Deployment Options

Learn about options for deploying Cisco Jabber.

On-Premises Deployments

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

Product Modes

For all deployments, the user's primary authentication is to a presence server. You must provision users with instant messaging and presence capabilities as the base for your deployment. You can then provision users with additional services, depending on your requirements.

Full UC

To deploy full UC, you enable instant messaging and presence capabilities. You then provision users with devices for audio and video in addition to voicemail and conferencing capabilities.

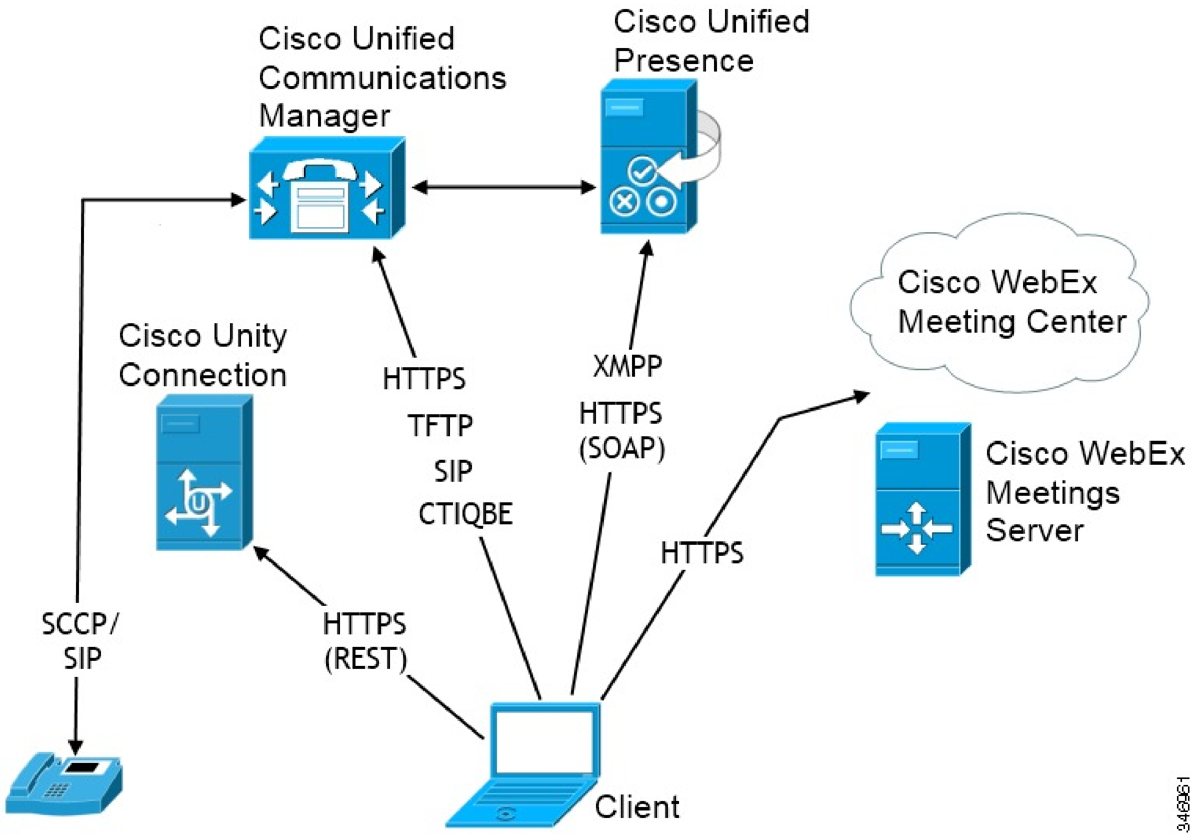
Default Mode Diagrams

Review architecture diagrams for on-premise deployments in the default product mode.

Diagram with Cisco Unified Presence

The following diagram illustrates the architecture of an on-premise deployment that includes Cisco Unified Presence:

Figure 1: On-Premise architecture



The following are the services available in an on-premise deployment:

Presence

Users can publish their availability and subscribe to other users' availability through Cisco Unified Presence.

Instant Messaging

Users send and receive instant messages through Cisco Unified Presence.

Audio Calls

Users place audio calls through desk phone devices or on their computers through Cisco Unified Communications Manager.

Video

Users place video calls through Cisco Unified Communications Manager.

Voicemail

Users send and receive voice messages through Cisco Unity Connection.

Conferencing

Integrate with one of the following:

Cisco WebEx Meeting Center

Provides hosted meeting capabilities.

Cisco WebEx Meetings Server

Provides on-premise meeting capabilities.

