Deployment Scenarios

On-Premises Deployment

An on-premises deployment is one in which you set up, manage, and maintain all services on your corporate network.

You can deploy Cisco Jabber in the following modes:

- **Full UC**—To deploy full UC mode, enable instant messaging and presence capabilities, provision voicemail and conferencing capabilities, and provision users with devices for audio and video.
- **IM-Only**—To deploy IM-only mode, enable instant messaging and presence capabilities. Do not provision users with devices.
- **Phone-Only Mode**—In Phone-Only mode, the user's primary authentication is to Cisco Unified Communications Manager. To deploy phone-only mode, provision users with devices for audio and video capabilities. You can also provision users with additional services such as voicemail.

The default product mode is one in which the user's primary authentication is to an IM and presence server.

On-Premises Deployment with Cisco Unified Communications Manager IM and Presence Service

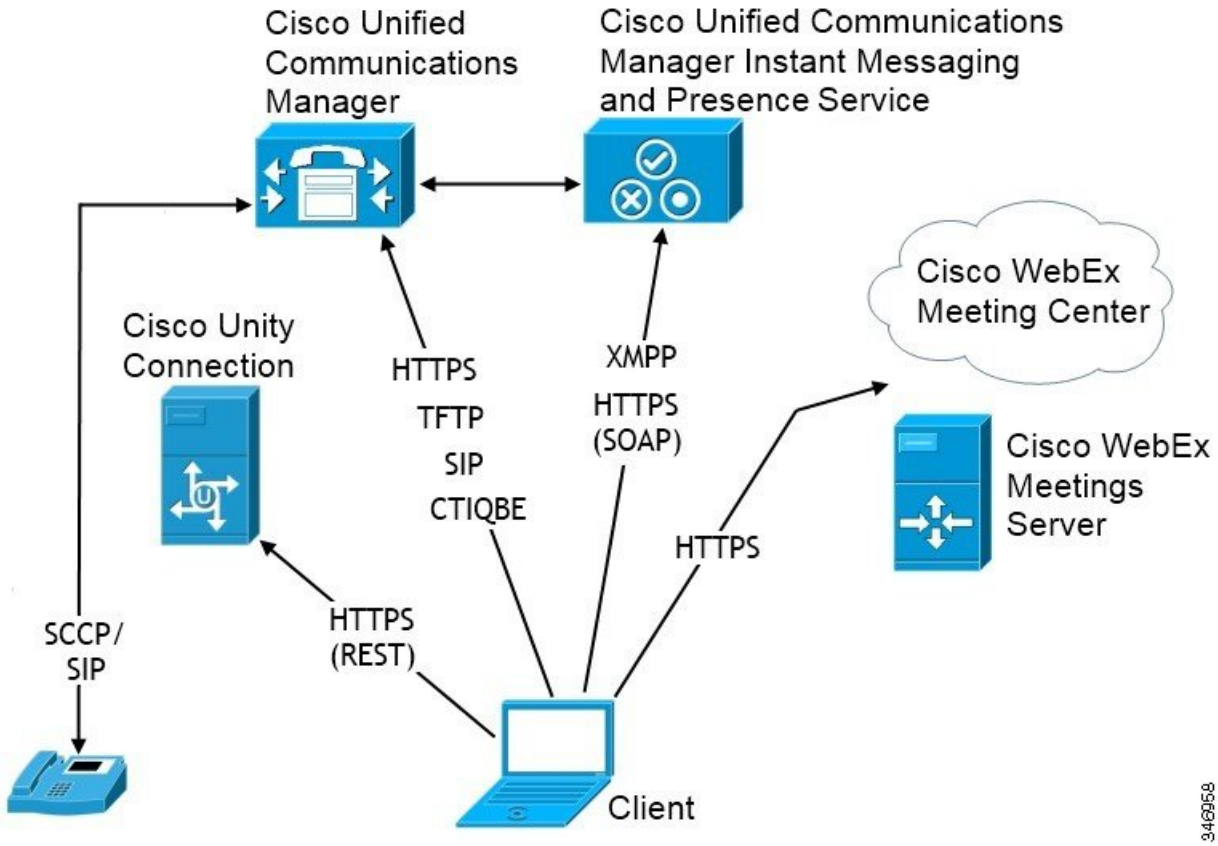
The following services are available in an on-premises deployment with Cisco Unified Communications Manager IM and Presence Service:

- **Presence**—Publish availability and subscribe to other users' availability through Cisco Unified Communications Manager IM and Presence Service.
- **IM**—Send and receive IMs through Cisco Unified Communications Manager IM and Presence Service.

- **File Transfers**—Send and receive files and screenshots through Cisco Unified Communications Manager IM and Presence Service.
- **Audio Calls**—Place audio calls through desk phone devices or computers through Cisco Unified Communications Manager.
- **Video**—Place video calls through Cisco Unified Communications Manager.
- **Voicemail**—Send and receive voice messages through Cisco Unity Connection.
- **Conferencing**—Integrate with one of the following:
  - Webex Meetings Center—Provides hosted meeting capabilities.
  - Webex Meetings Server—Provides on-premises meeting capabilities.

The following figure shows the architecture of an on-premises deployment with Cisco Unified Communications Manager IM and Presence Service.

Figure 1: On-Premises Deployment with Cisco Unified Communications Manager IM and Presence Service



Computer Telephony Integration

Cisco Jabber for Windows and Cisco Jabber for Mac for Mac support CTI of Cisco Jabber from a third party application.

Computer Telephony Integration (CTI) enables you to use computer-processing functions while making, receiving, and managing telephone calls. A CTI application can allow you to retrieve customer information from a database on the basis of information that caller ID provides and can enable you to use information that an interactive voice response (IVR) system captures.

For more information on CTI, see the CTI sections in the appropriate release of the *Cisco Unified Communications Manager System Guide*. Or you can see the following sites on the Cisco Developer Network for information about creating applications for CTI control through Cisco Unified Communications Manager APIs:

- Cisco TAPI: https://developer.cisco.com/site/jtapi/overview/
- Cisco JTAPI: https://developer.cisco.com/site/jtapi/overview/

On-Premises Deployment in Phone Mode

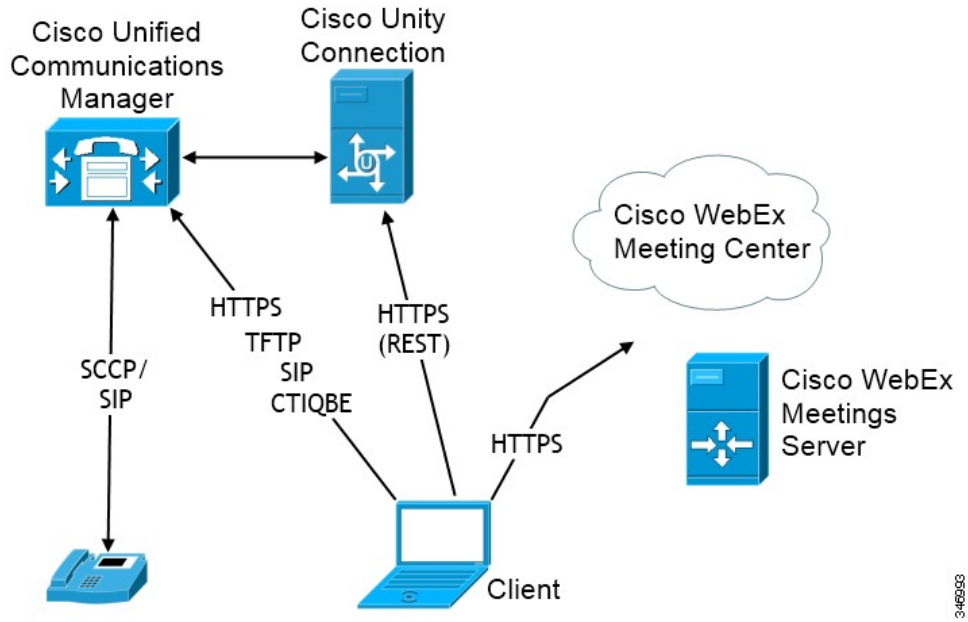
The following services are available in a phone mode deployment:

