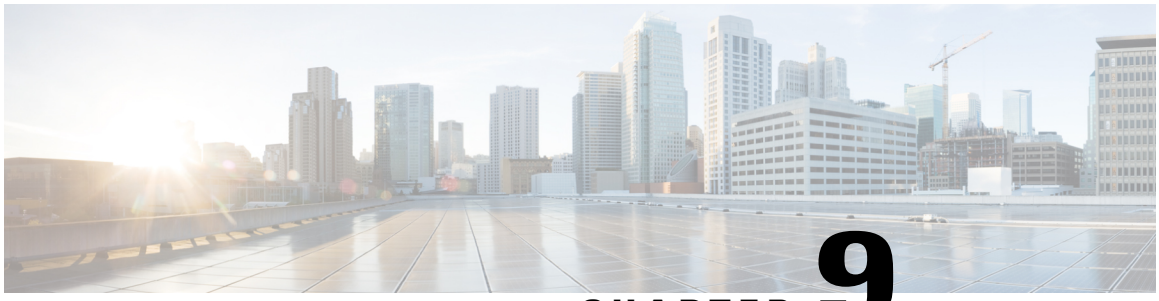
- Users do not enter the authentication string before the expiration time you set in the **Operation Completes By** field.

  In this case, you must generate a new authentication string on the user's device. The user must then enter that authentication string before the expiration time.

Important When you configure the end users in Cisco Unified Communications Manager, you must add them to the following user groups:

- **Standard CCM End Users**
- **Standard CTI Enabled**

Users must not belong to the Standard CTI Secure Connection user group.



CHAPTER 9

Configure Extend and Connect

- Configure Extend and Connect Workflow, page 37

Configure Extend and Connect Workflow

Procedure

	Command or Action	Purpose
Step 1	Enable User Mobility, on page 37	
Step 2	Create CTI Remote Devices, on page 38	
Step 3	Configure User Associations, on page 22	

Enable User Mobility

This task is only for desktop clients.

You must enable user mobility to provision CTI remote devices. If you do not enable mobility for users, you cannot assign those users as owners of CTI remote devices.

Before You Begin

This task is applicable only if:

- You plan to assign Cisco Jabber for Mac or Cisco Jabber for Windows users to CTI remote devices.
- You have Cisco Unified Communication Manager release 9.x and later.

Procedure

Step 1 Select **User Management** > **End User**.

The **Find and List Users** window opens.

Step 2 Specify the appropriate filters in the **Find User where** field to and then select **Find** to retrieve a list of users.

Step 3 Select the user from the list.
The **End User Configuration** window opens.

Step 4 Locate the **Mobility Information** section.

Step 5 Select **Enable Mobility**.

Step 6 Select **Save**.

Create CTI Remote Devices

CTI remote devices are virtual devices that monitor and have call control over a user's remote destination.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **Device** > **Phone**.
The **Find and List Phones** window opens.

Step 3 Select **Add New**.

Step 4 Select **CTI Remote Device** from the **Phone Type** drop-down list and then select **Next**.
The **Phone Configuration** window opens.

Step 5 Select the appropriate user ID from the **Owner User ID** drop-down list.

Note Only users for whom you enable mobility are available from the **Owner User ID** drop-down list. For more information, see Enable SAML SSO in the Client.

Cisco Unified Communications Manager populates the **Device Name** field with the user ID and a **CTIRD** prefix; for example, **CTIRDusername**

Step 6 Edit the default value in the **Device Name** field, if appropriate.

Step 7 Ensure you select an appropriate option from the **Rerouting Calling Search Space** drop-down list in the **Protocol Specific Information** section.
The **Rerouting Calling Search Space** drop-down list defines the calling search space for re-routing and ensures that users can send and receive calls from the CTI remote device.

Step 8 Specify all other configuration settings on the **Phone Configuration** window as appropriate.
See the *CTI remote device setup* topic in the System Configuration Guide for Cisco Unified Communications Manager documentation for more information.

Step 9 Select **Save**.
The fields to associate directory numbers and add remote destinations become available on the **Phone Configuration** window.

Configure User Associations

When you associate a user with a device, you provision that device to the user.

Before You Begin

Create and configure Cisco Jabber devices.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **User Management** > **End User**.
The **Find and List Users** window opens.

Step 3 Specify the appropriate filters in the **Find User where** field and then select **Find** to retrieve a list of users.

Step 4 Select the appropriate user from the list.
The **End User Configuration** window opens.

Step 5 Locate the **Service Settings** section.

Step 6 Select **Home Cluster**.

Step 7 Select the appropriate service profile for the user from the **UC Service Profile** drop-down list.

Step 8 Locate the **Device Information** section.

Step 9 Select **Device Association**.
The **User Device Association** window opens.

Step 10 Select the devices to which you want to associate the user. Jabber only supports a single softphone association per device type. For example, only one TCT, BOT, CSF, and TAB device can be associated with a user.

Step 11 Select **Save Selected/Changes**.

Step 12 Select **User Management** > **End User** and return to the **Find and List Users** window.

Step 13 Find and select the same user from the list.
The **End User Configuration** window opens.

Step 14 Locate the **Permissions Information** section.

Step 15 Select **Add to Access Control Group**.
The **Find and List Access Control Groups** dialog box opens.

Step 16 Select the access control groups to which you want to assign the user.
At a minimum you should assign the user to the following access control groups:

- **Standard CCM End Users**
- **Standard CTI Enabled**

Remember If you are provisioning users with secure phone capabilities, do not assign the users to the **Standard CTI Secure Connection** group.

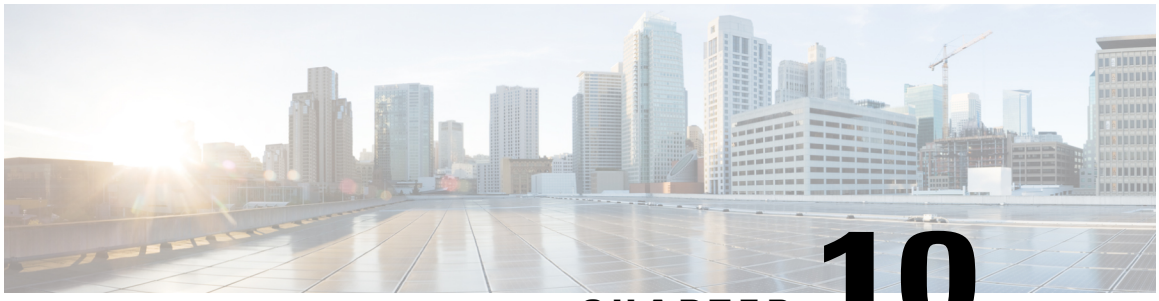
Certain phone models require additional control groups, as follows:

- Cisco Unified IP Phone 9900, 8900, or 8800 series or DX series, select **Standard CTI Allow Control of Phones supporting Connected Xfer and conf**.

- Cisco Unified IP Phone 6900 series, select **Standard CTI Allow Control of Phones supporting Rollover Mode**.

Step 17 Select **Add Selected**.
The **Find and List Access Control Groups** window closes.

Step 18 Select **Save** on the **End User Configuration** window.



CHAPTER 10

Configure Service Discovery for Remote Access

- Service Discovery Requirements, page 41

Service Discovery Requirements

Service discovery enables clients to automatically detect and locate services on your enterprise network. Expressway for Mobile and Remote Access allows you to access the services on your enterprise network. You should meet the following requirements to enable the clients to connect through Expressway for Mobile and Remote Access and discover services:

- DNS requirements
- Certificate requirements
- Test external SRV `_collab-edge`.

DNS Requirements

The DNS requirements for service discovery through remote access are:

- Configure a `_collab-edge` DNS SRV record on an external DNS server.
- Configure a `_cisco-uds` DNS SRV record on the internal name server.
- Optionally, if you deploy a hybrid cloud-based architecture where the domain of the IM and presence server differs from the domain of the voice server, ensure that you configure the Voice Services Domain to locate the DNS server that contains the `_collab-edge` record.

Certificate Requirements

Before you configure remote access, download the Cisco VCS Expressway and Cisco Expressway-E Server certificate. The Server certificate is used for both HTTP and XMPP.

For more information on configuring Cisco VCS Expressway certificate, see Configuring Certificates on Cisco VCS Expressway.

Test _collab-edge SRV Record

Procedure

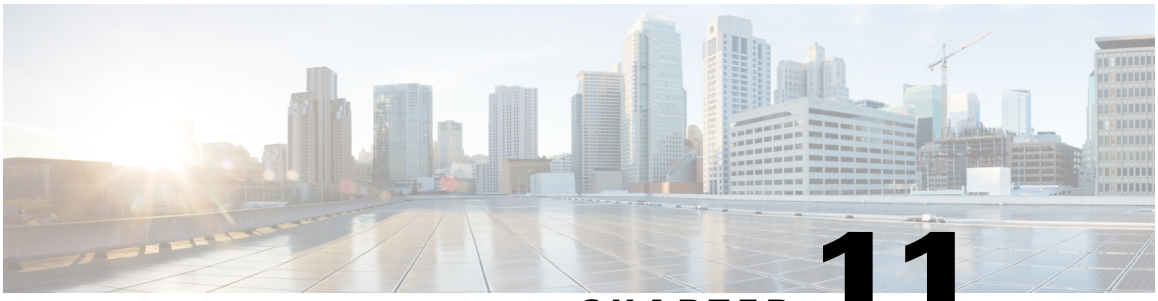
Step 1 Open a command prompt.

Step 2 Enter **nslookup**.
The default DNS server and address is displayed. Confirm that this is the expected DNS server.

Step 3 Enter **set type=SRV**.

Step 4 Enter the name for each of your SRV records.
For example `_collab-edge.`*`exampledomain`*

- Displays server and address—SRV record is accessible.
- Displays `_collab-edge.`*`exampledomain`*`: Non-existent domain`—There is an issue with your SRV record.



CHAPTER 11

Set Up Certificate Validation

- Certificate Validation for Cloud Deployments, page 43

Certificate Validation for Cloud Deployments

Cisco WebEx Messenger and Cisco WebEx Meeting Center present the following certificates to the client by default:

- CAS
- WAPI

Note Cisco WebEx certificates are signed by a public Certificate Authority (CA). Cisco Jabber validates these certificates to establish secure connections with cloud-based services.

Cisco Jabber validates the following XMPP certificates received from Cisco WebEx Messenger. If these certificates are not included in your operating system, you must provide them.

- VeriSign Class 3 Public Primary Certification Authority - G5 — This certificate is stored in the Trusted Root Certificate Authority
- VeriSign Class 3 Secure Server CA - G3 —T his certificate validates the Webex Messenger server identity and is stored in the Intermediate Certificate Authority.
- AddTrust External CA Root
- GoDaddy Class 2 Certification Authority Root Certificate

For more information about root certificates for Cisco Jabber for Windows, see http://www.identrust.co.uk/certificates/trustid/install-nes36.html.

