Service Discovery

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.

Cisco Webex Platform Service Discovery

Cisco Jabber sends an HTTPS request to Cisco Webex Platform Service to check whether the user is enabled for team messaging mode. If the user is enabled for team messaging, then Jabber continues to check for available on-premises services.

Cisco Webex Messenger Service Discovery

Cisco Jabber sends a cloud HTTP request to the CAS URL for the Webex Messenger service. Cisco Jabber authenticates users with Webex Messenger Service and connects to the available services.

The services are configured on Webex Administration Tool.

Cisco Intercluster Lookup Service

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

Expressway for Mobile and Remote Access Service Discovery

Expressway for Mobile and Remote Access enables remote users access services.

The client queries the name server for SRV records. With the `_collab-edge` SRV record the client connects to the internal network through Expressway for Mobile and Remote Access and discover services.

The name server returns the `_collab-edge` SRV record and the client gets the location of the Cisco Expressway-E server. The Cisco Expressway-E server then provides the client with the results of the query to the internal name server. This must include the `_cisco-uds` SRV record, the client then retrieves the service profiles from Cisco Unified Communication Manager

Note When your voice service domain is the same as the sign-in domain, don't configure voiceservicesdomain for MRA. Only configure voiceservicesdomain when the domains are different.

Recommended Connection Methods

The method that 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.

Table 1: On-Premises Deployments for Cisco Jabber for Windows

Product Mode	Server Versions	Discovery Method	Non DNS SRV Record Method
Full UC (default mode)	Release 9.1.2 and later: • Cisco Unified Communications Manager • Cisco Unified Communications Manager IM and Presence Service	A DNS SRV request against `_cisco-uds .<domain>`	Use the following installer switches and values: • `AUTHENTICATOR=CUP` • `CUP_ADDRESS=` `<presence_server_address>`

Product Mode	Server Versions	Discovery Method	Non DNS SRV Record Method
IM Only (default mode)	Release 9 and later: Cisco Unified Communications Manager IM and Presence Service	A DNS SRV request against `_cisco-uds.<domain>`	Use the following installer switches and values: • `AUTHENTICATOR=CUP` • `CUP_ADDRESS=<presence_server_address>`
Phone Mode	Release 9 and later: Cisco Unified Communications Manager	A DNS SRV request against `_cisco-uds.<domain>`	Use the following installer switches and values: • `AUTHENTICATOR=CUCM` • `TFTP=<CUCM_address>` • `CCMCIP=<CUCM_address>` • `PRODUCT_MODE=phone_mode` High availability is not supported using this method of deployment.

Cisco Unified Communications Manager release 9.x and earlier—If you enable Cisco Extension Mobility, the `Cisco Extension Mobility` service must be activated on the Cisco Unified Communications Manager nodes that are used for CCMCIP. For information about Cisco Extension Mobility, see the *Feature and Services* guide for your Cisco Unified Communications Manager release.

Note Cisco Jabber release 9.6 and later can still discover full Unified Communications and IM-only services using the `_cuplogin` DNS SRV request but a `_cisco-uds` request will take precedence if it is present.

Use the SERVICES_DOMAIN installer switch to specify the value of the domain where DNS records reside if you want users to bypass the email screen during the first login of a fresh installation.

Table 2: On-Premises Deployments for Cisco Jabber for Mac

Product Mode	Server Versions	Discovery Method
Full UC (default mode)	Release 9 and later: • Cisco Unified Communications Manager • Cisco Unified Communications Manager IM and Presence Service	A DNS SRV request against `_cisco-uds.<domain>`

Table 3: On-Premises Deployments for Cisco Jabber for Android and Cisco Jabber for iPhone and iPad

Product Mode	Server Versions	Discovery Method
Full UC (default mode)	Release 9 and later: • Cisco Unified Communications Manager • Cisco Unified Communications Manager IM and Presence Service	A DNS SRV request against `_cisco-uds .<domain>` and `_cuplogin.<domain>`
IM Only (default mode)	Release 9 and later: Cisco Unified Communications Manager IM and Presence Service	A DNS SRV request against `_cisco-uds .<domain>` and `_cuplogin.<domain>`
Phone mode	Release 9 and later: Cisco Unified Communications Manager	A DNS SRV request against `_cisco-uds.<domain>`

Note Cisco Unified Communications Manager version 9 and later can still discover full Unified Communications and IM-only services using the `_cuplogin` DNS SRV request but a `_cisco-uds` request will take precedence if it is present.