- **Contact**—This is applicable for mobile clients only. Cisco Jabber updates the contact information from the phone's contact address book.
- **Audio Calls**—Place audio calls through desk phone devices or on computers through Cisco Unified Communications Manager.
- **Video**—Place video calls through Cisco Unity Connection.
- **Voicemail**—Send and receive voice messages through Cisco Unity Connection.
- **Conferencing**—Integrate with one of the following:
  - **Webex Meetings Center**—Provides hosted meeting capabilities.
  - **Webex Meetings Server**—Provides on-premises meeting capabilities.

Note Cisco Jabber for Android and Cisco Jabber for iPhone and iPad do not support conferencing in phone mode.

The following figure shows the architecture of an on-premises deployment in phone mode.

Figure 2: On-Premises Deployment in Phone Mode



Softphone

Softphone mode downloads the configuration file from the TFTP server and operates as a SIP registered endpoint. The client uses the CCMCIP or UDS service to get the device name to register with Cisco Unified Communications Manager.

Deskphone

Deskphone mode creates a CTI connection with Cisco Unified Communications Manager to control the IP Phone. The client uses CCMCIP to gather the information about devices associated with a user and creates a list of IP phones available for control by the client.

Cisco Jabber for Mac in deskphone mode doesn't support desk phone video.

Extend and Connect

Cisco Unified Communications Manager Extend and Connect capabilities enable users control calls on devices such as public switched telephone network (PSTN) phones and private branch exchange (PBX) devices. For more information, see the Extend and Connect feature for your Cisco Unified Communications Manager release.

We recommend that you use extend and connect capabilities with Cisco Unified Communications Manager 9.1(1) and later.

Phone Mode with Contacts Deployment

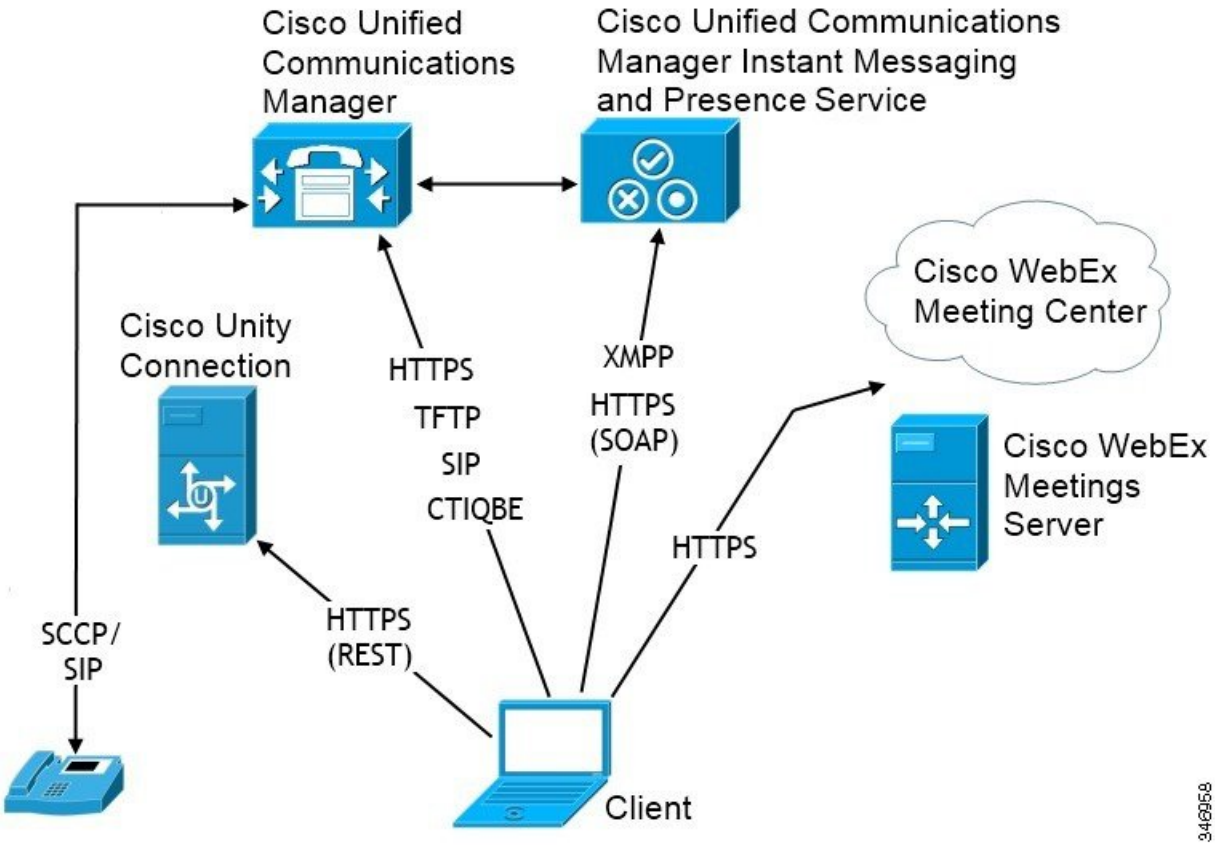
The following services are available in a phone mode with contacts deployment:

- **Contacts**—Contact information through Cisco Unified Communications Manager IM and Presence Service.

- **Presence**—Publish availability and subscribe to other users' availability through Cisco Unified Communications Manager IM and Presence Service.
- **Audio Calls**—Place audio calls through desk phone devices or computers through Cisco Unified Communications Manager.
- **Video**—Place video calls through Cisco Unified Communications Manager.
- **Voicemail**—Send and receive voice messages through Cisco Unity Connection.
- **Conferencing**—Integrate with one of the following:
  - Webex Meetings Center—Provides hosted meeting capabilities.
  - Webex Meetings Server—Provides on-premises meeting capabilities.

The following figure shows the architecture of an on-premises deployment with Cisco Unified Communications Manager IM and Presence Service.

Figure 3: Phone Mode with Contacts Deployment



Cloud-Based Deployments

A cloud-based deployment uses Webex to host services.

For cloud and hybrid deployments with Cisco Webex Messenger, you manage and monitor your cloud-based deployment using the Webex Administration Tool. You don't need to set up service profiles for your users.

