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

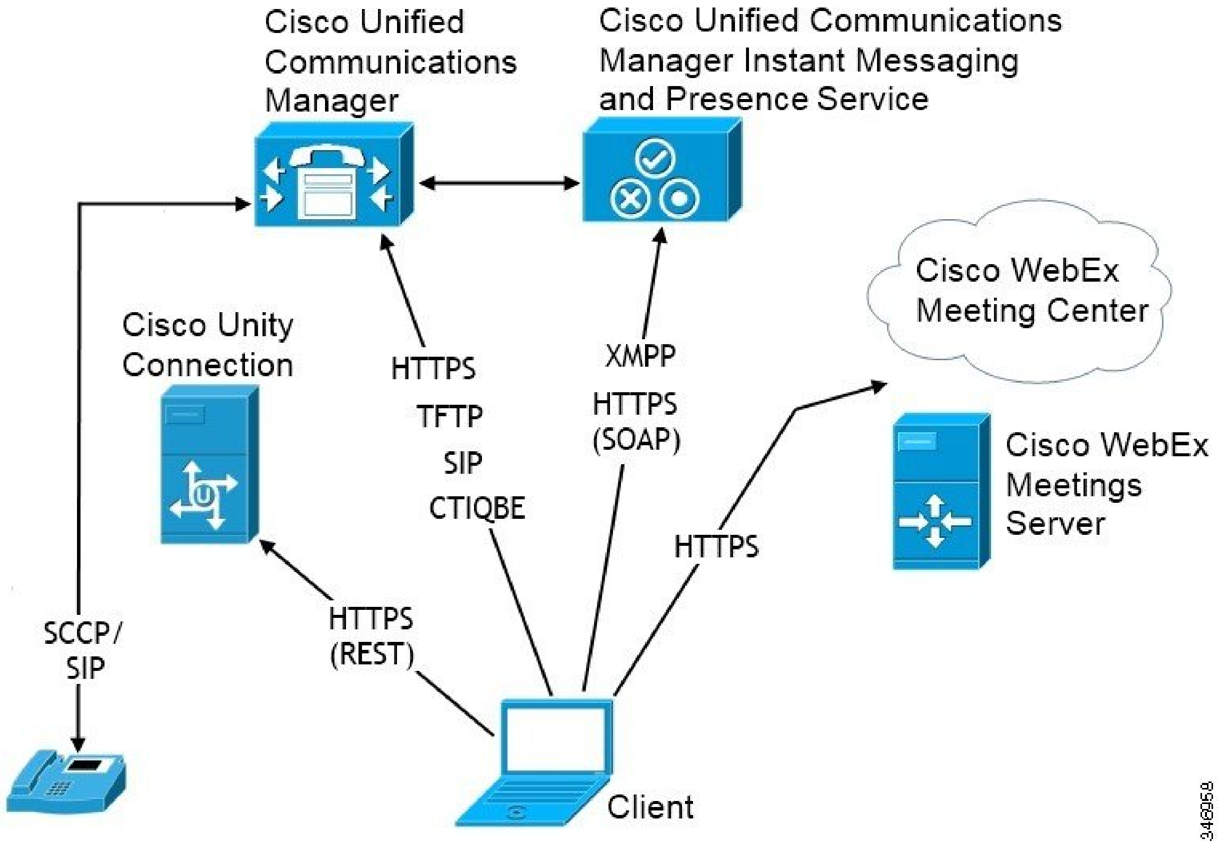
The following services are available in an on-premises deployment with Cisco Unified Communications Manager IM and Presence Service:

- **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:
  - Cisco Webex Meetings Center—Provides hosted meeting capabilities.
  - Cisco 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


Cisco Unified Communications Manager
Cisco Unified Communications Manager Instant Messaging and Presence Service
Cisco WebEx Meeting Center
Cisco Unity Connection
HTTPS
TFTP
SIP
CTIQBE
XMPP
HTTPS (SOAP)
Cisco WebEx Meetings Server
HTTPS
SCCP/ SIP
HTTPS (REST)
Client
346958