For more information about root certificates for Cisco Jabber for Mac, see http://support.apple.com.

Update Profile Photo URLs

In cloud-based deployments, Cisco WebEx assigns unique URLs to profile photos when you add or import users. When Cisco Jabber resolves contact information, it retrieves the profile photo from Cisco WebEx at the URL where the photo is hosted.

Profile photo URLs use HTTP Secure (`https://server_name/`) and present certificates to the client. If the server name in the URL is:

- A fully qualified domain name (FQDN) that contains the Cisco WebEx domain — The client can validate the web server that is hosting the profile photo against the Cisco WebEx certificate.
- An IP address — The client cannot validate the web server that is hosting the profile photo against the Cisco WebEx certificate. In this case, the client prompts users to accept certificates whenever they look up contacts with an IP address in their profile photo URLs.

Important

- We recommend that you update all profile photo URLs that contain an IP address as the server name. Replace the IP address with the FQDN that contains the Cisco WebEx domain to ensure that the client does not prompt users to accept certificates.
- When you update a photo, the photo can take up to 24 hours to refresh in the client.

The following steps describe how to update profile photo URLs. Refer to the appropriate Cisco WebEx documentation for detailed instructions.

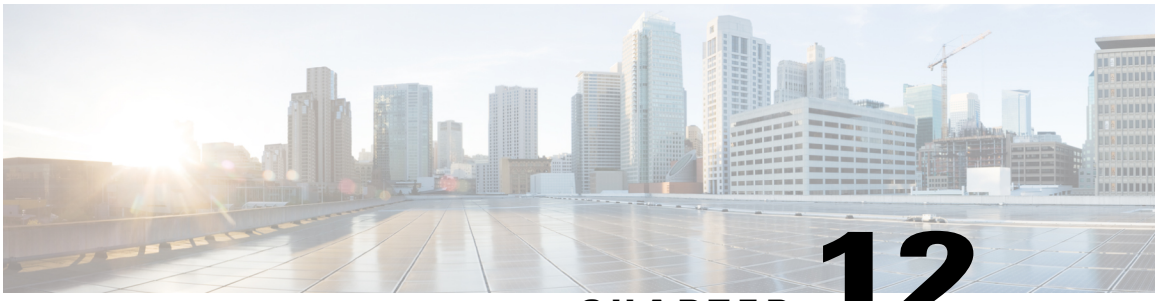
Procedure

Step 1 Export user contact data in CSV file format with the Cisco WebEx Administration Tool.

Step 2 In the **userProfilePhotoURL** field, replace IP addresses with the Cisco WebEx domain.

Step 3 Save the CSV file.

Step 4 Import the CSV file with the Cisco WebEx Administration Tool.



CHAPTER 12

Configure the Clients

- Client Configuration Workflow, page 45

Client Configuration Workflow

Procedure

	Command or Action	Purpose
Step 1	Introduction to Client Configuration, on page 45	
Step 2	Create and Host Client Configuration Files, on page 46	
Step 3	Set Parameters on Phone Configuration for Desktop Clients, on page 51	
Step 4	Set Parameters on Phone Configuration for Mobile Clients, on page 52	
Step 5	Configure Proxy Setting, on page 53	

Introduction to Client Configuration

Cisco Jabber can retrieve configuration settings from the following sources:

- Service Profiles — You can configure some client settings in UC service profiles on Cisco Unified Communications Manager release 9 and later. When users launch the client, it discovers the Cisco Unified Communications Manager home cluster using a DNS SRV record and automatically retrieves the configuration from the UC service profile.

  Applies to on-premises deployments only.

- Phone Configuration — You can set some client settings in the phone configuration on Cisco Unified Communications Manager release 9 and later. The client retrieves the settings from the phone configuration in addition to the configuration in the UC service profile.

  Applies to on-premises deployments only.

- Cisco Unified Communications Manager IM and Presence Service — You can enable instant messaging and presence capabilities and configure certain settings such as presence subscription requests.

  In the **Advanced settings** window, if you select **Cisco IM & Presence**, the client retrieves UC services from Cisco Unified Communications Manager IM and Presence Service. The client does not use service profiles or SSO discovery.

  Applies to on-premises deployments only.

- Client Configuration Files — You can create XML files that contain configuration parameters. You then host the XML files on a TFTP server. When users sign in, the client retrieves the XML file from the TFTP server and applies the configuration.

  Applies to on-premises and cloud-based deployments.

- Cisco WebEx Administration Tool — You can configure some client settings with the Cisco WebEx Administration Tool.

  You can upload a `jabber-config.xml` client configuration file into the Cisco WebEx Administration Tool. You can apply separate configuration files for groups in the Cisco WebEx Messenger Administration Tool. When the client successfully connects to Cisco WebEx Messenger it downloads the XML file and the configuration is applied.

  The client will use the following order for configuration settings:

  1. Settings in Cisco WebEx Messenger Administration Tool
  2. Settings in `jabber-config.xml` file from Cisco WebEx Messenger Administration Tool.

     Note Group configuration file settings take priority over the configuration file in Cisco WebEx Messenger Administration Tool.

  3. Settings in `jabber-config.xml` file from the TFTP server.

  If there are any conflicts with configuration settings, the settings set in Cisco WebEx Administration tool will take priority over this configuration file.

  Applies to cloud-based deployments only.

Create and Host Client Configuration Files

For on-premises and hybrid cloud-based deployments, create client configuration files and host them on the Cisco Unified Communications Manager TFTP service.

For cloud-based deployments, configure the client with the Cisco WebEx Administration Tool. However, you can optionally set up a TFTP server to configure the client with settings that are not available in Cisco WebEx Administration Tool.

For Cisco Jabber for iPhone and iPad and Cisco Jabber for Android, you must create a global configuration file to set up:

- Directory integration for on-premises deployments.
- Voicemail service credentials for hybrid-cloud deployments.

Note In most environments, Cisco Jabber for Windows and Cisco Jabber for Mac do not require any configuration to connect to services. Create a configuration file only if you require custom content such as automatic updates, problem reporting, or user policies and options.

Before You Begin

Note the following configuration file requirements:

- Configuration filenames are case-sensitive. Use lowercase letters in the filename to prevent errors and to ensure the client can retrieve the file from the TFTP server.
- You must use utf-8 encoding for the configuration files.
- The client cannot read configuration files that do not have a valid XML structure. Check the structure of your configuration file for closing elements and confirm that elements are nested correctly.
- Valid XML character entity references only are permitted in your configuration file. For example, use `&` instead of `&`. If your XML contains invalid characters, the client cannot parse the configuration file.

  To validate your configuration file, open the file in Microsoft Internet Explorer.

  - If Internet Explorer displays the entire XML structure, your configuration file does is valid.
  - If Internet Explorer displays only part of the XML structure, it is likely that your configuration file contains invalid characters or entities.

Procedure

	Command or Action	Purpose
Step 1	Specify Your TFTP Server Address, on page 47	Specify your TFTP server address for client to enable access to your configuration file.
Step 2	Create Global Configurations, on page 48	Configure the clients for users in your deployment.
Step 3	Create Group Configurations, on page 48	Apply different configuration to different set of users.
Step 4	Host Configuration Files, on page 49	Host configuration files on any TFTP server.
Step 5	Restart Your TFTP Server, on page 50	Restart the TFTP server before the client can access the configuration files.

Specify Your TFTP Server Address

The client gets configuration files from a TFTP server. The first step in configuring the client is to specify your TFTP server address so the client can access your configuration file.

Attention If Cisco Jabber gets the `_cisco-uds` SRV record from a DNS query, it can automatically locate the user's home cluster. As a result, the client can also locate the Cisco Unified Communications Manager TFTP service.

You do not need to specify your TFTP server address if you deploy the `_cisco-uds` SRV record.

Specify TFTP Servers in Phone Mode

If you deploy the client in phone mode you can provide the address of the TFTP server as follows:

- Users manually enter the TFTP server address when they start the client.
- You specify the TFTP server address during installation with the TFTP argument.
- You specify the TFTP server address in the Microsoft Windows registry.

Create Global Configurations

The client downloads the global configuration file from your TFTP server during the login sequence. Configure the client for all users in your deployment.

Before You Begin

If the structure of your configuration file is not valid, the client cannot read the values you set. Review the XML samples in this chapter for more information.

Procedure

Step 1 Create a file named `jabber-config.xml` with any text editor.

- Use lowercase letters in the filename.
- Use UTF-8 encoding.

Step 2 Define the required configuration parameters in `jabber-config.xml`.

Step 3 Host the group configuration file on your TFTP server.
If your environment has multiple TFTP servers, ensure that the configuration file is the same on all TFTP servers.

Create Group Configurations

Group configuration files apply to subsets of users and are supported on Cisco Jabber for desktop (CSF devices) and on Cisco Jabber for mobile devices. Group configuration files take priority over global configuration files.

If you provision users with CSF devices, specify the group configuration filenames in the **Cisco Support Field** field on the device configuration. If users do not have CSF devices, set a unique configuration filename for each group during installation with the TFTP_FILE_NAME argument.

Before You Begin

- If the structure of your configuration file is not valid, the client cannot read the values you set. Review the XML samples in this chapter for more information.

Procedure

Step 1 Create an XML group configuration file with any text editor.
The group configuration file can have any appropriate name; for example, `jabber-groupa-config.xml`.

Step 2 Define the required configuration parameters in the group configuration file.

Step 3 Add the group configuration file to applicable CSF devices.

a) Open the **Cisco Unified CM Administration** interface.
b) Select **Device** > **Phone**.
c) Find and select the appropriate CSF device to which the group configuration applies.
d) In the **Phone Configuration** window, navigate to **Product Specific Configuration Layout** > **Desktop Client Settings**.
e) In the **Cisco Support Field** field, enter `configurationfile=`*`group_configuration_file_name.xml`*. For example, enter `configurationfile=groupa-config.xml`.

Note If you host the group configuration file on your TFTP server in a location other than the default directory, you must specify the path and the filename; for example, `configurationfile=/customFolder/groupa-config.xml`.

Do not add more than one group configuration file. The client uses only the first group configuration in the **Cisco Support Field** field.

f) Select **Save**.

Step 4 Host the group configuration file on your TFTP server.

Host Configuration Files

You can host configuration files on any TFTP server. However, Cisco recommends hosting configuration files on the Cisco Unified Communications Manager TFTP server, which is the same as that where the device configuration file resides.

Procedure

Step 1 Open the **Cisco Unified OS Administration** interface on Cisco Unified Communications Manager.

Step 2 Select **Software Upgrades** > **TFTP File Management**.

Step 3 Select **Upload File**.

Step 4 Select **Browse** in the **Upload File** section.

Step 5 Select the configuration file on the file system.

Step 6 Do not specify a value in the **Directory** text box in the **Upload File** section.
You should leave an empty value in the **Directory** text box so that the configuration file resides in the default directory of the TFTP server.

Step 7 Select **Upload File**.

Restart Your TFTP Server

You must restart your TFTP server before the client can access the configuration files.