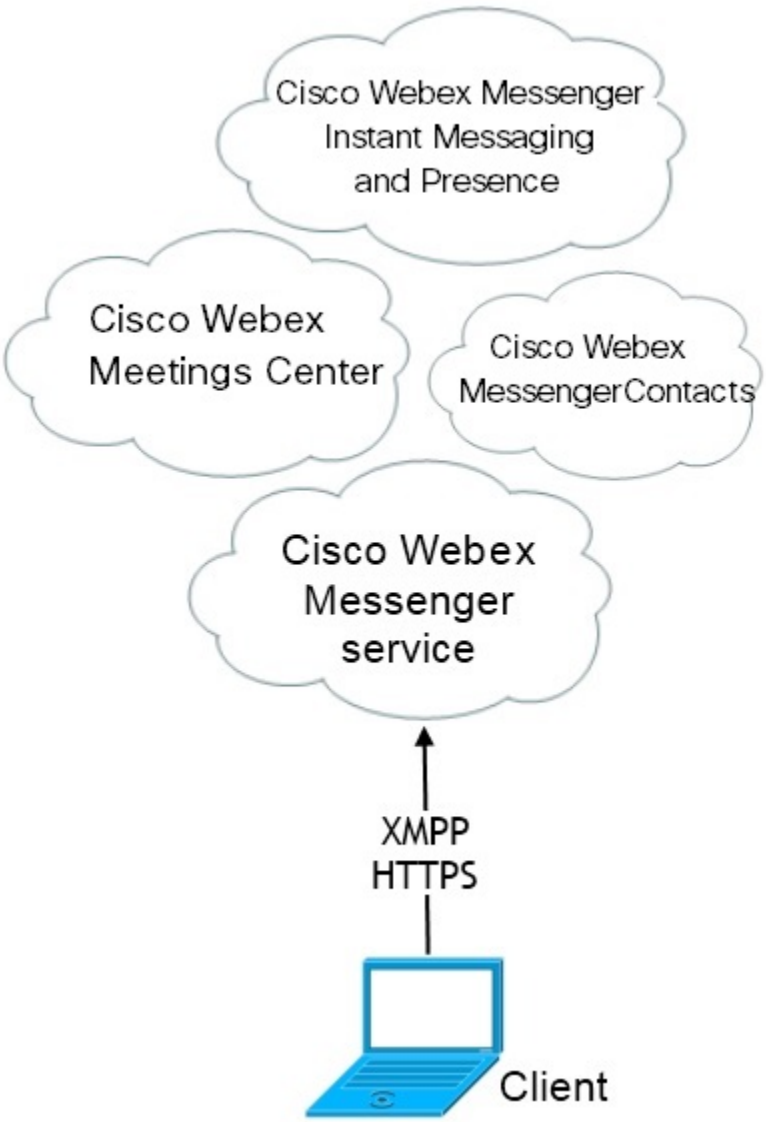
For cloud and hybrid deployments with Cisco Webex Platform service, you manage and monitor your deployment using the Cisco Control Hub.

Cloud-Based Deployment with Cisco Webex Messenger

The following services are available in a cloud-based deployment using Webex Messenger:

- **Contact Source**—Webex Messenger provides contact resolution.
- **Presence**—Webex Messenger lets users show their availability and see to other users' availability.
- **Instant Messaging**—Webex Messenger lets users send and receive instant messages.
- **Conferencing**—Webex Meetings Center provides hosted meeting capabilities.

The following figure shows the architecture of a cloud-based deployment.



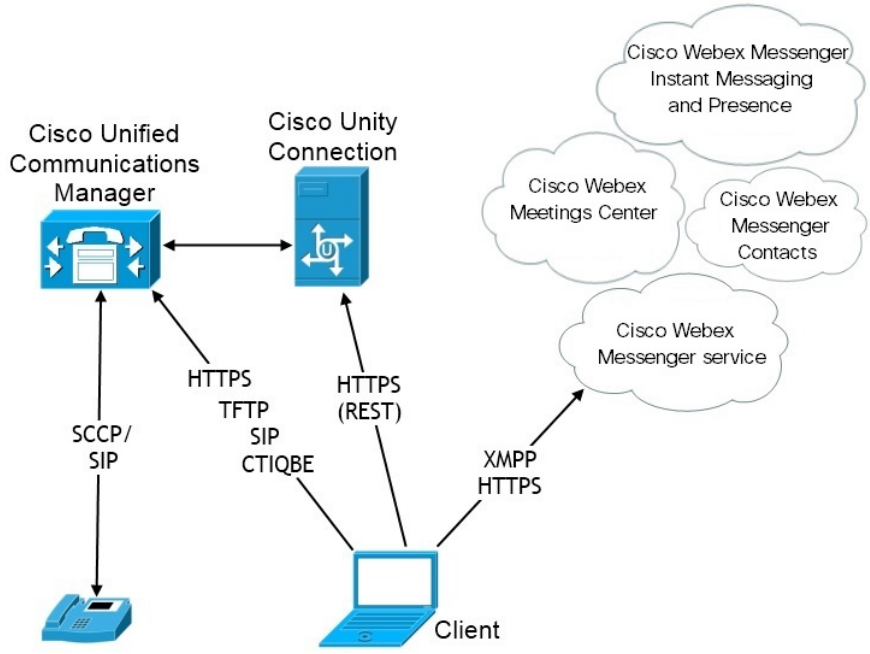
Hybrid Cloud-Based Deployment with Cisco Webex Messenger Service

The following services are available in a hybrid cloud-based deployment that uses Webex Messenger service:

- **Contact Source**—The Webex Messenger service provides contact resolution.
- **Presence**—The Webex Messenger service allows users to publish their availability and subscribe to other users' availability.
- **Instant Messaging**—The Webex Messenger service allows users to send and receive instant messages.
- **Audio**—Place audio calls through desk phone devices or computers through Cisco Unified Communications Manager.
- **Video**—Place video calls through Cisco Unified Communications Manager.

- **Conferencing**—Webex Meetings Center provides hosted meeting capabilities.
- **Voicemail**—Send and receive voice messages through Cisco Unity Connection.

The following figure shows the architecture of a hybrid cloud-based deployment.