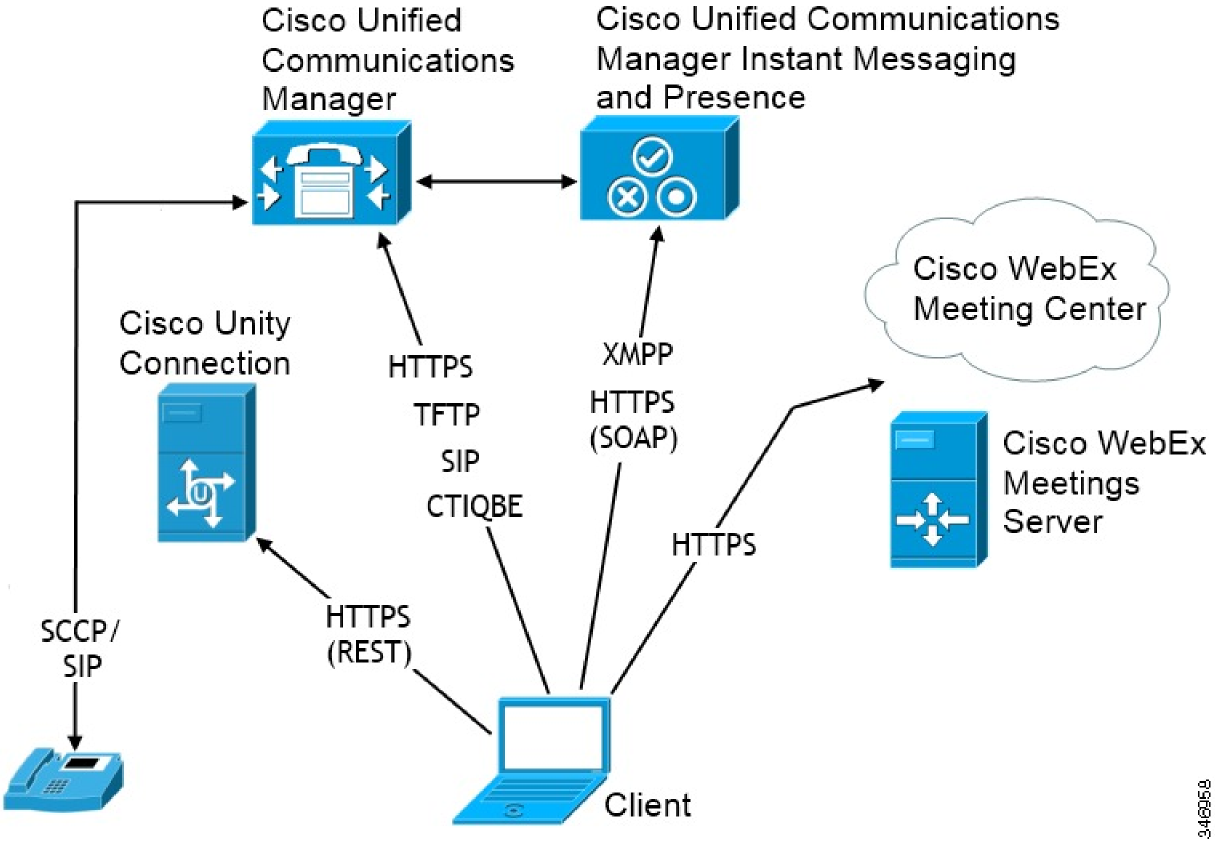
Related Topics

Integrate with Directory Sources

Diagram with Cisco Unified Communications IM and Presence

The following diagram illustrates the architecture of an on-premise deployment that includes Cisco Unified Communications IM and Presence:

Figure 2: On-Premise architecture


Cisco Unified Communications Manager
Cisco Unified Communications Manager Instant Messaging and Presence
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

The following are the services available in an on-premise deployment:

Presence

Users can publish their availability and subscribe to other users' availability through Cisco Unified Communications IM and Presence.

Instant Messaging

Users send and receive instant messages through Cisco Unified Communications IM and Presence.

Audio Calls

Users place audio calls through desk phone devices or on their computers through Cisco Unified Communications Manager.

Video

Users place video calls through Cisco Unified Communications Manager.

Voicemail

Users send and receive voice messages through Cisco Unity Connection.

Conferencing

Integrate with one of the following:

Cisco WebEx Meeting Center

Provides hosted meeting capabilities.

Cisco WebEx Meetings Server

Provides on-premise meeting capabilities.