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

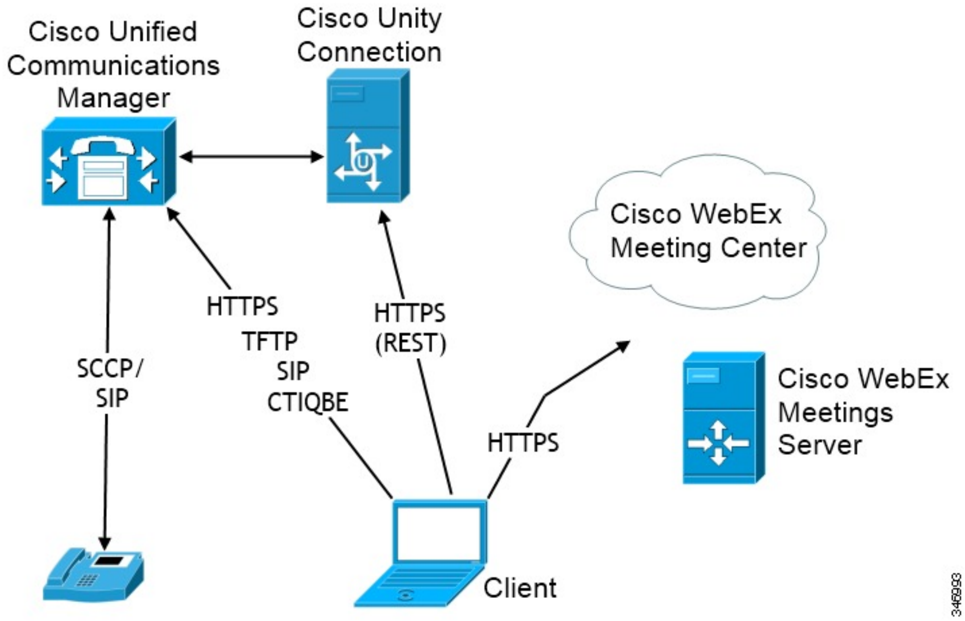
The following services are available in a phone mode deployment:

- **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:
  - **Cisco Webex Meetings Center**—Provides hosted meeting capabilities.
  - **Cisco 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


Cisco Unified Communications Manager
Cisco Unity Connection
Cisco WebEx Meeting Center
HTTPS
TFTP
SIP
CTIQBE
HTTPS (REST)
SCCP/ SIP
HTTPS
Cisco WebEx Meetings Server
Client
346093

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.

Cloud-Based Deployments

A cloud-based deployment is one in which Cisco Webex hosts services. You manage and monitor your cloud-based deployment with the Cisco Webex Administration Tool.

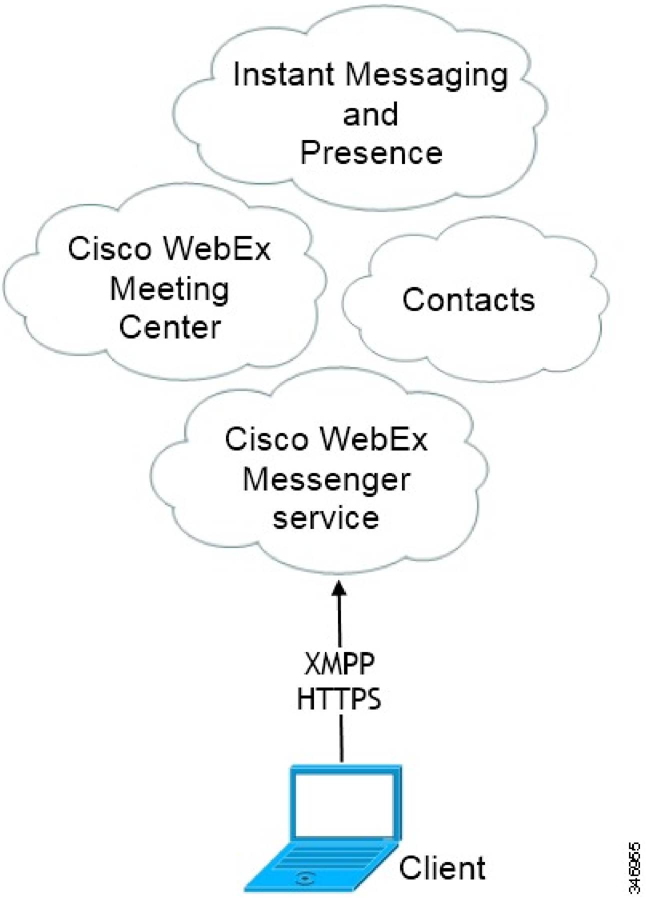
Cloud-Based Deployment

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

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

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

Figure 3: Cloud-Based Deployment


Instant Messaging and Presence
Cisco WebEx Meeting Center
Contacts
Cisco WebEx Messenger service
XMPP
HTTPS
Client
346955