Procedure

Step 1 Open the **Cisco Unified Serviceability** interface on Cisco Unified Communications Manager.

Step 2 Select **Tools** > **Control Center - Feature Services**.

Step 3 Select **Cisco Tftp** from the **CM Services** section.

Step 4 Select **Restart**.
A window displays to prompt you to confirm the restart.

Step 5 Select **OK**.
The **Cisco Tftp Service Restart Operation was Successful** status displays.

Step 6 Select **Refresh** to ensure the **Cisco Tftp** service starts successfully.

What to Do Next

To verify that the configuration file is available on your TFTP server, open the configuration file in any browser. Typically, you can access the global configuration file at the following URL:
`http://tftp_server_address:6970/jabber-config.xml`

Configuration File

For detailed information on the *jabber-config.xml* configuration file structure, group elements, parameters, and examples, see the Parameters Reference Guide for Cisco Jabber.

Set Parameters on Phone Configuration for Desktop Clients

The client can retrieve configuration settings in the phone configuration from the following locations on Cisco Unified Communications Manager:

Enterprise Phone Configuration

Applies to the entire cluster.

Note For users with only IM and Presence Service capabilities (IM only), you must set phone configuration parameters in the **Enterprise Phone Configuration** window.

Common Phone Profile Configuration

Applies to groups of devices and takes priority over the cluster configuration.

Cisco Unified Client Services Framework (CSF) Phone Configuration

Applies to individual CSF devices and takes priority over the group configuration.

Parameters in Phone Configuration

The following table lists the configuration parameters you can set in the **Product Specific Configuration Layout** section of the phone configuration and maps corresponding parameters from the client configuration file:

Desktop Client Settings Configuration	Description
Video Calling	Enables or disables video capabilities. **Enabled (default)** Users can send and receive video calls. **Disabled** Users cannot send or receive video calls. **Restriction** This parameter is available only on the CSF device configuration.
File Types to Block in File Transfer	Restricts users from transferring specific file types. Set a file extension as the value, for example, `.exe`. Use a semicolon to delimit multiple values, for example, `.exe;.msi;.rar;.zip`

Desktop Client Settings Configuration	Description
Automatically Start in Phone Control	Sets the phone type for users when the client starts for the first time. Users can change their phone type after the initial start. The client then saves the user preference and uses it for subsequent starts. **Enabled** Use the desk phone device for calls. **Disabled (default)** Use the software phone (CSF) device for calls.
Jabber For Windows Software Update Server URL	Specifies the URL to the XML file that holds client update information. The client uses this URL to retrieve the XML file from your web server. In hybrid cloud-based deployments, you should use the Cisco WebEx Administration Tool to configure automatic updates.
Problem Report Server URL	Specifies the URL for the custom script that allows users to submit problem reports.

Set Parameters on Phone Configuration for Mobile Clients

The client can retrieve configuration settings in the phone configuration from the following locations on Cisco Unified Communications Manager:

- Cisco Dual Mode for iPhone (TCT) Configuration — Applies to individual TCT devices and takes priority over the group configuration.
- Cisco Jabber for Tablet (TAB) Configuration — Applies to individual TAB devices and takes priority over the group configuration.

Parameters in Phone Configuration

The following table lists the configuration parameters you can set in the **Product Specific Configuration Layout** section of the phone configuration and maps corresponding parameters from the client configuration file:

Parameter	Description
On-Demand VPN URL	URL for initiating on-demand VPN. **Note** Applicable for iOS only.
Preset Wi-fi Networks	Enter the SSIDs for Wi-Fi networks (SSIDs) approved by your organization. Separate SSIDs with a forward slash (/). Devices do not connect to secure connect if connected to one of the entered Wi-Fi networks.

Parameter	Description
Default Ringtone	Sets the default ringtone to **Normal** or **Loud**.
Video Capabilities	Enables or disables video capabilities. • Enabled (default) — Users can send and receive video calls. • Disabled — Users cannot send or receive video calls.
Dial via Office **Note** TCT and BOT devices only.	Enables or disables Dial via Office. • Enabled — Users can dial via office. • Disabled (default) — Users cannot dial via office.

Configure Proxy Setting

The client uses proxy settings to connect to services.

The following limitations apply when using a proxy for these HTTP requests:

- Proxy Authentication is not supported.
- Wildcards in the bypass list are supported.
- Cisco Jabber supports proxy for HTTP request using HTTP CONNECT, but does not support proxy when using HTTPS CONNECT.

Configure Proxy Settings for Cisco Jabber for Windows

Configure proxy settings for Windows in the Local Area Network (LAN) settings for Internet properties.

Procedure

Step 1 In the **Connections** tab select **LAN Settings**.

Step 2 Configure a proxy using one of the following options:

- For automatic configuration, specify a `.pac` file URL.
- For Proxy Server, specify an explicit proxy address.

Configure Proxy Settings for Cisco Jabber for Mac

Configure proxy settings for Mac in **System Preferences**.

Procedure

Step 1 Select **System Preferences** > **Network**

Step 2 Choose your network service from the list and select **Advanced** > **Proxies** .

Step 3 Configure a proxy using one of the following options:

- For automatic configuration, specify a `.pac` file URL.
- For Proxy Server, specify an explicit proxy address.

Configure Proxy Settings for Cisco Jabber iPhone and iPad

Configure proxy settings in the Wi-Fi settings of an iOS device using one of the following methods:

Procedure

Step 1 Select **Wi-Fi** > **HTTP PROXY** > **Auto** and specify a `.pac` file URL as the automatic configuration script.

Step 2 Select **Wi-Fi** > **HTTP PROXY** > **Manual** and specify an explicit proxy address.

Configure Proxy Settings for Cisco Jabber for Android

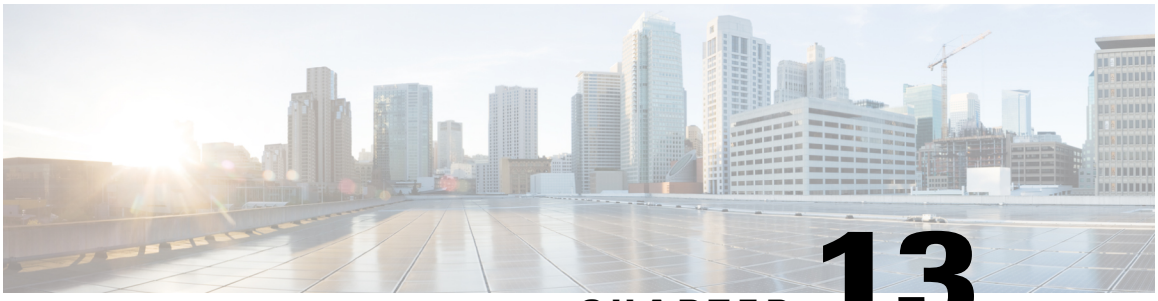
Procedure

Configure proxy settings in the Wi-Fi settings of an Android device using one of the following methods:

- Specify a .pac file URL as the automatic configuration script in the **Wi-Fi** > **Modify Network** > **Show Advanced Options** > **Proxy Settings** > **Auto** tab.

  Note This method is only supported on devices with Android OS 5.0 and later, and Cisco DX series devices.

- Specify an explicit proxy address in the **Wi-Fi Networks** > **Modify Network** > **Show Advanced Options** > **Proxy Settings** > **Auto** tab.



CHAPTER 13

Deploy Cisco Jabber Applications

- Download the Cisco Jabber Clients, page 55
- Install Cisco Jabber for Windows, page 55
- Install Cisco Jabber for Mac, page 81
- Install Cisco Jabber Mobile Clients, page 83

Download the Cisco Jabber Clients

If required, you can add your own Customer signature to the Jabber Installer or Cisco Dynamic Libraries by using the signing tools from the Operating System for that client.

Procedure

- Visit the Cisco Software Center to download the Cisco Jabber for Mac and Cisco Jabber for Windows clients.
- For Cisco Jabber for Android, download the app from Google Play.
- For Cisco Jabber for iPhone and iPad, download the app from the App store.

Install Cisco Jabber for Windows

Cisco Jabber for Windows provides an MSI installation package that you can use in the following ways:

Install Option	Description
Use the Command Line, on page 56	You can specify arguments in a command line window to set installation properties. Choose this option if you plan to install multiple instances.

Install Option	Description
Run the MSI Manually, on page 72	Run the MSI manually on the file system of the client workstation and then specify connection properties when you start the client. Choose this option if you plan to install a single instance for testing or evaluation purposes.
Create a Custom Installer, on page 73	Open the default installation package, specify the required installation properties, and then save a custom installation package. Choose this option if you plan to distribute an installation package with the same installation properties.
Deploy with Group Policy, on page 76	Install the client on multiple computers in the same domain.

Before You Begin

You must be logged in with local administrative rights.

Use the Command Line

Specify installation arguments in a command line window.

Procedure

Step 1 Open a command line window.

Step 2 Enter the following command:
```
msiexec.exe /i CiscoJabberSetup.msi
```

Step 3 Specify command line arguments as parameter=value pairs.
```
msiexec.exe /i CiscoJabberSetup.msi argument=value
```

Step 4 Run the command to install Cisco Jabber for Windows.

Cisco Jabber for Windows for Cloud Deployment

Ensure that the command line argument UPN_DISCOVERY_ENABLED is set to `false`.

Example Installation Commands

Review examples of commands to install Cisco Jabber for Windows.

Cisco Unified Communications Manager, Release 9.x

```
msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1
```

Where:

CLEAR=1 — Deletes any existing bootstrap file.
`/quiet` — Specifies a silent installation.

Cisco WebEx Messenger Service

```
msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1 AUTHENTICATOR=WEBEX
```

Where:

CLEAR=1 — Deletes any existing bootstrap file.
AUTHENTICATOR=WEBEX — Sets the Cisco WebEx Messenger service as the authenticator.
`/quiet` — Specifies a silent installation.

Cisco WebEx Messenger Service with SSO

```
msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1 AUTHENTICATOR=WEBEX
 SSO_ORG_DOMAIN=example.com
```

Where:

CLEAR=1 — Deletes any existing bootstrap file.
AUTHENTICATOR=WEBEX — Sets the Cisco WebEx Messenger service as the authenticator.
SSO_ORG_DOMAIN=example.com — Sets `example.com` as the single sign-on (SSO) domain.
`/quiet` — Specifies a silent installation.

Command Line Arguments

Review the command line arguments you can specify when you install Cisco Jabber for Windows.

Override Argument

The following table describes the parameter you must specify to override any existing bootstrap files from previous installations:

Argument	Value	Description
CLEAR	1	Specifies if the client overrides any existing bootstrap file from previous installations. The client saves the arguments and values you set during installation to a bootstrap file. The client then loads settings from the bootstrap file at startup.

If you specify CLEAR, the following occurs during installation:

1. The client deletes any existing bootstrap file.
2. The client creates a new bootstrap file.

If you do not specify CLEAR, the client checks for existing bootstrap files during installation.