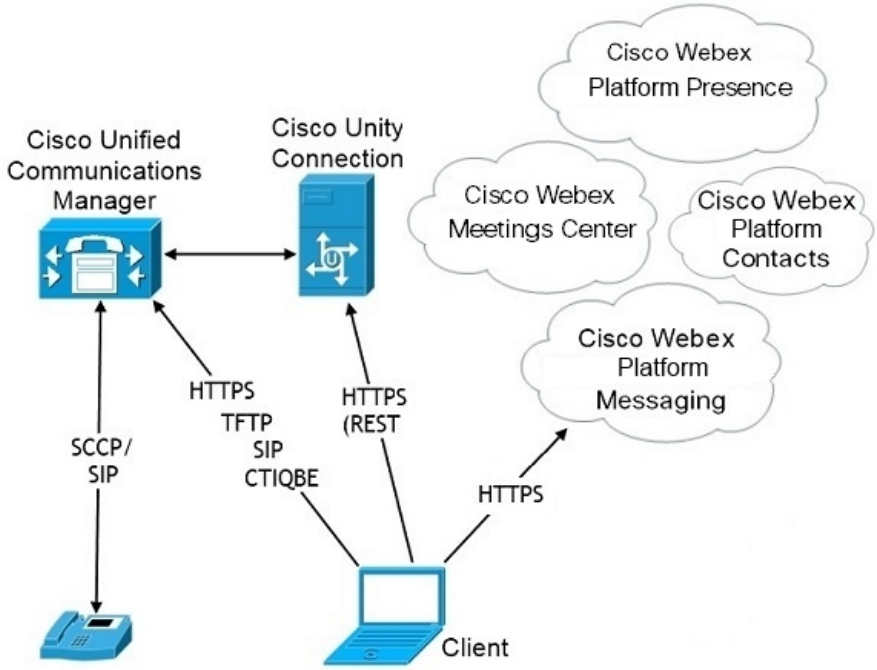


Hybrid Cloud-Based Deployment with Cisco Webex Platform Service

The following Jabber team messaging mode services are available in a Jabber hybrid cloud-based deployment with Cisco Webex Platform service:

- Contact Source—The Cisco Webex Platform service provides contacts.
- Presence—The Cisco Webex Platform service allows users to publish their availability and to view other users' availability.
- Messaging—The Cisco Webex Platform service allows users to send and receive messages.
- Audio—Make audio calls through desk phone devices or computers using Cisco UC Manager.
- Video—Make video calls using Cisco UC Manager.
- Conferencing—Webex Meetings Center provides hosted meeting capabilities.
- Voicemail—Send and receive voice messages through Cisco Unity Connection.

The following figure shows the architecture of a Jabber hybrid cloud-based deployment with Cisco Webex Platform service.



Contacts in Jabber Team Messaging Mode

Sign-In Flow

You must migrate your users' contacts while you enable team messaging mode in the Webex Control Hub.

This sign-in flow outlines the process for migrating users' contacts. The flow starts with the users being signed in to their current Jabber deployment. You enable Jabber team messaging mode and then migrate their contacts.

1. Users are signed into their current Jabber deployment, which connects to Cisco UC Manager IM&P or Cisco Webex Messenger.
2. The admin changes the configuration in the Webex Control Hub to enable Jabber team messaging mode, and optionally contact migration, and Jabber calls.
3. The next day, users sign into their current Jabber deployment. Within five minutes, Jabber performs the service discovery process, detecting that there is a Cisco Webex Platform service deployment for that user.
4. Jabber prompts the user to sign out of Jabber with the message, "Configuration changes detected."
5. Users sign back in again, this time authenticating to the Cisco Webex Platform service.
6. If you enabled contact migration, a message prompts the users to get their Jabber contacts. If they click Ok, then Jabber takes the contact list cache and uploads it to the Cisco Webex Platform service. If users selects **Cancel**, then Jabber doesn't migrate their contact list. They can later search for and add their contacts individually.

   During contact migration, Jabber only migrates contacts who are enabled for Cisco Webex Platform service. Jabber doesn't store custom contacts in Cisco Webex Platform service and can't add them to users' contact lists.

7. After Jabber connects to the Cisco Webex Platform service, it connects to Cisco UC Manager to download the service profile. If SSO is enabled on both Cisco Webex Platform service and UC Manager with different IdPs, or if SSO is only enabled on one, then users are prompted to enter their credentials. But, if SSO is on both with the same IdP, then no sign-in is necessary.

Deployment Considerations for Jabber Team Messaging Mode and Contact Migration

Your Cisco Webex Platform service org needs to have the same domain as the services domain. If they are different domains, then contact migration is not possible for users.

Deployment in a Virtual Environment

You can deploy Cisco Jabber for Windows in a virtual environment.

The following features are supported in a virtual environment:

- Instant messaging and presence with other Cisco Jabber clients
- Desk phone control
- Voicemail
- Presence integration with Microsoft Outlook 2007, 2010 and 2013
- Mobile and Remote Access (MRA)

Virtual Environment and Roaming Profiles

In a virtual environment, users do not always access the same virtual desktop. To guarantee a consistent user experience, these files must be accessible every time that the client is launched. Cisco Jabber stores user data in the following locations:

- `C:\Users\`*`username`*`\AppData\Local\Cisco\Unified Communications\Jabber\CSF`
  - **Contacts**—Contact cache files
  - **History**—Call and chat history
  - **Photo cache**—Caches the directory photos locally
- `C:\Users\`*`username`*`\AppData\Roaming\Cisco\Unified Communications\Jabber\CSF`
  - **Config**—Maintains user configuration files and stores configuration store cache
  - **Credentials**—Stores encrypted username and password file

Because file encryption and decryption are linked to the Windows user profile, ensure that the following folders are accessible:

- `C:\Users\`*`username`*`\AppData\Roaming\Microsoft\Credentials`
- `C:\Users\`*`username`*`\AppData\Roaming\Microsoft\Crypto`
- `C:\Users\`*`username`*`\AppData\Roaming\Microsoft\Protect`

- C:\Users*username*\AppData\Roaming\Microsoft\SystemCertificates
- C:\Users*username*\AppData\Local\Microsoft\Credentials
- C:\Users*username*\AppData\Local\Microsoft\identitycache

Note Cisco Jabber credentials caching is not supported when using Cisco Jabber in non-persistent virtual deployment infrastructure (VDI) mode.

If required, you can exclude files and folders from synchronization by adding them to an exclusion list. To synchronize a subfolder that is in an excluded folder, add the subfolder to an inclusion list.

To preserve personal user settings, do the following:

- Do not exclude the following directories:
  - AppData\Local\Cisco
  - AppData\Local\JabberWerxCPP
  - AppData\Roaming\Cisco
  - AppData\Roaming\JabberWerxCPP
- Use the following dedicated profile management solutions:
  - **Citrix Profile Management**—Provides a profile solution for Citrix environments. In deployments with random hosted virtual desktop assignments, Citrix profile management synchronizes each user's entire profile between the system it is installed on and the user store.
  - **VMware View Persona Management**—Preserves user profiles and dynamically synchronizes them with a remote profile repository. VMware View Persona Management does not require the configuration of Windows roaming profiles and can bypass Windows Active Directory in the management of VMware Horizon View user profiles. Persona Management enhances the functionality of existing roaming profiles.

Deploying Jabber Softphone for VDI

To deploy Jabber in a virtual environment with calling capabilities, you need to deploy Jabber Softphone for Virtual Desktop Infrastructure.

The workflow for deploying Jabber Softphone for VDI depends if you are deploying in an on-premises or hybrid environment, and follows Jabber deployment workflow up until application installation, at which point you follow Jabber Softphone for VDI deployment and installation workflows.

To get the on-premises deployment workflow for Jabber Softphone for VDI, see the *Full UC Deployment* workflow in the *Deployment and Installation Workflows* section of On-Premises Deployment for Cisco Jabber.

To get the hybrid deployment workflow for Jabber Softphone for VDI, see the *Hybrid Deployment using Webex Messenger* workflow in the *Workflows for Cloud and Hybrid Deployments* section of Cloud and Hybrid Deployments for Cisco Jabber.