Hybrid Cloud-Based Deployment

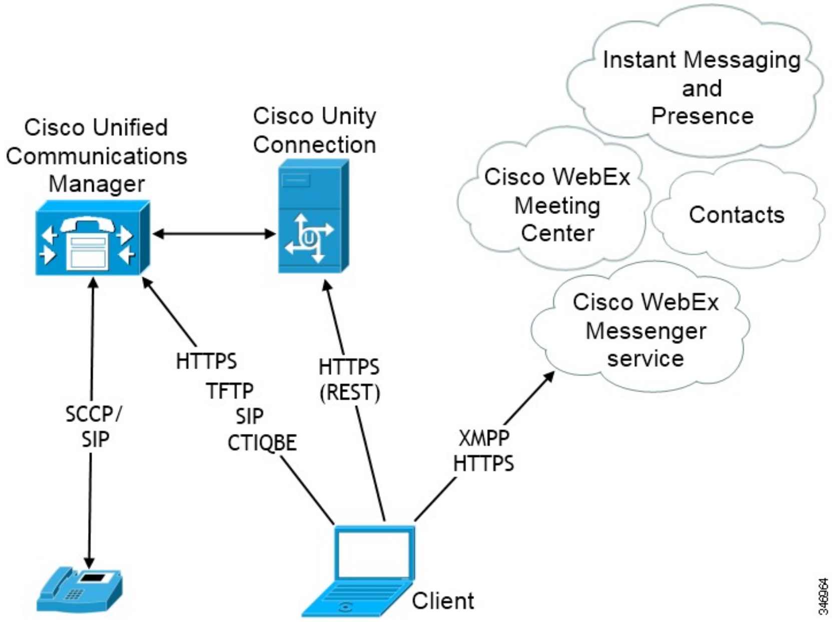
The following services are available in a hybrid cloud-based deployment:

- **Contact Source**—The Cisco Webex Messenger service provides contact resolution.

- **Presence**—The Cisco Webex Messenger service allows users to publish their availability and subscribe to other users' availability.
- **Instant Messaging**—The Cisco 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**—Cisco 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.

Figure 4: Hybrid Cloud-Based Deployment


Instant Messaging and Presence
Cisco Unified Communications Manager
Cisco Unity Connection
Cisco WebEx Meeting Center
Contacts
Cisco WebEx Messenger service
HTTPS
TFTP
SIP
CTIQBE
HTTPS (REST)
SCCP/ SIP
XMPP HTTPS
Client
346964

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

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

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, you should 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.

Remote Access

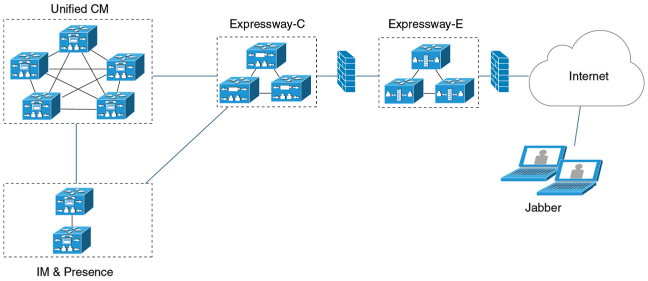
Your users may need to access their work from a location that's outside the corporate network. You can provide them access to their work using one of the Cisco products for remote access.

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 5: 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.



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	
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	

Service	Supported	Unsupported
Instant Messaging and Presence		
On-premises	X	
Cloud	X	
Chat	X	
Group 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
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

Service	Supported	Unsupported
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.	
Voicemail		
Visual voicemail	X * Using HTTP white list on Cisco Expressway-C	
Cisco Webex Meetings		
On-premises		X
Cloud	X	
Cisco Webex screen share (desktop clients only)	X	
Installation (Desktop clients)		
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		
End-to-end encryption	X	

Service	Supported	Unsupported
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	

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 Cisco 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.

Cisco Webex Meetings

When the client connects to services using Expressway for Mobile and Remote Access, it supports only cloud-based conferencing using Cisco Webex Meetings Center. The client cannot access the Cisco Webex Meetings Server or join or start on-premises Cisco Webex Meetings.

When users use the Cisco Webex Meetings Servers for meetings or the meeting siteType is ORION, the client cannot access the Cisco Webex Meetings Server, and join or start on-premises Cisco Webex Meetings over Mobile and Remote Access (MRA).

To use the Webex Meetings option in Cisco Jabber for Android, ensure that the meeting client is installed before installing Cisco Jabber for Android.

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.
- Single Sign-On (SSO) — If you have SSO enabled for your on-premises deployment, it also applies to your Expressway for Mobile and Remote access deployment. If you disable SSO, it is disabled for both on-premises and Expressway for Mobile and Remote access deployments.

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 Cisco 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

You must use SAML 2.0 to enable single sign-on (SSO) for Cisco Jabber clients using Cisco Unified Communications Manager services. SAML 2.0 is not compatible with SAML 1.1. You must select an IdP that uses the SAML 2.0 standard. The supported identity providers have been tested to be compliant with SAML 2.0 and can be used to implement SSO.

Supported Identity Providers

The IdP must be Security Assertion Markup Language (SAML) compliant. The clients support 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. Some parameters, such as the type of cookie (persistent or session), or the authentication mechanism (Kerberos or Web form), determine how often you have to be authenticated.

Cookies

To enable cookie sharing with the browser, you must 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 the client is launched.

You configure persistent cookies as a setting on the IdP. If you are using Open Access Manager as your IdP, you must 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

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

Required Browsers

To share the authentication cookie (issued by IdP) between the browser and the client, you must 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 cannot 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.
- 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 from inside to outside the corporate firewall and vice versa.