- If no bootstrap file exists, the client creates a bootstrap file during installation.
- If a bootstrap file exists, the client does not override that bootstrap file and preserves the existing settings.

Note If you are reinstalling Cisco Jabber for Windows, you should consider the following:

- The client does not preserve settings from existing bootstrap files. If you specify CLEAR, you must also specify all other installation arguments as appropriate.
- The client does not save your installation arguments to an existing bootstrap file. If you want to change the values for installation arguments, or specify additional installation arguments, you must specify CLEAR to override the existing settings.

To override existing bootstrap files, specify CLEAR in the command line as follows:

```
msiexec.exe /i CiscoJabberSetup.msi CLEAR=1
```

Mode Type Argument

The following table describes the command line argument with which you specify the product mode:

Argument	Value	Description
PRODUCT_MODE	Phone_Mode	Specifies the product mode for the client. You can set the following value: • Phone_Mode — Cisco Unified Communications Manager is the authenticator. Choose this value to provision users with audio devices as base functionality.

When to Set the Product Mode

In phone mode deployments Cisco Unified Communications Manager is the authenticator. When the client gets the authenticator, it determines the product mode is phone mode. However, because the client always starts in the default product mode on the initial launch, users must restart the client to enter phone mode after sign in.

- Cisco Unified Communications Manager, Release 9.x and Later — You should not set PRODUCT_MODE during installation. The client gets the authenticator from the service profile. After the user signs in, the client requires a restart to enter phone mode.

Change Product Modes

To change the product mode, you must change the authenticator for the client. The client can then determine the product mode from the authenticator.

The method for changing from one product mode to another after installation, depends on your deployment.

Note In all deployments, the user can manually set the authenticator in the Advanced settings window.

In this case, you must instruct the user to change the authenticator in the Advanced settings window to change the product mode. You cannot override the manual settings, even if you uninstall and then reinstall the client.

Change Product Modes with Cisco Unified Communications Manager Version 9.x and Later

To change product modes with Cisco Unified Communications Manager version 9.x and later, you change the authenticator in the service profile.

Procedure

Step 1 Change the authenticator in the service profiles for the appropriate users.

Change Default Mode > Phone Mode

Do not provision users with an IM and Presence service.

If the service profile does not contain an IM and presence service configuration, the authenticator is Cisco Unified Communications Manager.

Change Phone Mode > Default Mode

Provision users with an IM and Presence service.

If you set the value of the **Product type** field in the IM and Presence profile to:

- **Unified CM (IM and Presence)** the authenticator is Cisco Unified Communications Manager IM and Presence Service.
- **WebEx (IM and Presence)** the authenticator is the Cisco WebEx Messenger service.

Step 2 Instruct users to sign out and then sign in again.

When users sign in to the client, it retrieves the changes in the service profile and signs the user in to the authenticator. The client then determines the product mode and prompts the user to restart the client.

After the user restarts the client, the product mode change is complete.

Authentication Arguments

The following table describe the command line arguments you can set to specify the source of authentication:

Argument	Value	Description
AUTHENTICATOR	CUP CUCM WEBEX	Specifies the source of authentication for the client. This value is used if Service Discovery fails. Set one of the following as the value: • CUP—Cisco Unified Communications Manager IM and Presence Service. On-premises deployments in the default product mode. The default product mode can be either full UC or IM only. • CUCM—Cisco Unified Communications Manager. On-premises deployments in phone mode. • WEBEX—Cisco WebEx Messenger Service. Cloud-based or hybrid cloud-based deployments. In on-premises deployments with Cisco Unified Communications Manager version 9.x and later, you should deploy the `_cisco-uds` SRV record. The client can then automatically determine the authenticator.
CUP_ADDRESS	IP address Hostname FQDN	Specifies the address of Cisco Unified Communications Manager IM and Presence Service. Set one of the following as the value: • Hostname (*hostname*) • IP address (*123.45.254.1*) • FQDN (*hostname.domain.com*)
TFTP	IP address Hostname FQDN	Specifies the address of your TFTP server. Set one of the following as the value: • Hostname (*hostname*) • IP address (*123.45.254.1*) • FQDN (*hostname.domain.com*) You should specify this argument if you set Cisco Unified Communications Manager as the authenticator. If you deploy: • In phone mode—you should specify the address of the TFTP server that hosts the client configuration. • In default mode—you can specify the address of the Cisco Unified Communications Manager TFTP service that hosts the device configuration.

Argument	Value	Description
CTI	IP address Hostname FQDN	Sets the address of your CTI server. Specify this argument if: • You set Cisco Unified Communications Manager as the authenticator. • Users have desk phone devices and require a CTI server.
CCMCIP	IP address Hostname FQDN	Sets the address of your CCMCIP server. Specify this argument if: • You set Cisco Unified Communications Manager as the authenticator. • The address of your CCMCIP server is not the same as the TFTP server address. The client can locate the CCMCIP server with the TFTP server address if both addresses are the same. Cisco Unified Communications Manager release 9.x and earlier—If you enable Cisco Extension Mobility, the `Cisco Extension Mobility` service must be activated on the Cisco Unified Communications Manager nodes that are used for CCMCIP. For information about Cisco Extension Mobility, see the *Feature and Services* guide for your Cisco Unified Communications Manager release.
SERVICES_DOMAIN	Domain	Sets the value of the domain where the DNS SRV records for Service Discovery reside. This argument can be set to a domain where no DNS SRV records reside if you want the client to use installer settings or manual configuration for this information. If this argument is not specified and Service Discovery fails, the user will be prompted for services domain information.

Argument	Value	Description
VOICE_SERVICES_DOMAIN	Domain	In Hybrid Deployments the domain required to discover Webex via CAS lookup may be a different domain than where the DNS records are deployed. If this is the case then set the SERVICES_DOMAIN to be the domain used for Webex discovery (or let the user enter an email address) and set the VOICE_SERVICES_DOMAIN to be the domain where DNS records are deployed. If this setting is specified, the client will use the value of VOICE_SERVICES_DOMAIN to lookup the following DNS records for the purposes of Service Discovery and Edge Detection: • `_cisco-uds` • `_cuplogin` • `_collab-edge` This setting is optional and if not specified, the DNS records are queried on the Services Domain which is obtained from the SERVICES_DOMAIN, email address input by the user, or cached user configuration.
EXCLUDED_SERVICES	One or more of: • WEBEX • CUCM	Lists the services that you want Jabber to exclude from Service Discovery. For example, you may have done a trial with WebEx which means that your company domain is registered on WebEx, but you do not want Jabber users to authenticate using WebEx. You want Jabber to authenticate with CUCM server. In this case set: • EXCLUDED_SERVICES=WEBEX Possible values are CUCM, WEBEX. If you exclude all services, you need to use manual configuration or bootstrap configuration to configure the Jabber client.

Argument	Value	Description
UPN_DISCOVERY_ENABLED	true false	Allows you to define whether the client uses the User Principal Name (UPN) of a Windows session to get the User ID and domain for a user when discovering services. • true (default)—The UPN is used to find the User ID and the domain of the user, which is used during service discovery. Only the user discovered from UPN can log in to the client. • false—The UPN is not used to find the User ID and domain of the user. The user is prompted to enter credentials to find the domain for service discovery. Example installation command: `msiexec.exe /i CiscoJabberSetup.msi /quiet UPN_DISCOVERY_ENABLED=false`

TFTP Server Address

Cisco Jabber for Windows retrieves two different configuration files from the TFTP server:

- Client configuration files that you create.
- Device configuration files that reside on the Cisco Unified Communications Manager TFTP service when you provision users with devices.

To minimize effort, you should host your client configuration files on the Cisco Unified Communications Manager TFTP service. You then have only one TFTP server address for all configuration files and can specify that address as required.

You can, however, host your client configuration on a different TFTP server to the one that contains the device configuration. In this case, you have two different TFTP server addresses, one address for the TFTP server that hosts device configuration and another address for the TFTP server that hosts client configuration files.

Default Deployments

This section describes how you should handle two different TFTP server addresses in deployments that have a presence server.

You should do the following:

1. Specify the address of the TFTP server that hosts the client configuration on the presence server.
2. During installation, specify the address of the Cisco Unified Communications Manager TFTP service with the TFTP argument.

When the client starts for the first time, it:

1. Retrieves the address of the Cisco Unified Communications Manager TFTP service from the bootstrap file.
2. Gets device configuration from the Cisco Unified Communications Manager TFTP service.

3 Connects to the presence server.

4 Retrieves the address of the TFTP service that hosts the client configuration from the presence server.

5 Gets client configuration from the TFTP server.

Phone Mode Deployments

This section describes how you should handle two different TFTP server addresses in phone mode deployments.

You should do the following:

1 During installation, specify the address of the TFTP server that hosts the client configuration with the TFTP argument.

2 Specify the address of the TFTP server that hosts the device configuration in your client configuration file with the following parameter: TftpServer1.

3 Host the client configuration file on the TFTP server.

When the client starts for the first time, it:

1 Retrieves the address of the TFTP server from the bootstrap file.

2 Gets client configuration from the TFTP server.

3 Retrieves the address of the Cisco Unified Communications Manager TFTP service from the client configuration.

4 Gets device configuration from the Cisco Unified Communications Manager TFTP service.

Common Installation Arguments

The following table describes command line arguments that are common to all deployments:

Argument	Value	Description
LANGUAGE	LCID in decimal	Defines the Locale ID (LCID), in decimal, of the language that Cisco Jabber for Windows uses. The value must be an LCID in decimal that corresponds to a supported language. For example, you can specify one of the following: • 1033 specifies English. • 1036 specifies French. See the *LCID for Languages* topic for a full list of the languages that you can specify. This argument is optional. If you do not specify a value, Cisco Jabber for Windows uses the regional language for the current user as the default. From Release 11.1(1) onwards, if you do not specify a value, Cisco Jabber for Windows checks the value for the UseSystemLanguage parameter. If the UseSystemLanguage parameter is set to true, the same language is used as for the operating system. If the UseSystemLanguage parameter is to set to false or not defined, then the client uses the regional language for the current user as the default. The regional language is set at **Control Panel** > **Region and Language** > **Change the date, time, or number format** > **Formats tab** > **Format dropdown**.
FORGOT_PASSWORD_URL	URL	Specifies the URL where users can reset lost or forgotten passwords. This argument is optional but recommended. **Note** In cloud-based deployments, you can specify a forgot password URL using the Cisco WebEx Administration Tool. However, the client cannot retrieve that forgot password URL until users sign in.

Argument	Value	Description
AUTOMATIC_SIGN_IN	true false	Applies to Release 11.1(1) onwards. Specifies whether the **Sign me in when Cisco Jabber starts** check box is checked when the user installs the client. • true—The **Sign me in when Cisco Jabber starts** check box is checked when the user installs the client. • false (default)—The **Sign me in when Cisco Jabber starts** check box is not checked when the user installs the client.
TFTP_FILE_NAME	Filename	Specifies the unique name of a group configuration file. You can specify either an unqualified or fully qualified filename as the value. The filename you specify as the value for this argument takes priority over any other configuration file on your TFTP server. This argument is optional. **Remember** You can specify group configuration files in the **Cisco Support Field** on the CSF device configuration on Cisco Unified Communications Manager.