Table 4: Hybrid Cloud-Based Deployments

Server Versions	Connection Method
Webex Messenger	HTTPS request against `https://loginp.webexconnect.com/cas/FederatedSSO?org=<domain>`
Cisco Webex Platform service	HTTPS request against `atlas-a.wbx2.com`

Table 5: Cloud-Based Deployments

Deployment Type	Connection Method
Enabled for single sign-on (SSO)	Webex Administration Tool Bootstrap file to set the SSO_ORG_DOMAIN argument.
Not enabled for SSO	Webex Administration Tool

Sources of Authentication

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

Three possible sources of authentication are as follows:

- Cisco Unified Communications Manager IM and Presence—On-premises deployments in either full UC or IM only.
- Cisco Unified Communications Manager—On-premises deployments in phone mode.
- Webex Messenger Service—Cloud-based or hybrid cloud-based deployments.
- Cisco Webex Platform Service—Cloud-based or hybrid cloud-based deployments.

How the Client Locates Services

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

1. The 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 Domain Name System (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.
   - Mobile Configuration Using Enterprise Mobility Management—As an alternative to URL configuration, you can configure Cisco Jabber using Enterprise Mobility Management (EMM) with Android for Work on Cisco Jabber for Android and with Apple Managed App Configuration on Cisco Jabber for iPhone and iPad. You need to configure the same parameters in the EMM console that are used for creating URL configuration link.

   To create a URL configuration link, you include the following:
   - ServicesDomain—The domain that Cisco Jabber uses for service discovery.
   - VoiceServicesDomain—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 the Cisco Jabber 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

Note When all three parameters are included, service discovery does not happen and the user is 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 &ServiceDiscoveryExcludedServices=WEBEX,CUCM`

Provide the link to users using email or a website.

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 website.

3. The client gets the address of the DNS name server from the DHCP settings.
4. The client issues an HTTP query to a Central Authentication Service (CAS) URL for the Webex Messenger service.

   This query enables the client to determine if the domain is a valid Webex domain.
5. The client queries the name server for the following SRV records in order of priority:
   - `_cisco-uds`
   - `_collab-edge`

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

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

The following is an example of an SRV record entry:

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

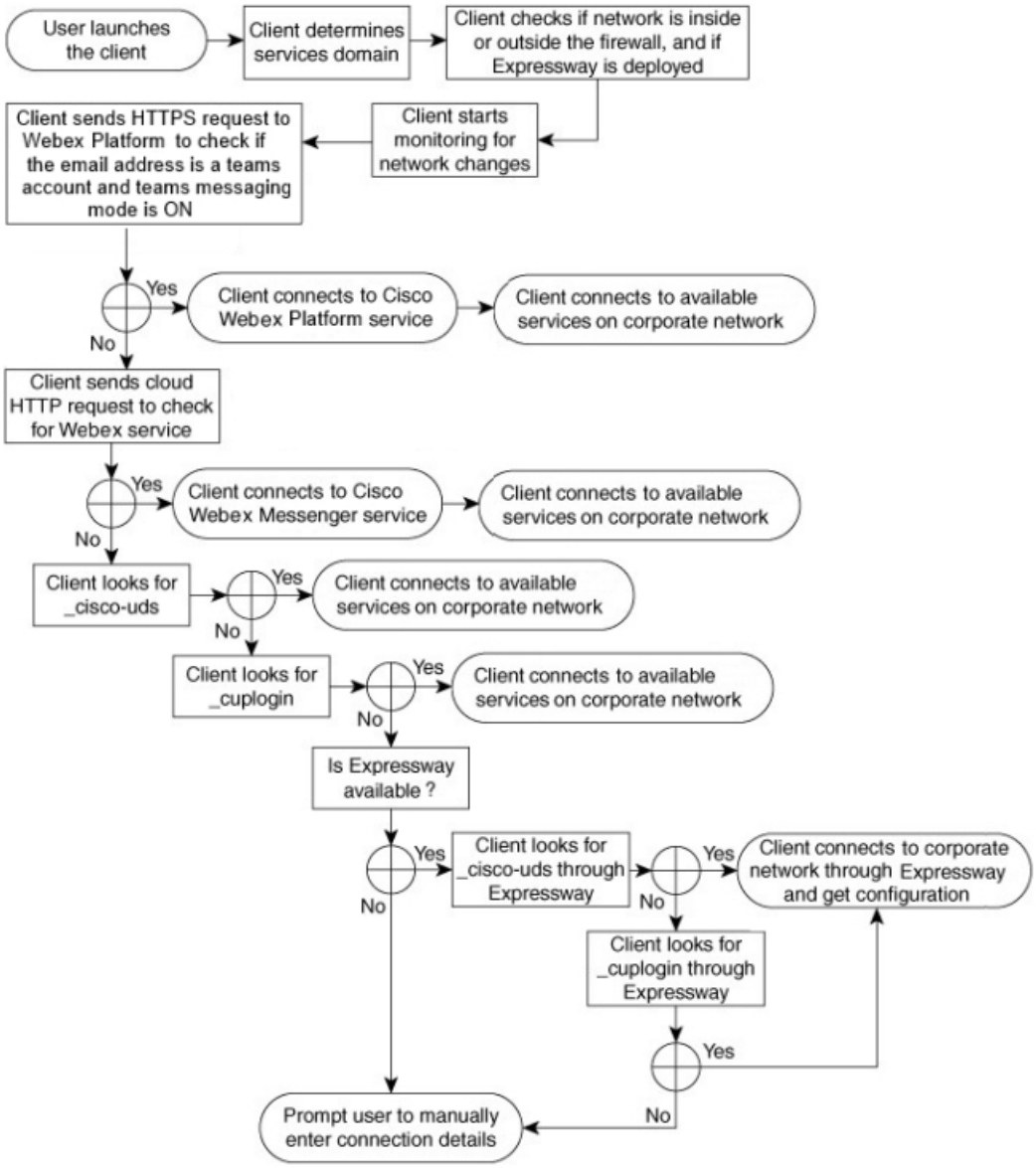
Method 1: Search For Services

We recommend that you use this method for how Cisco Jabber detects what services and features are available to users. Searching for services means that the client uses DNS service (SRV) records to determine which services are available to the client.

How the Client Discovers Available Services

The following figure shows the flow that the client uses to connect to services.

Figure 1: Login Flow for Service Discovery



To discover available services, the client does the following:

1. Checks if the network is inside or outside the firewall and if Expressway for Mobile and Remote Access is deployed. The client sends a query to the name server to get DNS Service (SRV) records.
2. Starts monitoring for network changes.

   When Expressway for Mobile and Remote Access is deployed, the client monitors the network to ensure that it can reconnect if the network changes from inside or outside the firewall.
3. Issues several HTTPS requests to Cisco Webex Platform Service to determine whether Jabber goes into team messaging mode. The request checks the user's email address to see whether the user has been enabled for team messaging in the Webex Control Hub.
4. Issues an HTTP query to a CAS URL for the Webex Messenger service.

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

   When Expressway for Mobile and Remote Access is deployed, the client connects to Webex Messenger Service and uses Expressway for Mobile and Remote Access to connect to Cisco Unified Communications Manager. When the client launches for the first time the user will see a Phone Services Connection Error and will have to enter their credentials in the client options screen, subsequent launches will use the cached information.
5. Queries the name server to get DNS Service (SRV) records, unless the records exist in the cache from a previous query.

   This query enables the client to do the following:

   - Determine which services are available.
   - Determine if it can connect to the corporate network through Expressway for Mobile and Remote Access.

Client Issues an HTTP Query for Cisco Webex Messenger Service

In addition to querying the name server for SRV records to locate available services, Cisco Jabber sends an HTTP query to the CAS URL for the Webex Messenger service. This request enables the client to determine cloud-based deployments and authenticate users to the Webex Messenger service.

When the client gets a services domain from the user, it appends that domain to the following HTTP query:

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

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

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

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

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

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

When the client sends the HTTP request to the CAS URL, it uses configured system proxies.