Enterprise Mobility Management Deployments

Jabber supports two SDK-based clients for Enterprise Mobility Management (EMM) deployments:

- Cisco Jabber for Intune
- Cisco Jabber for BlackBerry

Your organization can deploy these clients to enforce policies for using Jabber on mobile devices in deployments that allow "Bring Your Own Device". For example, these policies can:

- Prevent the use of insecure jail-broken or rooted devices.
- Enforce minimum OS and app versions.
- Prevent users from copying data in Jabber and pasting it into another app.

Use the new EMMType parameter to control the Jabber clients on which your users can sign in.

Remember These clients follow a delayed release cycle. The clients release later than the corresponding releases of Jabber for Android and Jabber for iPhone and iPad.

EMM with Jabber for Intune

When you use the Jabber for Intune client in your deployment, your administrator configures your management policies in Microsoft Azure. Users download the new client from the App Store or Google Play Store. When the user runs the new client, it synchs with the policies that the administrator created.

Caution Jabber for Intune doesn't support Apple Push Notification (APN) on the iOS platform. When you put Jabber in the background, iOS devices might not receive chat messages and calls.

Note For Android devices, users first install the Intune Company Portal. Then, they run the client through the portal.

The general process for setting up Jabber for Intune is:

1. Create a new Azure AD tenant.
2. Create new AD users or synch your on-premises AD users.
3. Create an Office 365 group or a Security group and add your users.
4. Add the Jabber for Intune client into Microsoft Intune.
5. Create and deploy your policies in Microsoft Intune.
6. Users sign in to the client and synch to receive your policies.

For details on these steps, see the Microsoft documentation.

This table lists the Microsoft Intune restrictions that we support in app protection policies for Cisco Jabber:

Restriction	Android	iPhone and iPad
Send data to other apps	Yes	Yes
Save copies of your organization's data	Yes	Yes
Cut, copy, and paste to other apps	Yes	Yes
Screen captures	Yes	N/A
Maximum PIN attempts	Yes	Yes
Offline grace periods	Yes	Yes
Minimum app versions	Yes	Yes
Use on jailbroken or rooted devices	Yes	Yes
Minimum device OS version	Yes	Yes
Minimum patch version	Yes	N/A
Work (or school) account credentials for access	Yes	Yes
Recheck the access requirements	Yes	Yes

EMM with Jabber for BlackBerry

When you use the Jabber for BlackBerry client in your deployment, your administrator configures your management policies in the BlackBerry Unified Endpoint Management (UEM). Users download the new client from the App Store or Google Play Store. Jabber for BlackBerry is undergoing BlackBerry certification and isn’t yet available in BlackBerry Marketplace.

Important Because the client is undergoing BlackBerry certification, we must grant access to your organization. To receive access, contact us (jabber-mobile-mam@cisco.com) and provide the Organization ID of your customer from their BlackBerry UEM server.

The new client has integrated the BlackBerry Dynamics SDK and can directly fetch the policies from BlackBerry UEM. The client bypasses BlackBerry Dynamics for connectivity and storage. The FIPS setting is not supported through the BlackBerry Dynamics SDK.

Your chat, voice, and video traffic bypasses the BlackBerry infrastructure. When the client isn't on-premises, it requires Mobile & Remote Access through a Cisco Expressway for all traffic.

Caution Jabber for BlackBerry doesn't support Apple Push Notification (APN) on the iOS platform. When you put Jabber in the background, iOS devices might not receive chat messages and calls.

Note Jabber for BlackBerry on Android requires Android 6.0 or above.

Jabber for BlackBerry on iOS requires iOS 11.0 or above.

For BlackBerry Dynamics, your administrator sets up policies in to control use of the Jabber for BlackBerry client.

The general process for setting up Jabber for BlackBerry is:

1. Create a server in the UEM.
2. Add the Jabber for BlackBerry client into BlackBerry Dynamics.
3. Create or import your users in BlackBerry Dynamics.

Note For Android users, you can optionally generate access keys in BlackBerry Dynamics.

4. Create and deploy your policies in UEM. Note the behavior of these settings on the Jabber for BlackBerry app configuration:
   - If you enable the optional DLP policy, BlackBerry requires that:
     - Use BlackBerry Works to send emails.
     - Use BlackBerry Access for SSO authentication in iOS devices. Enable **Use native browser** for iOS on Expressway and Unified Communications Manager. Then, add the **`ciscojabber`** scheme to the BlackBerry access policies in the BlackBerry UEM.
   - This list shows the Jabber parameters that are useful to set through app configuration in Jabber for BlackBerry deployments. See the *URL Configuration for Cisco Jabber for Android, iPhone, and iPad* section in the *Deployment Guide* for more details on these parameters:

Field	Supported on iOS	Supported on Android
Disable cross launch Webex Meetings [1]	Yes	Yes
Services Domain	Yes	Yes
Voice Services Domain	Yes	Yes
Service Discovery Excluded Services	Yes	Yes
Services Domain SSO Email Prompt	Yes	Yes
Invalid Certificate Behavior	Yes	Yes
Telephony Enabled	Yes	Yes
Allow Url Provisioning	Yes	Yes
IP Mode	Yes	Yes

[1] Enabling cross launch of Webex Meetings allows it to run as an exception in a BlackBerry Dynamics container that doesn't allow non-Dynamics apps.

5. Users sign in to the client.

For details on these steps, see the BlackBerry documentation.

This table lists the BlackBerry restrictions that we support in app protection policies for Cisco Jabber:

Group	Feature	Android	iPhone and iPad
IT policies	Wipe the device without network connectivity	Yes	Yes
Activation	Allowed Version	Yes	Yes
BlackBerry Dynamics	Password	Yes	Yes
	Data leakage prevention - Don’t allow copying data from BlackBerry Dynamics apps into non-BlackBerry Dynamics apps	Yes	Yes
	Data leakage prevention - Don’t allow copying data from non-BlackBerry Dynamics apps into BlackBerry Dynamics apps	Yes	Yes
	Data leakage prevention - Don’t allow screen captures on Android and Windows 10+ devices	Yes	N/A
	Data leakage prevention - Don’t allow screen recording and sharing on iOS devices	N/A	Yes
	Data leakage prevention - Don’t allow custom keyboards on iOS devices	N/A	Yes
Enterprise Management Agent profile	Allow personal app collection	Yes	Yes
Compliance profile	Rooted OS or failed attestation	Yes	Yes
	Restricted OS version is installed	Yes	Yes
	Required security patch level isn’t installed	Yes	N/A

IdP Connections in Jabber for BlackBerry

In Jabber for Android and iPhone and iPad deployments, the client connects to an Identity Provider (IdP) proxy in the DMZ. The proxy then passes the request to the IdP server behind the inner firewall.

In Jabber for BlackBerry, you have an alternate path available. If you enable the DLP policy in the BlackBerry UEM, clients on iOS devices can securely tunnel directly to the IdP server. To use this setup, configure your deployment as follows:

- Enable **Use native browser** for iOS on Expressway and Unified CM.
- Add the **`ciscojabber`** scheme to the BlackBerry access policies in the BlackBerry UEM.