Argument	Value	Description
LOGIN_RESOURCE	WBX MUT	Controls user sign in to multiple client instances. By default, users can sign in to multiple instances of Cisco Jabber at the same time. Set one of the following values to change the default behavior: • WBX—Users can sign in to one instance of Cisco Jabber for Windows at a time. Cisco Jabber for Windows appends the `wbxconnect` suffix to the user's JID. Users cannot sign in to any other Cisco Jabber client that uses the `wbxconnect` suffix. • MUT—Users can sign in to one instance of Cisco Jabber for Windows at a time, but can sign in to other Cisco Jabber clients at the same time. Each instance of Cisco Jabber for Windows appends the user's JID with a unique suffix.
LOG_DIRECTORY	Absolute path on the local filesystem	Defines the directory where the client writes log files. Use quotation marks to escape space characters in the path, as in the following example: `"C:\my_directory\Log Directory"` The path you specify must not contain Windows invalid characters. The default value is `%USER_PROFILE%\AppData\Local\Cisco\Unified Communications\Jabber\CSF\Logs`
CLICK2X	DISABLE	Disables click-to-x functionality with Cisco Jabber. If you specify this argument during installation, the client does not register as a handler for click-to-x functionality with the operating system. This argument prevents the client from writing to the Microsoft Windows registry during installation. You must re-install the client and omit this argument to enable click-to-x functionality with the client after installation.

Argument	Value	Description
ENABLE_PRT	true false	• true (default)—The **Report a problem** menu item is enabled in the **Help** menu in the client. • false—The Jabber menu item option **Report a problem** is removed from the **Help** menu in the client. If you set the argument to false, users can still manually use the **Start Menu** > **Cisco Jabber** directory, or the Program files directory and launch the Problem Report Tool manually. If a user manually creates a PRT, and this parameter value is set to false, then the zip file created from the PRT has no content.
ENABLE_PRT_ENCRYPTION	true false	Enables problem report encryption. You must configure this argument with the PRT_CERTIFICATE_NAME argument. • true—PRT files sent by Jabber clients are encrypted. • false (default)—PRT files sent by Jabber clients are not encrypted. PRT encryption requires a public/private key pair to encrypt and decrypt the Cisco Jabber problem report.
PRT_CERTIFICATE_NAME	Certificate name	Specifies the name of a certificate with a public key in the Enterprise Trust or Trusted Root Certificate Authorities certificate store. The certificate public key is used to encrypt Jabber Problem reports. You must configure this argument with the ENABLE_PRT_ENCRYPTION argument.

Argument	Value	Description
INVALID_CERTIFICATE_BEHAVIOR	RejectAndNotify PromptPerSession	Specifies the client behavior for invalid certificates. • RejectAndNotify—A warning dialog displays and the client doesn't load. • PromptPerSession—A warning dialog displays and the user can accept or reject the invalid certificate. For invalid certificates in FIPS mode, this argument is ignored, the client displays a warning message and doesn't load.
Telemetry_Enabled	true false	Specifies whether analytics data is gathered. The default value is true. To improve your experience and product performance, Cisco Jabber may collect and send non-personally identifiable usage and performance data to Cisco. The aggregated data is used by Cisco to understand trends in how Jabber clients are being used and how they are performing. Full details on what analytics data Cisco Jabber does and does not collect can be found in the Cisco Jabber Supplement to Cisco's On-Line Privacy Policy at http://www.cisco.com/web/siteassets/legal/privacy_02Jun10.html.
LOCATION_MODE	ENABLED DISABLED ENABLEDNOPROMPT	Specifies whether the Location feature is enabled and whether users are notified when new locations are detected. • ENABLED(default)—Location feature is turned on. Users are notified when new locations are detected. • DISABLED—Location feature is turned off. Users are not notified when new locations are detected. • ENABLEDNOPROMPT—Location feature is turned on. Users are not notified when new locations are detected.

Argument	Value	Description
FIPS_MODE	true false	Specifies whether the Cisco Jabber is in FIPS mode. Cisco Jabber can be in FIPS mode on an operating system that is not FIPS enabled. Only connections with non-Window's APIs are in FIPS mode. If you don't include this setting, Cisco Jabber will determine the FIPS mode from the operating system.
ENABLE_DPI_AWARE	true false	Enables DPI awareness. DPI awareness enables Cisco Jabber to automatically adjust the display of text and images to suit different screen sizes. • true (default)—DPI awareness is enabled. • false—DPI awareness is not enabled. DPI awareness is enabled by default. To disable DPI awareness, use the following command: `msiexec.exe /i CiscoJabberSetup.msi CLEAR=1 ENABLE_DPI_AWARE=false`

SSO Arguments

This section describes the command line arguments you can use to deploy Cisco Jabber for Windows with single sign on (SSO) capabilities.

Cloud-Based SSO Arguments

The arguments in the following table apply to cloud-based deployments only:

Argument	Value	Description
SSO_ORG_DOMAIN	Domain name	Specifies the domain name for the Cisco WebEx Org that contains the URL for the SSO service. Cisco Jabber for Windows uses this argument to retrieve the URL of the SSO service from the Org. When Cisco Jabber for Windows gets the SSO service URL, it can request login tokens to authenticate with Cisco WebEx Messenger. **Note** You specify the URL for the SSO service as the value of the Customer SSO Service Login URL in the Cisco WebEx Administration Tool.

LCID for Languages

The following table lists the Locale Identifier (LCID) or Language Identifier (LangID) for the languages that the Cisco Jabber clients support.

Supported Languages	Cisco Jabber for Windows	Cisco Jabber for Mac	Cisco Jabber for Android, Cisco Jabber for iPhone and iPad	LCID/LangID
Arabic - Saudi Arabia	X		X	1025
Bulgarian - Bulgaria	X	X		1026
Catalan - Spain	X	X		1027
Chinese (Simplified) - China	X	X	X	2052
Chinese (Traditional) - Taiwan	X	X	X	1028
Croatian - Croatia	X	X		1050
Czech - Czech Republic	X	X		1029
Danish - Denmark	X	X	X	1030
Dutch - Netherlands	X	X	X	1043
English - United States	X	X	X	1033
Finnish - Finland	X	X		1035
French - France	X	X	X	1036
German - Germany	X	X	X	1031
Greek - Greece	X	X		1032
Hebrew - Israel	X			1037
Hungarian - Hungary	X	X		1038
Italian - Italy	X	X	X	1040

Supported Languages	Cisco Jabber for Windows	Cisco Jabber for Mac	Cisco Jabber for Android, Cisco Jabber for iPhone and iPad	LCID/LangID
Japanese - Japan	X	X	X	1041
Korean - Korea	X	X	X	1042
Norwegian - Norway	X	X		2068
Polish - Poland	X	X		1045
Portuguese - Brazil	X	X	X	1046
Portuguese - Portugal	X	X		2070
Romanian - Romania	X	X		1048
Russian - Russia	X	X	X	1049
Serbian	X	X		1050
Slovak - Slovakian	X	X		1051
Slovenian -Slovenia	X	X		1060
Spanish - Spain (Modern Sort)	X	X	X	3082
Swedish - Sweden	X	X	X	5149
Thai - Thailand	X	X		1054
Turkish	X	X		1055

Run the MSI Manually

You can run the installation program manually to install a single instance of the client and specify connection settings in the Advanced settings window.

Procedure

Step 1 Launch `CiscoJabberSetup.msi`.

The installation program opens a window to guide you through the installation process.

Step 2 Follow the steps to complete the installation process.

Step 3 Start Cisco Jabber for Windows.

Step 4 Select **Manual setup and sign in**.
The Advanced settings window opens.

Step 5 Specify values for the connection settings properties.

Step 6 Select **Save**.

Create a Custom Installer

You can transform the default installation package to create a custom installer.

Note You use Microsoft Orca to create custom installers. Microsoft Orca is available as part of the Microsoft Windows SDK for Windows 7 and .NET Framework 4.

Download and install Microsoft Windows SDK for Windows 7 and .NET Framework 4 from the Microsoft website.

Procedure

	Command or Action	Purpose
Step 1	Get the Default Transform File, on page 73	You must have the default transform file to modify the installation package with Microsoft Orca.
Step 2	Create Custom Transform Files, on page 74	Transform files contain installation properties that you apply to the installer.
Step 3	Transform the Installer, on page 74	Apply a transform file to customize the installer.

Get the Default Transform File

You must have the default transform file to modify the installation package with Microsoft Orca.

Procedure

Step 1 Download the Cisco Jabber administration package from Software Download page.

Step 2 Copy `CiscoJabberProperties.msi` from the Cisco Jabber administration package to your file system.

What to Do Next

Create Custom Transform Files, on page 74

Create Custom Transform Files

To create a custom installer, you use a transform file. Transform files contain installation properties that you apply to the installer.

The default transform file lets you specify values for properties when you transform the installer. You should use the default transform file if you are creating one custom installer.

You can optionally create custom transform files. You specify values for properties in a custom transform file and then apply it to the installer.

Create custom transform files if you require more than one custom installer with different property values. For example, create one transform file that sets the default language to French and another transform file that sets the default language to Spanish. You can then apply each transform file to the installation package separately. The result is that you create two installers, one for each language.

Before You Begin

Get the Default Transform File, on page 73

Procedure

Step 1 Start Microsoft Orca.

Step 2 Open `CiscoJabberSetup.msi` and then apply `CiscoJabberProperties.msi`.

Step 3 Specify values for the appropriate installer properties.

Step 4 Generate and save the transform file.

a) Select **Transform** > **Generate Transform**.

b) Select a location on your file system to save the transform file.

c) Specify a name for the transform file and select **Save**.

The transform file you created is saved as *`file_name`*`.mst`. You can apply this transform file to modify the properties of `CiscoJabberSetup.msi`.

What to Do Next

Transform the Installer, on page 74

Transform the Installer

Apply a transform file to customize the installer.

Note Applying transform files will alter the digital signature of `CiscoJabberSetup.msi`. Attempts to modify or rename `CiscoJabberSetup.msi` will remove the signature entirely.

Before You Begin

Create Custom Transform Files, on page 74

Procedure

Step 1 Start Microsoft Orca.

Step 2 Open `CiscoJabberSetup.msi` in Microsoft Orca.

a) Select **File** > **Open**.
b) Browse to the location of `CiscoJabberSetup.msi` on your file system.
c) Select `CiscoJabberSetup.msi` and then select **Open**.

The installation package opens in Microsoft Orca. The list of tables for the installer opens in the **Tables** pane.

Step 3 Remove all language codes except for 1033 (English).

Restriction You must remove all language codes from the custom installer except for 1033 (English).