Related Topics

Integrate with Directory Sources

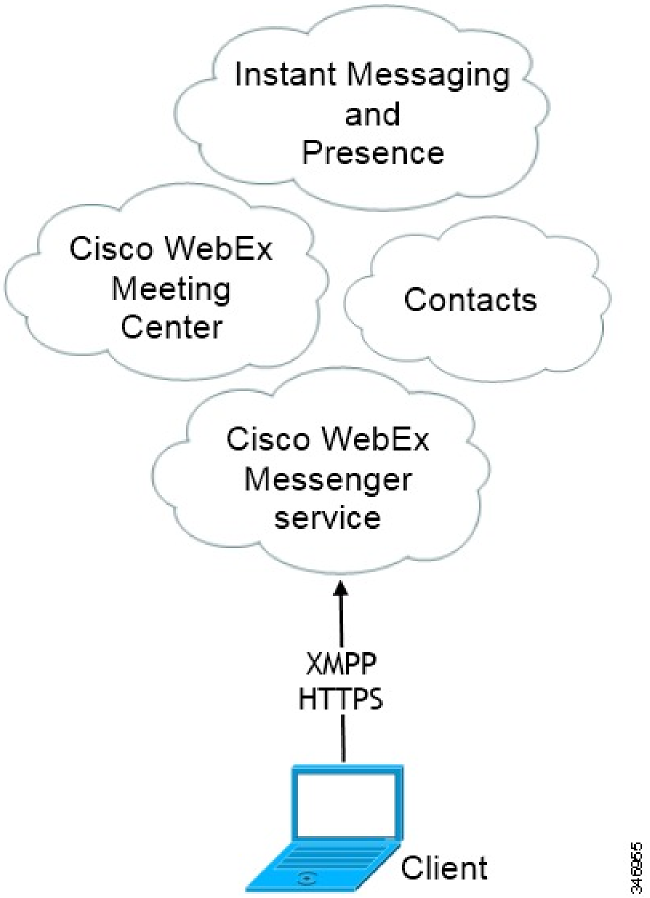
Cloud-Based Deployments

In cloud-based deployments, the user's primary authentication is to the Cisco WebEx Messenger service. Cisco WebEx hosts all services. You manage and monitor cloud-based deployments with the Cisco WebEx Administration Tool.

Cloud-Based Diagram

The following diagram illustrates the architecture of a cloud-based deployment:

Figure 3: Cloud-Based architecture


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

The following are the services 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.

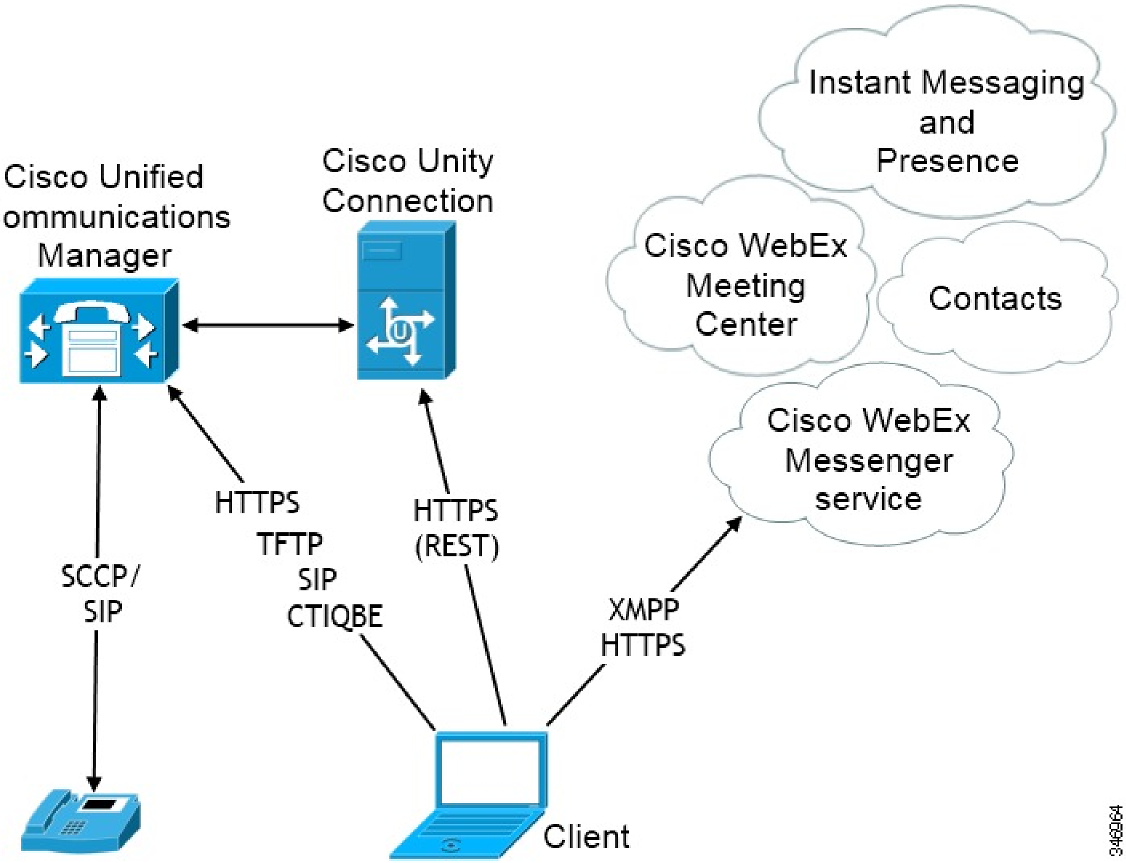
Conferencing

Cisco WebEx Meeting Center provides hosted meeting capabilities.

Hybrid Cloud-Based Diagram

The following diagram illustrates the architecture of a hybrid cloud-based deployment:

Figure 4: Hybrid cloud-based architecture


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

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

Contact Source

The Cisco WebEx Messenger service provides contact resolution.

Presence

The Cisco WebEx Messenger service lets users can 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 Meeting Center provides hosted meeting capabilities.

Audio Calls

Users place audio calls through desk phone devices or on their computers through Cisco Unified Communications Manager.

Video

Users place video calls through Cisco Unified Communications Manager.

Voicemail

Users send and receive voice messages through Cisco Unity Connection.

How the Client Connects to Services

To connect to services, Cisco Jabber requires the following information:

- Source of authentication that enables users to sign in to the client.
- Location of services.

You can provide that information to the client with the following methods:

URL Configuration

Users are sent an email from their administrators. The email contains a URL that will configure the domain needed for service discovery.

Service Discovery

The client automatically locates and connects to services.