Jabber for BlackBerry on the Android OS always connects to the IdP proxy for SSO.

If your deployment only contains devices running on iOS, you don’t need an IdP proxy in the DMZ. But, if your deployment contains any devices running on Android OS, you require the IdP proxy.

App Transport Security on iOS

iOS includes the App Transport Security (ATS) feature. ATS requires that Jabber for BlackBerry and Jabber for Intune makes secure network connections over TLS with reliable certificates and encryption. ATS blocks connections to servers that don't have an X.509 digital certificate. The certificate must pass these checks:

- An intact digital signature
- A valid expiration date
- A name that matches the DNS name of the server
- A chain of valid certificates to a trusted anchor certificate from a CA

Note For more information on trusted anchor certificates that are part of iOS, see *Lists of available trusted root certificates in iOS* at https://support.apple.com/en-us/HT204132. A system administrator or user can also install their own trusted anchor certificate, as long as it meets the same requirements.

For more information on ATS, see *Preventing Insecure Network Connections* at https://developer.apple.com/documentation/security/preventing_insecure_network_connections.

Remote Access

Your users may need to access their work from a location that's outside the corporate network. You can provide them access to their work using one of the Cisco products for remote access.

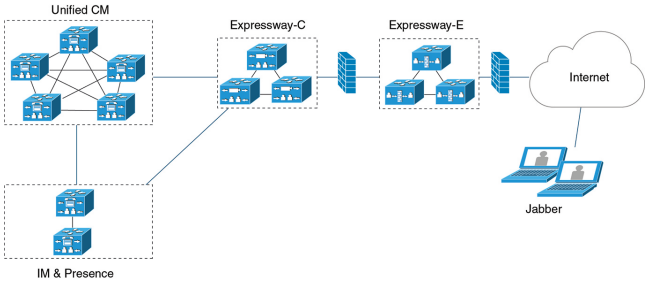
Jabber is not tested or validated with any third-party VPN client.

Expressway for Mobile and Remote Access

Expressway for Mobile and Remote Access for Cisco Unified Communications Manager allows users to access their collaboration tools from outside the corporate firewall without using a virtual private network (VPN). Using Cisco collaboration gateways, the client can connect securely to your corporate network from remote locations such as public Wi-Fi networks or mobile data networks.

Figure 4: How the Client Connects to the Expressway for Mobile and Remote Access

The following diagram illustrates the architecture of an Expressway for Mobile and Remote Access environment.



First Time Signing into Jabber Using Expressway for Mobile and Remote Access

Applies to Cisco Jabber for mobile clients.

Users can sign in to the client for the first time using Expressway for Mobile and Remote Access to connect to services from outside the corporate firewall. In the following cases, however, initially sign in while on the corporate network:

- If the voice services domain is different from the other services domain, then users must be inside the corporate network to get the correct voice services domain from the `jabber-config.xml` file. For a hybrid deployment, administrator can configure the VoiceServicesDomain parameter, refer to the latest version of the *Parameters Reference Guide for Cisco Jabber*. In this case, users are not required to sign in inside the corporate network.
- If Cisco Jabber must complete the CAPF enrollment process, which is required when using a secure or mixed mode cluster.

We do not support first-time sign-in on a public network if user is using a secure phone through Expressway for Mobile and Remote Access environment. If the configuration is for a secure profile with encrypted TFTP, then the first-time sign-in must be in on-premises to allow CAPF enrolment. First-time sign-in on a public network cannot be supported without Cisco Unified Communications Manager, Expressway for Mobile and Remote Access, and Cisco Jabber enhancements. However we do support:

- Encrypted TFTP, with first-time sign-in through on-premises.
- Unencrypted TFTP, with first-time sign-in through Expressway for Mobile and Remote Access or on-premises.

Supported Services

The following table summarizes the services and functionality that are supported when the client uses Expressway for Mobile and Remote Access to remotely connect to Cisco Unified Communications Manager.

Table 1: Summary of Supported Services for Expressway for Mobile and Remote Access

Service	Supported	Unsupported
Directory		
UDS directory search	X	

Service	Supported	Unsupported
LDAP directory search		X
Directory photo resolution	X * Using HTTP white list on Cisco Expressway-C	
Intradomain federation	X * Contact search support depends on the format of your contact IDs. For more information, see the note below.	
Interdomain federation	X	
Instant Messaging and Presence		
On-premises	X	
Cloud	X	
Chat	X	
Group chat	X	
Persistent chat	X	
High Availability: On-premises deployments	X	
File transfer: On-premises deployments	X Advanced options available for file transfer using Cisco Unified Communications Manager IM and Presence Service 10.5(2) or later, see the note below.	
File transfer: Cloud deployments	X	
Video screen share - BFCP	X (Cisco Jabber for mobile clients only support BFCP receive.)	
IM-Only Screen Share		x
Audio and Video		
Audio and video calls	X * Cisco Unified Communications Manager 9.1(2) and later	
Deskphone control mode (CTI) (desktop clients only)		X
Extend and connect (desktop clients only)		X

Service	Supported	Unsupported
Remote desktop control (desktop clients only)		X
Silent Monitoring and Call Recording		X
Dial via Office - Reverse (mobile clients only)	X	
Session persistency		X
Early media		X
Self Care Portal access		X
Graceful Registration	X * Applies to Cisco Jabber for Android. Jabber for Android supports graceful registration over Expressway for Mobile and Remote Access from Cisco Unified Communications Manager Release 10.5.(2) 10000-1.	
Shared line	X Prerequisites: • Cisco Expressway to X8.9.1 or later • Cisco Unified Communications Manager to 11.5 SU(2) or later	
Voicemail		
Visual voicemail	X * Using HTTP white list on Cisco Expressway-C	
Webex Meetings		
On-premises		X * Unsupported, except with an on-premises Cisco Webex Meeting Server from Jabber 11.6 forward.
Cloud	X	
Webex screen share (desktop clients only)	X	
Installation (Desktop clients)		

Service	Supported	Unsupported
Installer update	X * Using HTTP white list on Cisco Expressway-C	X Not supported on Cisco Jabber for Mac
Customization		
Custom HTML tabs		X
Enhanced911 Prompt	X * To ensure that the web page renders correctly for all Jabber clients operating outside the corporate network, the web page must be a static HTML page because the scripts and link tags are not supported by the E911NotificationURL parameter. For more inforation, see the latest *Parameter Reference Guide for Cisco Jabber*.	
Security		
ICE protocol for media	X	
CAPF enrollment		X
Single Sign-On	X	
Advanced Encryption Standard (AES) 256 and TLS1.2	X * Applies to Cisco Jabber for Android. Advanced encryption is supported only on corporate Wi-Fi	
Troubleshooting (Desktop clients only)		
Problem report generation	X	
Problem report upload		X
High Availability (failover)		
Audio and Video services		X
Voicemail services		X
IM and Presence services	X	
Contact search	X	

Service	Supported	Unsupported
Contact resolution	X	
Configuration Management		
Fast Sign-in	X	
Authentication and Authorization		
O-Auth support for SSO Jabber users	X	

Directory

When the client connects to services using Expressway for Mobile and Remote Access, it supports directory integration with the following limitations.