Microsoft Orca does not retain any language files in custom installers except for the default, which is 1033. If you do not remove all language codes from the custom installer, you cannot run the installer on any operating system where the language is other than English.

a) Select **View** > **Summary Information**.
The **Edit Summary Information** window displays.
b) Locate the **Languages** field.
c) Delete all language codes except for 1033.
d) Select **OK**.

English is set as the language for your custom installer.

Step 4 Apply a transform file.

a) Select **Transform** > **Apply Transform**.
b) Browse to the location of the transform file on your file system.
c) Select the transform file and then select **Open**.

Step 5 Select **Property** from the list of tables in the **Tables** pane.
The list of properties for `CiscoJabberSetup.msi` opens in the right panel of the application window.

Step 6 Specify values for the properties you require.

Tip Values are case sensitive. Ensure the value you enter matches the value in this document.

Tip Set the value of the CLEAR property to `1` to override any existing bootstrap file from previous installations. If you do not override existing bootstrap files, the values you set in the custom installer do not take effect.

Step 7 Remove any properties that you do not require.
It is essential to remove any properties that are not being set, otherwise the properties being set will not take effect. Remove each property that is not needed one at a time.

a) Right-click the property you want to remove.
b) Select **Drop Row**.
c) Select **OK** when Microsoft Orca prompts you to continue.

Step 8 Enable your custom installer to save embedded streams.

a) Select **Tools** > **Options**.

b) Select the **Database** tab.
c) Select **Copy embedded streams during 'Save As'**.
d) Select **Apply** and then **OK**.

Step 9 Save your custom installer.

a) Select **File** > **Save Transformed As**.
b) Select a location on your file system to save the installer.
c) Specify a name for the installer and then select **Save**.

Installer Properties

The following are the properties you can modify in a custom installer:

- CLEAR
- PRODUCT_MODE
- AUTHENTICATOR
- CUP_ADDRESS
- TFTP
- CTI
- CCMCIP
- LANGUAGE
- TFTP_FILE_NAME
- FORGOT_PASSWORD_URL
- SSO_ORG_DOMAIN
- LOGIN_RESOURCE
- LOG_DIRECTORY
- CLICK2X
- SERVICES_DOMAIN

These properties correspond to the installation arguments and have the same values.

Deploy with Group Policy

Install Cisco Jabber for Windows with Group Policy using the Microsoft Group Policy Management Console (GPMC) on Microsoft Windows Server.

Note To install Cisco Jabber for Windows with Group Policy, all computers or users to which you plan to deploy Cisco Jabber for Windows must be in the same domain.

Procedure

	Command or Action	Purpose
Step 1	Set a Language Code, on page 77	You must use this procedure and set the Language field to 1033 only if the MSI is to be modified by Orca in any way.
Step 2	Deploy the Client with Group Policy, on page 78	Deploy Cisco Jabber for Windows with Group Policy.

Set a Language Code

Altering the installation language is not necessary in Group Policy deployment scenarios where the exact MSI file provided by Cisco will be used. The installation language will be determined from the Windows User Locale (Format) in these situations. You must use this procedure and set the Language field to 1033 only if the MSI is to be modified by Orca in any way.

Procedure

Step 1 Start Microsoft Orca.
Microsoft Orca is available as part of the Microsoft Windows SDK for Windows 7 and ,NET Framework 4 that you can download from the Microsoft website.

Step 2 Open `CiscoJabberSetup.msi`.
a) Select **File** > **Open**.
b) Browse to the location of `CiscoJabberSetup.msi` on your file system.
c) Select `CiscoJabberSetup.msi` and then select **Open**.

Step 3 Select **View** > **Summary Information**.

Step 4 Locate the **Languages** field.

Step 5 Set the **Languages** field to 1033.

Step 6 Select **OK**.

Step 7 Enable your custom installer to save embedded streams.
a) Select **Tools** > **Options**.
b) Select the **Database** tab.
c) Select **Copy embedded streams during 'Save As'**.
d) Select **Apply** and then **OK**.

Step 8 Save your custom installer.
a) Select **File** > **Save Transformed As**.

b) Select a location on your file system to save the installer.
c) Specify a name for the installer and then select **Save**.

What to Do Next

Deploy the Client with Group Policy, on page 78

Deploy the Client with Group Policy

Complete the steps in this task to deploy Cisco Jabber for Windows with Group Policy.

Before You Begin

Set a Language Code, on page 77

Procedure

Step 1 Copy the installation package to a software distribution point for deployment.
All computers or users to which you plan to deploy Cisco Jabber for Windows must be able to access the installation package on the distribution point.

Step 2 Select **Start** > **Run** and then enter the following command:
`GPMC.msc`

The **Group Policy Management** console opens.

Step 3 Create a new group policy object.

a) Right-click on the appropriate domain in the left pane.
b) Select **Create a GPO in this Domain, and Link it here**.
The **New GPO** window opens.
c) Enter a name for the group policy object in the **Name** field.
d) Leave the default value or select an appropriate option from the **Source Starter GPO** drop-down list and then select **OK**.
The new group policy displays in the list of group policies for the domain.

Step 4 Set the scope of your deployment.

a) Select the group policy object under the domain in the left pane.
The group policy object displays in the right pane.
b) Select **Add** in the **Security Filtering** section of the **Scope** tab.
The **Select User, Computer, or Group** window opens.
c) Specify the computers and users to which you want to deploy Cisco Jabber for Windows.

Step 5 Specify the installation package.

a) Right-click the group policy object in the left pane and then select **Edit**.
The **Group Policy Management Editor** opens.
b) Select **Computer Configuration** and then select **Policies** > **Software Settings**.
c) Right-click **Software Installation** and then select **New** > **Package**.

d) Enter the location of the installation package next to **File Name**; for example, `\\server\software_distribution`.

Important You must enter a Uniform Naming Convention (UNC) path as the location of the installation package. If you do not enter a UNC path, Group Policy cannot deploy Cisco Jabber for Windows.

e) Select the installation package and then select **Open**.

f) In the **Deploy Software** dialog box, select **Assigned** and then **OK**.

Group Policy installs Cisco Jabber for Windows on each computer the next time each computer starts.

Cisco Media Services Interface

Cisco Jabber for Windows supports Cisco Media Services Interface version 4.1.2 for Microsoft Windows 7 and later.

Cisco Jabber for Mac supports Cisco Media Services Interface version 4.0.2 or later.

Desk Phone Video Capabilities

You must install Cisco Media Services Interface to enable desk phone video capabilities. Cisco Media Services Interface provides a driver that enables Cisco Jabber for Windows to do the following:

- Discover the desk phone device.
- Establish and maintain a connection to the desk phone device using the CAST protocol.

Install Cisco Media Services Interface

Procedure

Step 1 Download the Cisco Media Services Interface installation program from the download site on cisco.com.

Step 2 Install Cisco Media Services Interface on each computer on which you install Cisco Jabber.
See the appropriate Cisco Medianet documentation for installing Cisco Media Services Interface.

Uninstall Cisco Jabber for Windows

You can uninstall Cisco Jabber for Windows using either the command line or the Microsoft Windows control panel. This document describes how to uninstall Cisco Jabber for Windows using the command line.

Use the Installer

If the installer is available on the file system, use it to remove Cisco Jabber for Windows.

Procedure

Step 1 Open a command line window.

Step 2 Enter the following command:
`msiexec.exe /x path_to_CiscoJabberSetup.msi`

For example,
`msiexec.exe /x C:\Windows\Installer\CiscoJabberSetup.msi /quiet`
Where `/quiet` specifies a silent uninstall.

The command removes Cisco Jabber for Windows from the computer.

Use the Product Code

If the installer is not available on the file system, use the product code to remove Cisco Jabber for Windows.

Procedure

Step 1 Find the product code.

a) Open the Microsoft Windows registry editor.
b) Locate the following registry key: `HKEY_CLASSES_ROOT\Installer\Products`
c) Select **Edit** > **Find**.
d) Enter Cisco Jabber in the **Find what** text box in the **Find** window and select **Find Next**.
e) Find the value of the **ProductIcon** key.
The product code is the value of the **ProductIcon** key, for example, `C:\Windows\Installer\{product_code}\ARPPRODUCTICON.exe`.

Note The product code changes with each version of Cisco Jabber for Windows.

Step 2 Open a command line window.

Step 3 Enter the following command:
`msiexec.exe /x product_code`

For example,
`msiexec.exe /x 45992224-D2DE-49BB-B085-6524845321C7 /quiet`
Where `/quiet` specifies a silent uninstall.

The command removes Cisco Jabber for Windows from the computer.

Install Cisco Jabber for Mac

URL Configuration for Cisco Jabber for Mac

To enable users to launch Cisco Jabber without having to manually enter service discovery information, create and distribute a configuration URL to users.

You can provide a configuration URL link to users by emailing the link to the user directly, or by posting the link to a website.

You can include and specify the following parameters in the URL:

- ServicesDomain—Required. Every configuration URL must include the domain of the IM and presence server that Cisco Jabber needs for service discovery.
- VoiceServiceDomain—Required only if you deploy a hybrid cloud-based architecture where the domain of the IM and presence server differs from the domain of the voice server. Set this parameter to ensure that Cisco Jabber can discover voice services.
- ServiceDiscoveryExcludedServices—Optional. You can exclude any of the following services from the service discovery process:
    - WEBEX—When you set this value, the client:
        - Does not perform CAS lookup
        - Looks for:
            - `_cisco-uds`
            - `_cuplogin`
            - `_collab-edge`
    - CUCM—When you set this value, the client:
        - Does not look for `_cisco-uds`
        - Looks for:
            - `_cuplogin`
            - `_collab-edge`
    - CUP—When you set this value, the client:
        - Does not look for `_cuplogin`
        - Looks for:
            - `_cisco-uds`
            - `_collab-edge`

You can specify multiple, comma-separated values to exclude multiple services.

If you exclude all three services, the client does not perform service discovery and prompts the user to manually enter connection settings.

- ServicesDomainSsoEmailPrompt—Optional. Specifies whether the user is shown the email prompt for the purposes of determining their home cluster.
  - ON
  - OFF
- EnablePRTEncryption—Optional. Specifies that the PRT file is encrypted. Applies to Cisco Jabber for Mac.
  - true
  - false
- PRTCertificateName—Optional. Specifies the name of the certificate. Applies to Cisco Jabber for Mac.
- InvalidCertificateBehavior—Optional. Specifies the client behavior for invalid certificates.
  - RejectAndNotify—A warning dialog displays and the client doesn't load.
  - PromptPerSession—A warning dialog displays and the user can accept or reject the invalid certificate.
- Telephony_Enabled—Specifies whether the user has phone capability or not. The default is true.
  - True
  - False

Create the configuration URL in the following format:

```
ciscojabber://provision?ServicesDomain=<domain_for_service_discover>
&VoiceServicesDomain=<domain_for_voice_services>
&ServiceDiscoveryExcludedServices=<services_to_exclude_from_service_discover>
&ServicesDomainSsoEmailPrompt=<ON/OFF>
```

Note The parameters are case sensitive. When you create the configuration URL, you must use the following capitlization:

- `ServicesDomain`
- `VoiceServicesDomain`
- `ServiceDiscoveryExcludedServices`
- `ServicesDomainSsoEmailPrompt`
- `EnablePRTEncryption`
- `PRTCertificateName`
- `InvalidCertificateBehavior`
- `Telephony_Enabled`

Examples

- `ciscojabber://provision?ServicesDomain=cisco.com`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com`
- `ciscojabber://provision?ServicesDomain=service_domain &VoiceServicesDomain=voiceservice_domain&ServiceDiscoveryExcludedServices=WEBEX`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP &ServicesDomainSsoEmailPrompt=OFF`

Install Cisco Jabber Mobile Clients

Procedure

Step 1 To install Cisco Jabber for Android, download the app from Google Play from your mobile device.