Manual Connection Settings

Users manually enter connection settings in the client user interface.

Recommended Connection Methods

The method you should use to provide the client with the information it needs to connect to services depends on your deployment type, server versions, and product modes. The following tables highlight various deployment methods and how to provide the client with the necessary information.

On-Premises Deployments for Cisco Jabber for Mac

Product Mode	Server Versions	Discovery Method
Full UC (Default Mode)	Version 9 and higher: • Cisco Unified Communications Manager • Cisco Unified Communications Manager IM and Presence Service	A DNS SRV request against `_cisco-uds.<domain>`
Full UC (Default Mode)	Version 8.x: • Cisco Unified Communications Manager • Cisco Unified Presence	A DNS SRV request against `_cuplogin.<domain>`

Hybrid Cloud-Based Deployments

Server Versions	Connection Method
Cisco WebEx Messenger	HTTPS request against `http://loginp.webexconnect.com/cas/FederatedSSO?org=<domain>`

Cloud-Based Deployments

Deployment Type	Connection Method
Enabled for single sign-on (SSO)	Cisco WebEx Administration Tool
Not enabled for SSO	Cisco WebEx Administration Tool

Sources of Authentication

A source of authentication, or an authenticator, enables users to sign in to the client.

There are three possible sources of authentication, as follows:

Cisco Unified Presence

On-premises deployments in either full UC or IM only.

Cisco Unified Communications Manager

On-premises deployments in phone mode.

Cisco WebEx Messenger Service

Cloud-based or hybrid cloud-based deployments.

How the Client Gets an Authenticator

Cisco Jabber looks for an authenticator as follows:

1. Client checks cache for manual settings.

   Users can manually enter authenticator through the client user interface.

2. Client checks cache to discover if the user's domain is a Webex organisation..

   The client chooses Webex as the authenticator.

3. Client makes a Webex cloud service HTTP request to discover if the user's organisation domain is a Webex organisation.

   The client chooses Webex as the authenticator.

4. Client checks cache for service discovery.

   The client loads settings from previous queries for service (SRV) records.

5. Client queries for SRV records.

   The client queries the DNS name server for SRV records to locate services.

   If the client finds the `_cisco-uds` SRV record, it can get the authenticator from the service profile.

If the client cannot get an authenticator, it prompts the user to manually select the source of authentication in the client user interface.

Service Discovery

Service discovery enables clients to automatically detect and locate services on your enterprise network. Clients query domain name servers to retrieve service (SRV) records that provide the location of servers.

The primary benefits to using service discovery are:

- Speeds time to deployment.
- Allows you to centrally manage server locations.

Important Migrating from Cisco Unified Presence 8.x to Cisco Unified Communications IM and Presence 9.0 or later.

You must specify the Cisco Unified Presence server FQDN in the migrated UC service on Cisco Unified Communications Manager. Open **Cisco Unified Communications Manager Administration** interface. Select **User Management > User Settings > UC Service**.

For UC services with type **IM and Presence**, when you migrate from Cisco Unified Presence 8.x to Cisco Unified Communications IM and Presence the **Host Name/IP Address** field is populated with a domain name and you must change this to the Cisco Unified Presence server FQDN.

However, the client can retrieve different SRV records that indicate to the client different servers are present and different services are available. In this way, the client derives specific information about your environment when it retrieves each SRV record.

The following table lists the SRV records you can deploy and explains the purpose and benefits of each record:

SRV Record	Purpose	Why You Deploy
`_cisco-uds`	Provides the location of Cisco Unified Communications Manager version 9.0 and higher. The client can retrieve service profiles from Cisco Unified Communications Manager to determine the authenticator.	• Eliminates the need to specify installation arguments. • Lets you centrally manage configuration in UC service profiles. • Enables the client to discover the user's home cluster. As a result, the client can automatically get the user's device configuration and register the devices. You do not need to provision users with CCMCIP profiles or TFTP server addresses. • Supports mixed product modes. You can easily deploy users with full UC, IM only, or phone mode capabilities. • Supports Expressway for Mobile and Remote Access.
`_cuplogin`	Provides the location of Cisco Unified Presence. Sets Cisco Unified Presence as the authenticator.	• Supports deployments with Cisco Unified Communications Manager and Cisco Unified Presence version 8.x. • Supports deployments where all clusters have not yet been upgraded to Cisco Unified Communications Manager 9.

SRV Record	Purpose	Why You Deploy
`_collab-edge`	Provides the location of Cisco VCS Expressway or Cisco Expressway-E. The client can retrieve service profiles from Cisco Unified Communications Manager to determine the authenticator.	• Supports deployments with Expressway for Mobile and Remote Access.

How the Client Locates Services

The following steps describe how the client locates services with SRV records:

1. Client's host computer or device gets a network connection.

   When the client's host computer gets a network connection, it also gets the address of a DNS name server from the DHCP settings.

2. The user employs one of the following methods to discover the service during the first sign-in:

   Manual

   The user starts Cisco Jabber and then inputs an email-like address on the welcome screen.

URL Configuration

URL configuration allows users to click on a link to cross-launch Cisco Jabber without manually inputting an email.

To create a URL configuration link, you include:

ServicesDomain

The domain that Cisco Jabber uses for service discovery.