- LDAP contact resolution —The client cannot use LDAP for contact resolution when outside of the corporate firewall. Instead, the client must use UDS for contact resolution.

  When users are inside the corporate firewall, the client can use either UDS or LDAP for contact resolution. If you deploy LDAP within the corporate firewall, Cisco recommends that you synchronize your LDAP directory server with Cisco Unified Communications Manager to allow the client to connect with UDS when users are outside the corporate firewall.

- Directory photo resolution — To ensure that the client can download contact photos, you must add the server on which you host contact photos to the white list of your Cisco Expressway-C server. To add a server to Cisco Expressway-C white list, use the **HTTP server allow** setting. For more information, see the relevant Cisco Expressway documentation.

- Intradomain federation — When you deploy intradomain federation and the client connects with Expressway for Mobile and Remote Access from outside the firewall, contact search is supported only when the contact ID uses one of the following formats:

  - sAMAccountName@domain
  - UserPrincipleName (UPN)@domain
  - EmailAddress@domain
  - employeeNumber@domain
  - telephoneNumber@domain

- Interdomain federation using XMPP — Expressway for Mobile and Remote Access doesn't enable XMPP Interdomain federation itself. Cisco Jabber clients connecting over Expressway for Mobile and Remote Access can use XMPP Interdomain federation if it has been enabled on Cisco Unified Communications Manager IM and Presence.

Instant Messaging and Presence

When the client connects to services using Expressway for Mobile and Remote Access, it supports instant messaging and presence with the following limitations:

File transfer has the following limitations for desktop and mobile clients:

- For Webex cloud deployments, file transfer is supported.
- For on-premises deployments with Cisco Unified Communication IM and Presence Service 10.5(2) or later, the **Managed File Transfer** selection is supported, however the **Peer-to-Peer** option is not supported.
- For on-premises deployments with Cisco Unified Communications Manager IM and Presence Service 10.0(1) or earlier deployments, file transfer is not supported.
- For Expressway for Mobile and Remote Access deployments with unrestricted Cisco Unified Communications Manager IM and Presence Server, Managed File Transfer is not supported.

Audio and Video Calling

When the client connects to services using Expressway for Mobile and Remote Access, it supports voice and video calling with the following limitations.

- Cisco Unified Communications Manager — Expressway for Mobile and Remote Access supports video and voice calling with Cisco Unified Communications Manager Version 9.1.2 and later.
- Deskphone control mode (CTI) (Desktop clients only) — The client does not support deskphone control mode (CTI), including extension mobility.
- Extend and connect (Desktop clients only) — The client cannot be used to:
  - Make and receive calls on a Cisco IP Phone in the office.
  - Perform mid-call control such as hold and resume on a home phone, hotel phone, or Cisco IP Phone in the office.
- Session Persistency — The client cannot recover from audio and video calls drop when a network transition occurs. For example, if a users start a Cisco Jabber call inside their office and then they walk outside their building and lose Wi-Fi connectivity, the call drops as the client switches to use Expressway for Mobile and Remote Access.
- Early Media — Early Media allows the client to exchange data between endpoints before a connection is established. For example, if a user makes a call to a party that is not part of the same organization, and the other party declines or does not answer the call, Early Media ensures that the user hears the busy tone or is sent to voicemail.

  When using Expressway for Mobile and Remote Access, the user does not hear a busy tone if the other party declines or does not answer the call. Instead, the user hears approximately one minute of silence before the call is terminated.
- Self care portal access (Desktop clients only) — Users cannot access the Cisco Unified Communications Manager Self Care Portal when outside the firewall. The Cisco Unified Communications Manager user page cannot be accessed externally.

  Cisco Expressway-E proxies all communications between the client and unified communications services inside the firewall. However, the Cisco Expressway-E does not proxy services that are accessed from a browser that is not part of the Cisco Jabber application.

Voicemail

Voicemail service is supported when the client connects to services using Expressway for Mobile and Remote Access.

Note To ensure that the client can access voicemail services, you must add the voicemail server to the white list of your Cisco Expressway-C server. To add a server to Cisco Expressway-C white list, use the **HTTP server allow** setting. For more information, see the relevant Cisco Expressway documentation.

Installation

Cisco Jabber for Mac — When the client connects to services using Expressway for Mobile and Remote Access, it doesn't support installer updates.

Cisco Jabber for Windows — When the client connects to services using Expressway for Mobile and Remote Access, it supports installer updates.

Note To ensure that the client can download installer updates, you must add the server that hosts the installer updates to the white list of your Cisco Expressway-C server. To add a server to the Cisco Expressway-C white list, use the **HTTP server allow** setting. For more information, see the relevant Cisco Expressway documentation.

Security

When the client connects to services using Expressway for Mobile and Remote Access, it supports most security features with the following limitations.

- Initial CAPF enrollment — Certificate Authority Proxy Function (CAPF) enrollment is a security service that runs on the Cisco Unified Communications Manager Publisher that issues certificates to Cisco Jabber (or other clients). To successfully enrol for CAPF, the client must connect from inside the firewall or using VPN.
- End-to-end encryption — When users connect through Expressway for Mobile and Remote Access and participate in a call:
  - Media is always encrypted on the call path between the Cisco Expressway-C and devices that are registered to the Cisco Unified Communications Manager using Expressway for Mobile and Remote Access.
  - Media is not encrypted on the call path between the Cisco Expressway-C and devices that are registered locally to Cisco Unified Communications Manager, if either Cisco Jabber or an internal device is not configured with Encrypted security mode.
  - Media is encrypted on the call path between the Expressway-C and devices that are registered locally to Cisco Unified Communication Manager, if both Cisco Jabber and internal device are configured with Encypted security mode.
  - In case where Cisco Jabber clients always connects through Expressway for Mobile and Remote access, CAPF enrollment is not required to achieve end-to-end encryption. However, Cisco Jabber devices must still be configured with encrypted security mode, and Cisco Unified Communications Manager must be enabled to support mixed mode.
  - You can configure ICE passthrough support on your Expressway-C or Expressway-E servers to ensure media sent over Jabber is encrypted when outside the corporate network. For more information on how to set it up, see the *Deployment Guide* for *Mobile and Remote Access through Cisco Expressway* .

Troubleshooting

Cisco Jabber for Windows only. Problem report upload — When the desktop client connects to services using Expressway for Mobile and Remote Access, it cannot send problem reports because the client uploads problem reports over HTTPS to a specified internal server.

To work around this issue, users can save the report locally and send the report in another manner.

High Availability (failover)

High Availability means that if the client fails to connect to the primary server, it fails over to a secondary server with little or no interruption to the service. In relation to high availability being supported on the Expressway for Mobile and Remote Access, high availability refers to the server for the specific service failing over to a secondary server (such as Instant Messaging and Presence).

Some services are available on the Expressway for Mobile and Remote Access that are not supported for high availability. This means that if users are connected to the client from outside the corporate network and the instant messaging and presence server fails over, the services will continue to work as normal. However, if the audio and video server or voicemail server fails over, those services will not work as the relevant servers do not support high availability.