Step 2 To install Cisco Jabber for iPhone and iPad, download the app from the App Store from your mobile device.

URL Configuration for Cisco Jabber for Android, iPhone, and iPad

To enable users to launch Cisco Jabber without having to manually enter service discovery information, create and distribute a configuration URL to users.

You can provide a configuration URL link to users by emailing the link to the user directly, or by posting the link to a website.

You can include and specify the following parameters in the URL:

- ServicesDomain—Required. Every configuration URL must include the domain of the IM and presence server that Cisco Jabber needs for service discovery.
- VoiceServiceDomain—Required only if you deploy a hybrid cloud-based architecture where the domain of the IM and presence server differs from the domain of the voice server. Set this parameter to ensure that Cisco Jabber can discover voice services.
- ServiceDiscoveryExcludedServices—Optional. You can exclude any of the following services from the service discovery process:
  - WEBEX—When you set this value, the client:
    - Does not perform CAS lookup
    - Looks for:
      - `_cisco-uds`
      - `_cuplogin`
      - `_collab-edge`
  - CUCM—When you set this value, the client:
    - Does not look for `_cisco-uds`
    - Looks for:
      - `_cuplogin`
      - `_collab-edge`
  - CUP—When you set this value, the client:
    - Does not look for `_cuplogin`
    - Looks for:
      - `_cisco-uds`
      - `_collab-edge`

  You can specify multiple, comma-separated values to exclude multiple services.

  If you exclude all three services, the client does not perform service discovery and prompts the user to manually enter connection settings.
- ServicesDomainSsoEmailPrompt—Optional. Specifies whether the user is shown the email prompt for the purposes of determining their home cluster.
  - ON
  - OFF
- InvalidCertificateBehavior—Optional. Specifies the client behavior for invalid certificates.

- RejectAndNotify—A warning dialog displays and the client doesn't load.
- PromptPerSession—A warning dialog displays and the user can accept or reject the invalid certificate.

- PRTCertificateUrl—Specifies the name of a certificate with a public key in the trusted root certificate store. Applies to Cisco Jabber mobile clients.
- Telephony_Enabled—Specifies whether the user has phone capability or not. The default is true.
  - True
  - False
- ForceLaunchBrowser—Used to force user to use the external browser. Applies to Cisco Jabber mobile clients.
  - True
  - False

Note ForceLaunchBrowser is used for client certificate deployments and for devices with Android OS below 5.0.

Create the configuration URL in the following format:

```
ciscojabber://provision?ServicesDomain=<domain_for_service_discover>
&VoiceServicesDomain=<domain_for_voice_services>
&ServiceDiscoveryExcludedServices=<services_to_exclude_from_service_discover>
&ServicesDomainSsoEmailPrompt=<ON/OFF>
```

Note The parameters are case sensitive. When you create the configuration URL, use the following capitalization:

- `ServicesDomain`
- `VoiceServicesDomain`
- `ServiceDiscoveryExcludedServices`
- `ServicesDomainSsoEmailPrompt`
- `PRTCertificateURL`
- `InvalidCertificateBehavior`
- `Telephony_Enabled`
- `ForceLaunchBrowser`

Examples

- `ciscojabber://provision?ServicesDomain=cisco.com`

- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com`
- `ciscojabber://provision?ServicesDomain=service_domain &VoiceServicesDomain=voiceservice_domain&ServiceDiscoveryExcludedServices=WEBEX`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP &ServicesDomainSsoEmailPrompt=OFF`

Mobile Configuration Using Enterprise Mobility Management

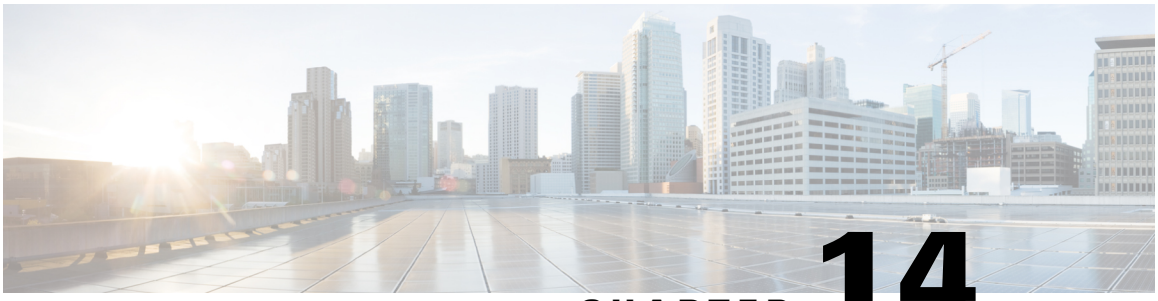
Before using Enterprise Mobility Management (EMM), ensure:

- The EMM vendor supports Android for Work or Apple Managed App Configuration.
- Android devices OS is 5.0 or later

To allow users to launch Cisco Jabber for Android or Cisco Jabber for iPhone and iPad, you can configure Cisco Jabber using Enterprise Mobility Management (EMM).

For more information on setting up EMM, refer to the instructions for administrators provided by the EMM provider.

If you want Jabber to run only on managed devices, then you can deploy certificate-based authentication, and enroll the client certificate through EMM.



CHAPTER 14

Remote Access

- Service Discovery Requirements Workflow, page 87
- Cisco Anyconnect Deployment Workflow, page 89

Service Discovery Requirements Workflow

Procedure

	Command or Action	Purpose
Step 1	Service Discovery Requirements, on page 41	
Step 2	DNS Requirements, on page 41	
Step 3	Certificate Requirements, on page 41	
Step 4	Test _collab-edge SRV Record, on page 88	

Service Discovery Requirements

Service discovery enables clients to automatically detect and locate services on your enterprise network. Expressway for Mobile and Remote Access allows you to access the services on your enterprise network. You should meet the following requirements to enable the clients to connect through Expressway for Mobile and Remote Access and discover services:

- DNS requirements
- Certificate requirements
- Test external SRV `_collab-edge`.

DNS Requirements

The DNS requirements for service discovery through remote access are:

- Configure a `_collab-edge` DNS SRV record on an external DNS server.
- Configure a `_cisco-uds` DNS SRV record on the internal name server.
- Optionally, if you deploy a hybrid cloud-based architecture where the domain of the IM and presence server differs from the domain of the voice server, ensure that you configure the Voice Services Domain to locate the DNS server that contains the `_collab-edge` record.

Certificate Requirements

Before you configure remote access, download the Cisco VCS Expressway and Cisco Expressway-E Server certificate. The Server certificate is used for both HTTP and XMPP.

For more information on configuring Cisco VCS Expressway certificate, see Configuring Certificates on Cisco VCS Expressway.

Test _collab-edge SRV Record

Test SRV Records

After creating your SRV records test to see if they are accessible.

Procedure

Step 1 Open a command prompt.

Step 2 Enter **nslookup**.
The default DNS server and address is displayed. Confirm that this is the expected DNS server.

Step 3 Enter **set type=SRV**.

Step 4 Enter the name for each of your SRV records.
For example `_cisco-uds.`*`exampledomain`*

- Displays server and address—SRV record is accessible.
- Displays `_cisco-uds.`*`exampledomain`*`: Non-existent domain`—There is an issue with your SRV record.

Cisco Anyconnect Deployment Workflow

Procedure

	Command or Action	Purpose
Step 1	Application Profiles, on page 89	
Step 2	Automate VPN Connection, on page 90	
Step 3	AnyConnect Documentation Reference, on page 93	
Step 4	Session Parameters, on page 93	

Cisco AnyConnect Deployment

Application Profiles

After you download the Cisco AnyConnect Secure Mobility Client to their device, the ASA must provision a configuration profile to the application.

The configuration profile for the Cisco AnyConnect Secure Mobility Client includes VPN policy information such as the company ASA VPN gateways, the connection protocol (IPSec or SSL), and on-demand policies.

You can provision application profiles for Cisco Jabber for iPhone and iPad in one of the following ways:

ASDM

We recommend that you use the profile editor on the ASA Device Manager (ASDM) to define the VPN profile for the Cisco AnyConnect Secure Mobility Client.

When you use this method, the VPN profile is automatically downloaded to the Cisco AnyConnect Secure Mobility Client after the client establishes the VPN connection for the first time. You can use this method for all devices and OS types, and you can manage the VPN profile centrally on the ASA.

For more information, see the *Creating and Editing an AnyConnect Profile* topic of the *Cisco AnyConnect Secure Mobility Client Administrator Guide* for your release.

iPCU

You can provision iOS devices using an Apple configuration profile that you create with the iPhone Configuration Utility (iPCU). Apple configuration profiles are XML files that contain information such as device security policies, VPN configuration information, and Wi-Fi, mail, and calendar settings.

The high-level procedure is as follows:

1. Use iPCU to create an Apple configuration profile.

   For more information, see the iPCU documentation.

2. Export the XML profile as a .mobileconfig file.

3 Email the .mobileconfig file to users.

After a user opens the file, it installs the AnyConnect VPN profile and the other profile settings to the client application.

MDM

You can provision iOS devices using an Apple configuration profile that you create with third-party Mobile Device Management (MDM) software. Apple configuration profiles are XML files that contain information such as device security policies, VPN configuration information, and Wi-Fi, mail, and calendar settings.

The high-level procedure is as follows:

1 Use MDM to create the Apple configuration profiles.

For information on using MDM, see the Apple documentation.

2 Push the Apple configuration profiles to the registered devices.

To provision application profiles for Cisco Jabber for Android, use the profile editor on the ASA Device Manager (ASDM) to define the VPN profile for the Cisco AnyConnect Secure Mobility Client. The VPN profile is automatically downloaded to the Cisco AnyConnect Secure Mobility Client after the client establishes the VPN connection for the first time. You can use this method for all devices and OS types, and you can manage the VPN profile centrally on the ASA. For more information, see the *Creating and Editing an AnyConnect Profile* topic of the *Cisco AnyConnect Secure Mobility Client Administrator Guide* for your release.