VoiceServiceDomain

For a hybrid deployment, the domain that Cisco Jabber uses to retrieve the DNS SRV records can be different from the ServicesDomain that is used to discover Cisco WebEx domain.

ServiceDiscoveryExcludedServices

In certain deployment scenarios services can be excluded from the service discovery process. These values can be a combination of the following:

- WEBEX
- CUCM
- CUP

Note When all three parameters are included, service discovery will not happen and the user will be prompted to manually enter connection settings.

Create the link in the following format:

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

Examples:

- `ciscojabber://provision?servicesdomain=example.com`
- `ciscojabber://provision?servicesdomain=example.com &VoiceServicesDomain=VoiceServices.example.com`
- `ciscojabber://provision?servicesdomain=example.com &ServiceDiscoveryExcludeServices=WEBEX,CUP`

Provide the link to users using email or a web site.

Note If your organization uses a mail application that supports cross launching proprietary protocols or custom links, you can provide the link to users using email, otherwise provide the link to users using a web site.

3 The client gets the address of the DNS name server from the DHCP settings.

4 The client issues an HTTP query to a CAS URL for the Cisco WebEx Messenger service.

This query enables the client to determine if the domain is a valid Cisco WebEx domain.

5 The client queries the name server for the following SRV records in order of priority:

- `_cisco-uds`
- `_cuplogin`
- `_collab-edge`

The client caches the results of the DNS query to load on subsequent launches.

The following is an example of an SRV record entry:

```
_cuplogin._tcp.DOMAIN SRV service location:
 priority = 0
 weight = 0
 port = 8443
 svr hostname=192.168.0.26
```

Client Issues HTTP Query

In addition to querying the name server for SRV records to locate available services, the client sends an HTTP query to the CAS URL for the Cisco WebEx Messenger service. This request enables the client to determine cloud-based deployments and authenticate users to the Cisco WebEx Messenger service.
When the client gets a domain from the user, it appends that domain to the following HTTP query:

`http://loginp.webexconnect.com/cas/FederatedSSO?org=`

For example, if the client gets `example.com` as the domain from the user, it issues the following query:

`http://loginp.webexconnect.com/cas/FederatedSSO?org=example.com`

That query returns an XML response that the client uses to determine if the domain is a valid Cisco WebEx domain.

If the client determines the domain is a valid Cisco WebEx domain, it prompts users to enter their Cisco WebEx credentials. The client then authenticates to theCisco WebEx Messenger service and retrieves configuration and UC services configured in Cisco WebEx Org Admin.

If the client determines the domain is not a valid Cisco WebEx domain, it uses the results of the query to the name server to locate available services.

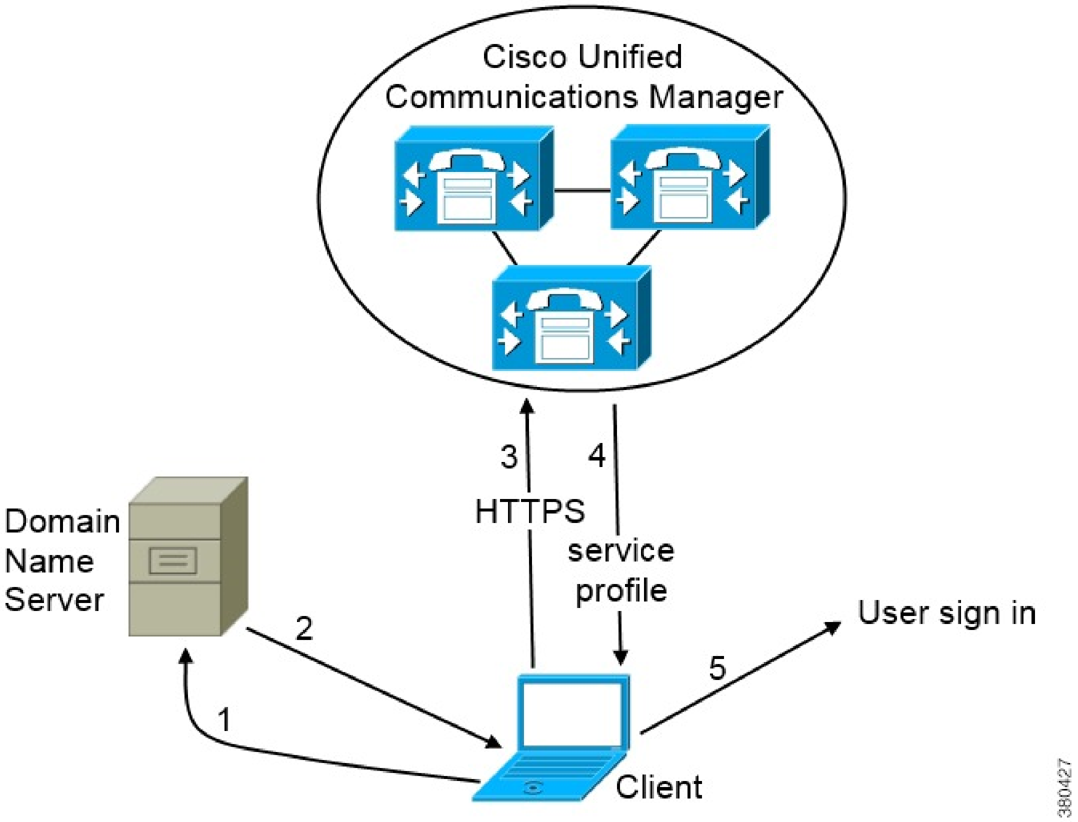
Note The client will use any configured system proxies when sending the HTTP request to the CAS URL. Proxy support for this request has the following limitations :

- Proxy Authentication is not supported.
- Wildcards in the bypass list are not supported. Use `example.com` instead of `*.example.com` for example.