Cisco AnyConnect Deployments

Cisco AnyConnect refers to a server-client infrastructure that enables the client to connect securely to your corporate network from remote locations such as Wi-Fi networks or mobile data networks.

The Cisco AnyConnect environment includes the following components:

- Cisco Adaptive Security Appliance — Provides a service to secure remote access.
- Cisco AnyConnect Secure Mobility Client — Establishes a secure connection to Cisco Adaptive Security Appliance from the user's device.

This section provides information that you should consider when deploying the Cisco Adaptive Security Appliance (ASA) with the Cisco AnyConnect Secure Mobility Client. Cisco AnyConnect is the supported VPN for Cisco Jabber for Android and Cisco Jabber for iPhone and iPad. If you use an unsupported VPN client, ensure that you install and configure the VPN client using the relevant third-party documentation.

For Samsung devices running Android OS 4.4.x, use Samsung AnyConnect version 4.0.01128 or later. For Android OS version above 5.0, you must use Cisco AnyConnect software version later than 4.0.01287.

Cisco AnyConnect provides remote users with secure IPsec (IKEv2) or SSL VPN connections to the Cisco 5500 Series ASA. Cisco AnyConnect can be deployed to remote users from the ASA or using enterprise software deployment systems. When deployed from the ASA, remote users make an initial SSL connection to the ASA by entering the IP address or DNS name in the browser of an ASA configured to accept clienteless SSL VPN connections. The ASA then presents a login screen in the browser window, if the user satisfies the login and authentication, it downloads the client that matches the computer operating system. After downloading, the client installs and configures itself and establishes an IPsec (IKEv2) or SSL connection to the ASA.

For information about requirements for Cisco Adaptive Security Appliance and Cisco AnyConnect Secure Mobility Client, see the *Software Requirements* topic.

Related Topics

Navigating the Cisco ASA Series Documentation
Cisco AnyConnect Secure Mobility Client

Deployment with Single Sign-On

You can enable your services with Security Assertion Markup Language (SAML) single sign-on (SSO). SAML SSO can be used in on-premises, cloud, or hybrid deployments.

The following steps describe the sign-in flow for SAML SSO after your users start their Cisco Jabber client:

1. The user starts the Cisco Jabber client. If you configure your Identity Provider (IdP) to prompt your users to sign in using a web form, the form is displayed within the client.
2. The Cisco Jabber client sends an authorization request to the service that it is connecting to, such as Webex Messenger service, Cisco Unified Communications Manager, or Cisco Unity Connection.
3. The service redirects the client to request authentication from the IdP.
4. The IdP requests credentials. Credentials can be supplied in one of the following methods:
    - Form-based authentication that contains username and password fields.
    - Kerberos for Integrated Windows Authentication (IWA) (Windows only)
    - Smart card authentication (Windows only)
    - Basic HTTP authentication method in which client offers the username and password when making an HTTP request.
5. The IdP provides a cookie to the browser or other authentication method. The IdP authenticates the identity using SAML, which allows the service to provide the client with a token.
6. The client uses the token for authentication to log in to the service.

Authentication Methods

The authentication mechanism impacts how a user signs on. For example, if you use Kerberos, the client does not prompt users for credentials, because your users already provided authentication to gain access to the desktop.

User Sessions

Users sign in for a *session*, which gives them a predefined period to use Cisco Jabber services. To control how long sessions last, you configure cookie and token timeout parameters.

Configure the IdP timeout parameters with an appropriate amount of time to ensure that users are not prompted to log in. For example, when Jabber users switch to an external Wi-Fi, are roaming, their laptops hibernate, or their laptop goes to sleep due to user inactivity. Users will not have to log in after resuming the connection, provided the IdP session is still active.

When a session has expired and Jabber is not able to silently renew it, because user input is required, the user is prompted to reauthenticate. This can occur when the authorization cookie is no longer valid.

If Kerberos or a Smart card is used, no action is needed to reauthenticate, unless a PIN is required for the Smart card; there is no risk of interruption to services, such as voicemail, incoming calls, or instant messaging.

Single Sign-On Requirements

SAML 2.0

Use SAML 2.0 to enable single sign-on (SSO) for Cisco Jabber clients using Cisco Unified Communications Manager services. SAML 2.0 isn't compatible with SAML 1.1. Select an IdP that uses the SAML 2.0 standard. Since the supported identity providers are compliant with SAML 2.0, you can use them to implement SSO.

Supported Identity Providers

We support IdPs that are Security Assertion Markup Language (SAML) compliant. We have tested the following identity providers:

- Ping Federate 6.10.0.4
- Microsoft Active Directory Federation Services (ADFS) 2.0
- Open Access Manager (OpenAM) 10.1

Note Ensure that you configure Globally Persistent cookies for use with OpenAM.

When you configure the IdP, the configured settings impact how you sign into the client. Parameters, such as the cookie type (persistent or session) or the authentication mechanism (Kerberos or Web form), determine how often you have to authenticate.

Cookies

To enable cookie sharing with the browser, use persistent cookies and not session cookies. Persistent cookies prompt the user to enter credentials one time in the client or in any other desktop application that uses Internet Explorer. Session cookies require that users enter their credentials every time that they launch the client. You configure persistent cookies as a setting on the IdP. If you're using Open Access Manager as your IdP, configure Globally Persistent cookies (and not Realm Specific Persistent Cookies).

When a user has successfully signed in to Cisco Jabber for iPhone and iPad using SSO credentials, cookies are saved in the iOS keychain by default. If cookies are in the iOS keychain, users don't need to enter sign in credentials for the next sign-in, unless the cookie expires during sign in. Cookies are deleted from iOS keychain in the following scenarios:

- Manually sign out of Cisco Jabber.
- Cisco Jabber is reset.
- After rebooting the iOS device
- Cisco Jabber is closed manually.

Note If you use the embedded Safari browser, Jabber can't control the cookies that Safari controls. Because Jabber can't clear these cookies, Jabber can only clear the SSO token in this case. If Safari has the user credentials in a persistent cookie, the cookie allows the user to avoid reentering their credentials when Jabber clears the SSO token.

If the iOS system stops Cisco Jabber for iPhone and iPad in the background, Jabber allows users to automatically sign in without entering a password.

Required Browsers

To share the authentication cookie (issued by IdP) between the browser and the client, specify one of the following browsers as your default browser:

Product	Required Browser
Cisco Jabber for Windows	Internet Explorer
Cisco Jabber for Mac	Safari
Cisco Jabber for iPhone and iPad	Safari
Cisco Jabber for Android	Chrome or Internet Explorer

Note An embedded browser can’t share a cookie with an external browser when using SSO with Cisco Jabber for Android.

Single Sign-On and Remote Access

For users that provide their credentials from outside the corporate firewall using Expressway Mobile and Remote Access, single sign-on has the following restrictions:

- Single sign-on (SSO) is available with Cisco Expressway 8.5 and Cisco Unified Communications Manager release 10.5.2 or later. You must either enable or disable SSO on both.
- You can't use SSO over the Expressway for Mobile and Remote Access on a secure phone.
- The Identity Provider used must have the same internal and external URL. If the URL is different, the user may be prompted to sign in again when changing between inside and outside the corporate firewall.