Automate VPN Connection

When users open Cisco Jabber from outside the corporate Wi-Fi network, Cisco Jabber needs a VPN connection to access the Cisco UC application servers. You can set up the system to allow Cisco AnyConnect Secure Mobility Client to automatically establish a VPN connection in the background, which helps ensure a seamless user experience.

Note VPN will not be launched because Expressway for Mobile and Remote Access has the higher connection priority even if VPN is set to automatic connection.

Set Up Trusted Network Connection

The Trusted Network Detection feature enhances the user experience by automating the VPN connection based on the user's location. When the user is inside the corporate Wi-Fi network, Cisco Jabber can reach the Cisco UC infrastructure directly. When the user leaves the corporate Wi-Fi network, Cisco Jabber automatically detects that it is outside the trusted network. After this occurs, Cisco AnyConnect Secure Mobility Client initiates the VPN to ensure connectivity to the UC infrastructure.

Note The Trusted Network Detection feature works with both certificate- and password-based authentication. However, certificate-based authentication provides the most seamless user experience.

Procedure

Step 1 Using ASDM, open the Cisco AnyConnect client profile.

Step 2 Enter the list of Trusted DNS Servers and Trusted DNS Domain Suffixes that an interface can receive when the client is within a corporate Wi-Fi network. The Cisco AnyConnect client compares the current interface DNS servers and domain suffix with the settings in this profile.

Note You must specify all your DNS servers to ensure that the Trusted Network Detection feature works properly. If you set up both the TrustedDNSDomains and TrustedDNSServers, sessions must match both settings to be defined as a trusted network.

For detailed steps for setting up Trusted Network Detection, see the *Trusted Network Detection* section in the *Configuring AnyConnect Features* chapter (Release 2.5) or *Configuring VPN Access* (releases 3.0 or 3.1) of the *Cisco AnyConnect Secure Mobility Client Administrator Guide* for your release.

Set Up Connect On-Demand VPN

The Apple iOS Connect On Demand feature enhances the user experience by automating the VPN connection based on the user's domain.

When the user is inside the corporate Wi-Fi network, Cisco Jabber can reach the Cisco UC infrastructure directly. When the user leaves the corporate Wi-Fi network, Cisco AnyConnect automatically detects if it is connected to a domain that you specify in the AnyConnect client profile. If so, the application initiates the VPN to ensure connectivity to the UC infrastructure. All applications on the device including Cisco Jabber can take advantage of this feature.

Note Connect On Demand supports only certificate-authenticated connections.

The following options are available with this feature:

- **Always Connect —** Apple iOS always attempts to initiate a VPN connection for domains in this list.
- **Connect If Needed —** Apple iOS attempts to initiate a VPN connection to the domains in the list only if it cannot resolve the address using DNS.
- **Never Connect —** Apple iOS never attempts to initiate a VPN connection to domains in this list.

Attention Apple plans to remove the Always Connect option in the near future. After the Always Connect option is removed, users can select the Connect If Needed option. In some cases, Cisco Jabber users may have issues when using the Connect If Needed option. For example, if the hostname for the Cisco Unified Communications Manager is resolvable outside the corporate network, iOS will not trigger a VPN connection. The user can work around this issue by manually launching Cisco AnyConnect Secure Mobility Client before making a call.

Procedure

Step 1 Use the ASDM profile editor, iPCU, or MDM software to open the AnyConnect client profile.

Step 2 In the AnyConnect client profile, under the Connect if Needed section, enter your list of on-demand domains. The domain list can include wild-card options (for example, cucm.cisco.com, cisco.com, and *.webex.com).

Set Up Automatic VPN Access on Cisco Unified Communications Manager

Before You Begin

- The mobile device must be set up for on-demand access to VPN with certificate-based authentication. For assistance with setting up VPN access, contact the providers of your VPN client and head end.
- For requirements for Cisco AnyConnect Secure Mobility Client and Cisco Adaptive Security Appliance, see the *Software Requirements* topic.
- For information about setting up Cisco AnyConnect, see the *Cisco AnyConnect VPN Client Maintain and Operate Guides*.

Procedure

Step 1 Identify a URL that will cause the client to launch VPN on Demand.

a) Use one of the following methods to identify a URL that will cause the client to launch VPN on Demand.

- Connect if Needed
  - Configure Cisco Unified Communications Manager to be accessed through a domain name (not an IP address) and ensure that this domain name is not resolvable outside the firewall.
  - Include this domain in the “Connect If Needed” list in the Connect On Demand Domain List of the Cisco AnyConnect client connection.
- Always Connect
  - Set the parameter in step 4 to a nonexistent domain. A nonexistent domain causes a DNS query to fail when the user is inside or outside the firewall.
  - Include this domain to the “Always Connect” list in the Connect On Demand Domain List of the Cisco AnyConnect client connection.

    The URL must include only the domain name. Do not include a protocol or a path (for example, use “cm8ondemand.company.com” instead of “https://cm8ondemand.company.com/vpn”.

b) Enter the URL in Cisco AnyConnect and verify that a DNS query on this domain fails.

Step 2 Open the **Cisco Unified CM Administration** interface.

Step 3 Navigate to the device page for the user.

Step 4 In the **Product Specific Configuration Layout** section, in the **On-Demand VPN URL** field, enter the URL that you identified and used in Cisco AnyConnect in Step 1.
The URL must be a domain name only, without a protocol or path.

Step 5 Select **Save**.
When Cisco Jabber opens, it initiates a DNS query to the URL (for example, ccm-sjc-111.cisco.com). If this URL matches the On-Demand domain list entry that you defined in this procedure (for example, cisco.com), Cisco Jabber indirectly initiates the AnyConnect VPN connection.

What to Do Next

- Test this feature.
  - Enter this URL into the Internet browser on the iOS device and verify that VPN launches automatically. You should see a VPN icon in the status bar.
  - Verify that the iOS device can connect to the corporate network using VPN. For example, access a web page on your corporate intranet. If the iOS device cannot connect, contact the provider of your VPN technology.
  - Verify with your IT department that your VPN does not restrict access to certain types of traffic (for example, if the administrator set the system to allow only email and calendar traffic).
- Verify that you set up the client to connect directly to the corporate network.

AnyConnect Documentation Reference

For detailed information on AnyConnect requirements and deployments review the documentation for your release at the following: http://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/products-user-guide-list.html

Session Parameters

You can configure ASA session parameters to improve performance for secure connections. For the best user experience, you should configure the following ASA session parameters:

- Datagram Transport Layer Security (DTLS) — DTLS is an SSL protocol that provides a data path that prevents latency and data loss.
- Auto Reconnect — Auto reconnect, or session persistence, lets Cisco AnyConnect Secure Mobility Client recover from session disruptions and re-establish sessions.
- Session Persistence — This parameter allows the VPN session to recover from service disruptions and re-establish the connection.
- Idle Timeout — Idle timeout defines a period of time after which ASA terminates secure connections, if no communication activity occurs.

- Dead-Peer Detection (DTD) — DTD ensures that ASA and Cisco AnyConnect Secure Mobility Client can quickly detect failed connections.

Set ASA Session Parameters

Cisco recommends that you set up the ASA session parameters as follows to optimize the end user experience for Cisco AnyConnect Secure Mobility Client.

Procedure

Step 1 Set up Cisco AnyConnect to use DTLS.
For more information, see the *Enabling Datagram Transport Layer Security (DTLS) with AnyConnect (SSL) Connections* topic in the *Configuring AnyConnect Features Using ASDM* chapter of the *Cisco AnyConnect VPN Client Administrator Guide, Version 2.0*.

Step 2 Set up session persistence (auto-reconnect).

a) Use ASDM to open the VPN client profile.

b) Set the **Auto Reconnect Behavior** parameter to **Reconnect After Resume**.

For more information, see the *Configuring Auto Reconnect* topic in the *Configuring AnyConnect Features* chapter (Release 2.5) or *Configuring VPN Access* chapter (releases 3.0 or 3.1) of the *Cisco AnyConnect Secure Mobility Client Administrator Guide* for your release.

Step 3 Set the idle timeout value.

a) Create a group policy that is specific to Cisco Jabber clients.

b) Set the idle timeout value to 30 minutes.

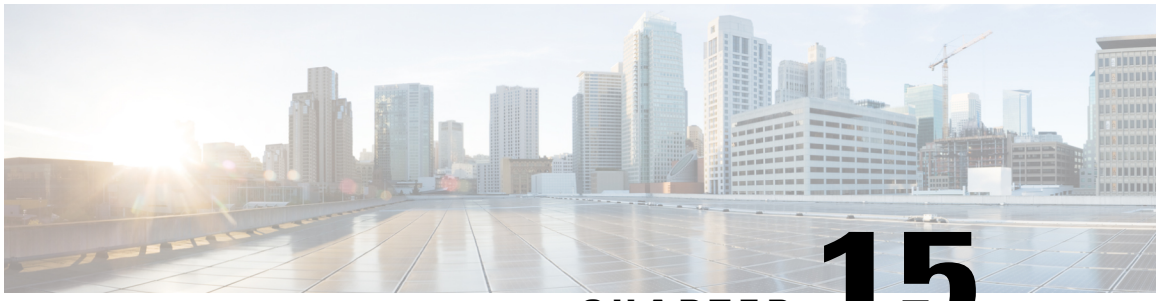
For more information, see the *vpn-idle-timeout* section of the *Cisco ASA 5580 Adaptive Security Appliance Command Reference* for your release

Step 4 Set up Dead Peer Detection (DPD).

a) Disable server-side DPD.

b) Enable client-side DPD.

For more information, see the *Enabling and Adjusting Dead Peer Detection* topic of the *Configuring VPN* chapter of the *Cisco ASA 5500 Series Configuration Guide using the CLI, 8.4 and 8.6*.



CHAPTER 15

Troubleshooting

- Update the SSO Certificate for the Cisco Jabber Domain, page 95

Update the SSO Certificate for the Cisco Jabber Domain

This procedure applies to cloud or hybrid deployments. Use this procedure to upload an updated single sign-on (SSO) certificate for your Cisco Jabber domain.

Note Only certificates with 1024, 2048, or 4096 encryption bits and RC4-MD5 algorithms are supported.

Before You Begin

The certificate must be in a .CER or .CRT file format.

Procedure

Step 1 Log in to the WebEx Org Admin tool at https://www.webex.com/go/connectadmin.

Step 2 After loading the Administration tool, click the **Configuration** tab.

Step 3 In the left navigation bar, click on **Security Settings**.

Step 4 Click the link for **Organization Certificate Management**.
Previously imported X.509 certificates are displayed.

Step 5 In the **Alias** field, enter your company's Cisco WebEx Organization.

Step 6 Click **Browse** to navigate to the X.509 certificate.
The certificate must be in a .CER or .CRT file format.

Step 7 Click **Import** to import the certificate.
If the certificate is not according to the format specified for an X.509 certificate, an error is displayed.

Step 8 Click **Close** twice to return to the **SSO Related Options** screen.

Step 9 Click **Save** to save your Federated Web single sign-on configuration details.