Cisco UDS SRV Record

In deployments with Cisco Unified Communications Manager version 9 and higher, the client can automatically discover services and configuration with the following SRV record: `_cisco-uds`.

The following image illustrates how the client uses the `_cisco-uds` SRV record:



1 The client queries the domain name server for SRV records.

2 The name server returns the `_cisco-uds` SRV record.

3 The client locates the user's home cluster.

As a result of automatically locating the user's home cluster, the client can retrieve the device configuration for the user and automatically register telephony services.

Important In an environment with multiple Cisco Unified Communications Manager clusters, you can configure the Intercluster Lookup Service (ILS). ILS enables the client to find the user's home cluster and discover services.

If you do not configure ILS, then you must manually configure remote cluster information, similar to the EMCC remote cluster set up. For more information on Remote Cluster Configuration, see the Cisco Unified Communications Manager Features and Services Guide.

4 The client retrieves the user's service profile.

The user's service profile contains the addresses and settings for UC services and client configuration.

The client also determines the authenticator from the service profile.

5 The client signs the user in to the authenticator.

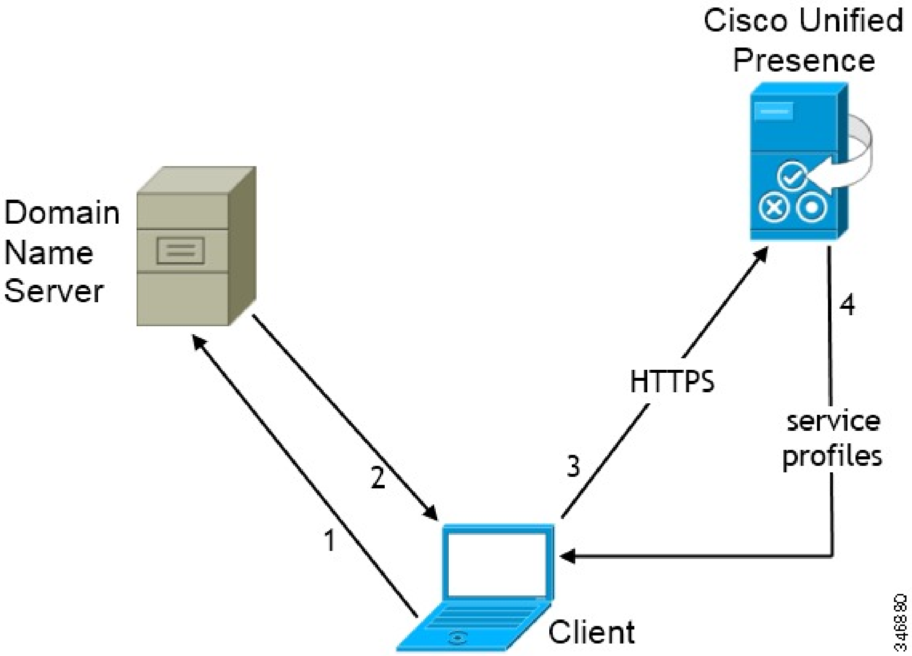
The following is an example of the `_cisco-uds` SRV record:

```
_cisco-uds._tcp.example.com     SRV service location:
          priority       = 6
          weight         = 30
          port           = 8443
          svr hostname   = cucm3.example.com
_cisco-uds._tcp.example.com     SRV service location:
          priority       = 2
          weight         = 20
          port           = 8443
          svr hostname   = cucm2.example.com
_cisco-uds._tcp.example.com     SRV service location:
          priority       = 1
          weight         = 5
          port           = 8443
          svr hostname   = cucm1.example.com
```

CUP Login SRV Record

Cisco Jabber can automatically discover and connect to Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service with the following SRV record: `_cuplogin`.

The following image illustrates how the client uses the `_cuplogin` SRV record:



1 The client queries the domain name server for SRV records.

2 The name server returns the `_cuplogin` SRV record.

As a result, Cisco Jabber can locate the presence server and determine that Cisco Unified Presence is the authenticator.

3 The client prompts the user for credentials and authenticates to the presence server.

4 The client retrieves service profiles from the presence server.

Tip The `_cuplogin` SRV record also sets the default server address on the **Advanced Settings** window.

The following is an example of the `_cuplogin` SRV record:

```
_cuplogin._tcp.example.com      SRV service location:
          priority       = 8
          weight         = 50
          port           = 8443
          svr hostname   = cup3.example.com
_cuplogin._tcp.example.com      SRV service location:
          priority       = 5
          weight         = 100
          port           = 8443
          svr hostname   = cup1.example.com
_cuplogin._tcp.example.com      SRV service location:
          priority       = 7
          weight         = 4
          port           = 8443
          svr hostname   = cup2.example.com
```

Manual Connection Settings

Manual connection settings provide a fallback mechanism for Service Discovery in situations where Service Discovery has not been deployed.

When you launch Cisco Jabber, you can specify the authenticator and server addresses in the **Advanced Settings** window. The client then caches the server addresses to the local application configuration that it loads on subsequent launches.

Cisco Jabber prompts users to enter settings in the **Advanced Settings** window on the initial launch as follows:

On-Premises with Cisco Unified Communications Manager Version 9.x and Higher

If the client cannot get the authenticator and server addresses from the service profile.

Cloud-Based or On-Premises with Cisco Unified Communications Manager Version 8.x

The client also prompts users to enter server addresses in the **Advanced Settings** window if you do not set server addresses with SRV records.

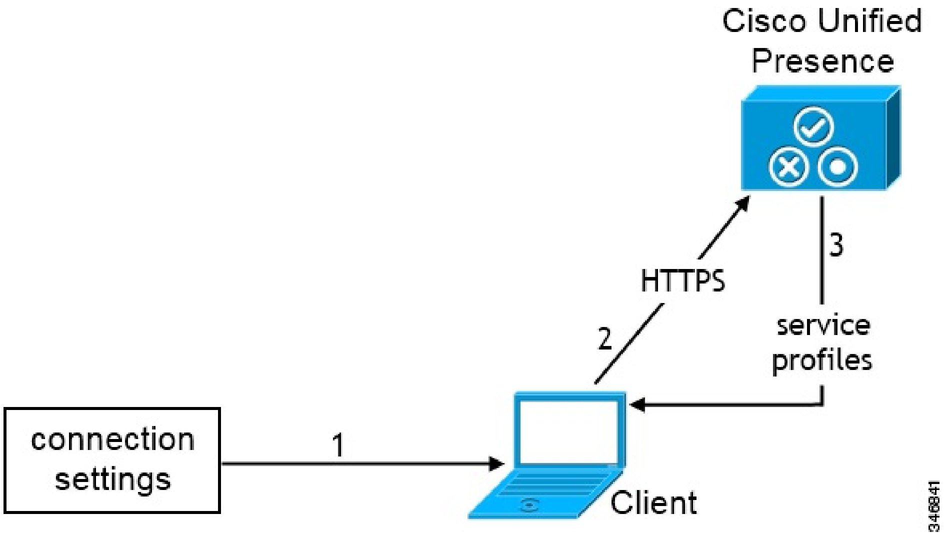
Settings that you enter in the **Advanced Settings** window take priority over any other sources including SRV records.

Manual Connection Settings for On-Premises Deployments

Users can set Cisco Unified Presence as the authenticator and specify the server address in the **Advanced Settings** window.

Remember You can automatically set the default server address with the `_cuplogin` SRV record.

The following diagram illustrates how the client uses manual connection settings in on-premises deployments:



1 Users manually enter connection settings in the **Advanced Settings** window.

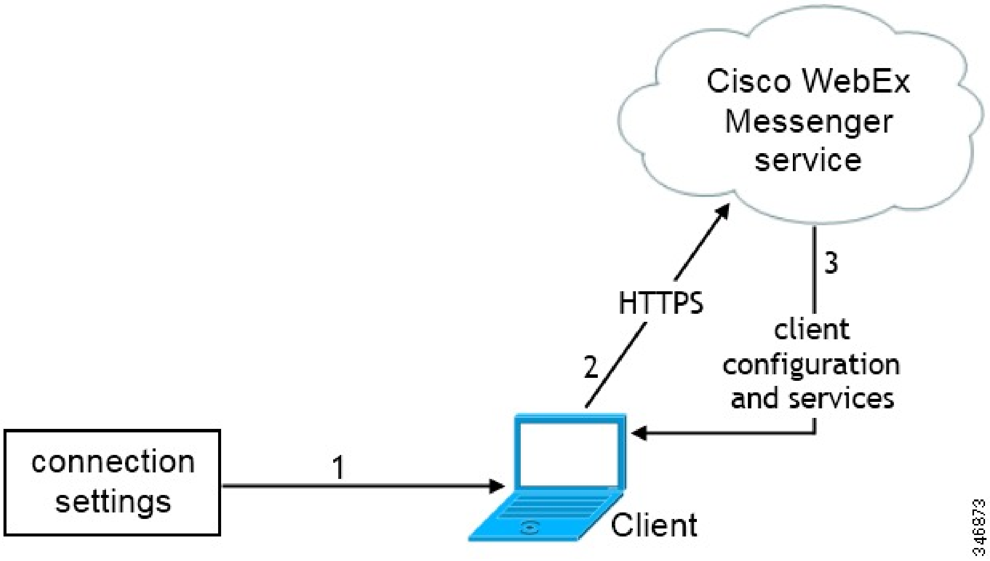
2 The client authenticates to Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service.

3 The client retrieves service profiles from the presence server.

Manual Connection Settings for Cloud-Based Deployments

Users can set the Cisco WebEx Messenger service as the authenticator and specify the CAS URL for login in the **Advanced Settings** window.

The following diagram illustrates how the client uses manual connection settings in cloud-based deployments:


Cisco WebEx Messenger service
HTTPS
2
3
client configuration and services
connection settings
1
Client
346873

1 Users manually enter connection settings in the **Advanced Settings** window.

2 The client authenticates to the Cisco WebEx Messenger service.

3 The client retrieves configuration and services.

Manual Connection Settings for Service Discovery

Users can select the **Automatic** option in the **Advanced Settings** window to discover servers automatically.

This option lets users change from manually setting the service connection details to using service discovery. For example, on the initial launch, you manually set the authenticator and specify a server address in the **Advanced Settings** window.

The client always checks the cache for manual settings. The manual settings also take higher priority over SRV records. For this reason, if you decide to deploy SRV records and use service discovery, you must override the manual settings from the initial launch.

Expressway for Mobile and Remote Access Deployments

Expressway for Mobile and Remote Access for Cisco Unified Communications Manager allows users to access their collaboration tools from outside the corporate firewall without a VPN client. 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.

You must do the following to set up the Expressway for Mobile and Remote Access feature:

1 Set up servers to support Expressway for Mobile and Remote Access using Cisco Expressway-E and Cisco Expressway-C.*

   a See the following documents to set up the Cisco Expressway servers:

   - *Cisco Expressway Basic Configuration Deployment Guide*
   - *Mobile and Remote Access via Cisco Expressway Deployment Guide*

   * If you currently deploy a Cisco TelePresence Video Communication Server (VCS) environment, you can set up Expressway for Mobile and Remote Access. For more information, see *Cisco VCS Basic Configuration (Control with Expressway) Deployment Guide* and *Mobile and Remote Access via Cisco VCS Deployment Guide*.

   b Add any relevant servers to the whitelist for your Cisco Expressway-C server to ensure that the client can access services that are located inside the corporate network.

   To add a server to the Cisco Expressway-C whitelist, use the **HTTP server allow** setting.

   This list can include the servers on which you host voicemail or contact photos.

2 Configure an external DNS server that contains the `_collab-edge` DNS SRV record to allow the client locate the Expressway for Mobile and Remote Access server.

3 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.

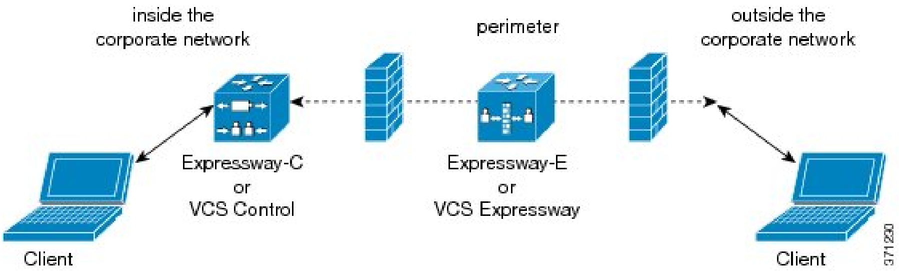
   The Voice Services Domain allows the client to locate the DNS server that contains the`_collab-edge` record.

Important In most cases, 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, users must perform initial sign in while on the corporate network:

- If the voice services domain is different from the services domain. In this case, users must be inside the corporate network to get the correct voice services domain from the jabber-config.xml file.
- If the client needs to complete the CAPF enrollment process, which is required when using a secure or mixed mode cluster.

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

Figure 5: Cisco Jabber for Windows and Mac Architecture Diagram


inside the corporate network
perimeter
outside the corporate network
Expressway-C or VCS Control
Expressway-E or VCS Expressway
Client
Client
371230

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 whitelist on Cisco Expressway-C	

Service		Supported	Unsupported
	Intradomain federation	x * Contact search support depends of 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	
	High Availability: On-premises deployments	x	
	File Transfer: On-premises deployments		x
	File Transfer: Cloud deployments	x (Desktop clients only)	
Audio and Video			
	Audio and video calls	x * Cisco Unified Communications Manager 9.1(2) and later	
	Deskphone control mode (CTI)		x
	Extend and Connect		x
	Session persistency		x
	Early media		x
	Self Care Portal access		x
Voicemail			
	Visual voicemail	x * Using HTTP whitelist on Cisco Expressway-C	
Cisco WebEx Meetings			

Service		Supported	Unsupported
	On-premises		x
	Cloud	x	
	Cisco WebEx Desktop Share	x	
Security			
	End-to-end encryption		x
	CAPF enrollment		x
Troubleshooting			
	Problem report generation	x	
	Problem report upload		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 whitelist of your Cisco Expressway-C server. To add a server to Cisco Expressway-C whitelist, 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

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

The client does not support file transfer including screen capture with Cisco Unified Communications Manager IM and Presence Service deployments. File Transfer is supported only with Cisco WebEx cloud deployments with desktop clients.

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. Expressway for Mobile and Remote Access is not supported with Cisco Unified Communications Manager Version 8.x.

Deskphone control mode (CTI)

The client does not support deskphone control mode (CTI), including extension mobility.

Extend and Connect

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

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.

The 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 whitelist of your Cisco Expressway-C server. To add a server to Cisco Expressway-C whitelist, 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 Meeting Center.

The client cannot access the Cisco WebEx Meetings Server or join or start on-premises Cisco WebEx meetings.

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 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.

Troubleshooting

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.