For more information, see the *Configure Proxy Settings* section in the *Cisco Jabber Deployment and Installation Guide*.

Client Queries the Name Server

When the client queries a name server, it sends separate, simultaneous requests to the name server for SRV records.

The client requests the following SRV records in the following order:

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

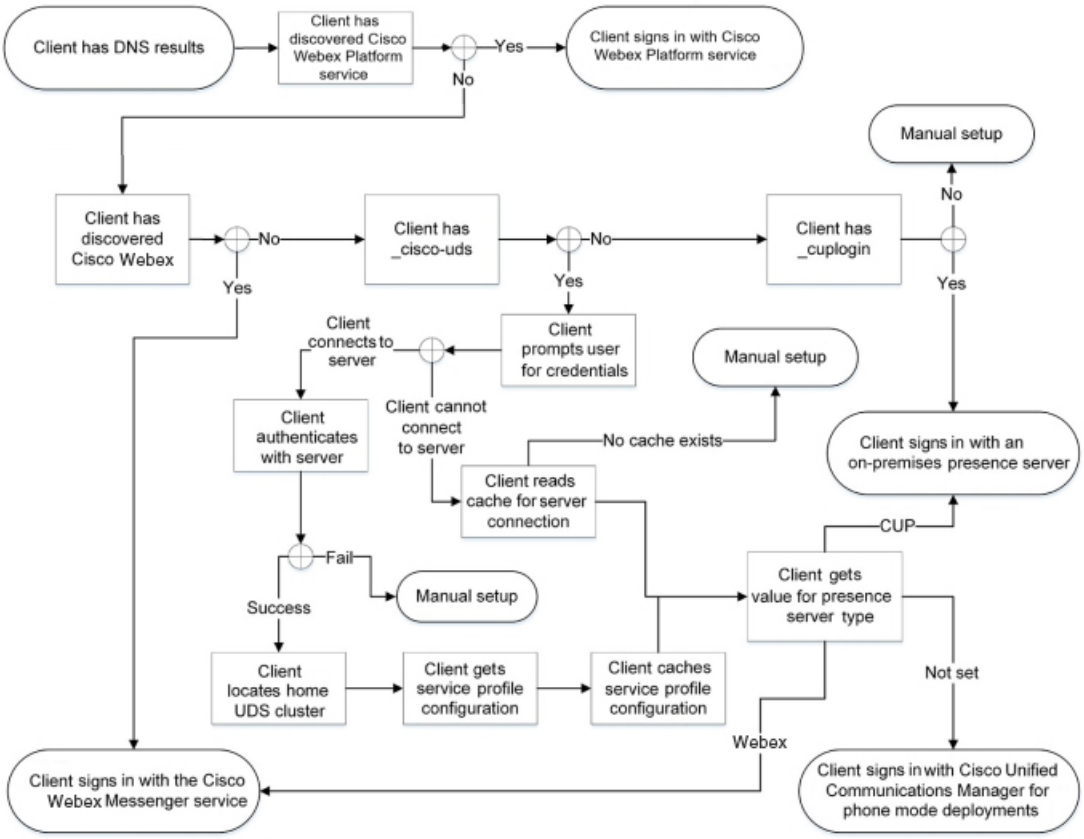
If the name server returns:

- `_cisco-uds`—The client detects it is inside the corporate network and connects to Cisco Unified Communications Manager.
- `_collab-edge`—The client attempts to connect to the internal network through Expressway for Mobile and Remote Access and discover services
- None of the SRV records—The client prompts users to manually enter setup and sign-in details.

Client Connects to Internal Services

The following figure shows how the client connects to internal services:

Figure 2: Client Connecting to Internal Services



When connecting to internal services, the goals are to determine the authenticator, sign users in, and connect to available services.

From the sign-in screen, users authenticate with one of these services:

- Cisco Webex Platform service—Cloud or hybrid deployments.
- Webex Messenger service—Cloud or hybrid deployments.
- Cisco Unified Communications Manager—On-premises deployments in phone mode.

The client connects to any services it discovers, which varies depending on the deployment.

1. If the client discovers that the user is enabled for team messaging mode, then the client does the following:
   a. Determines that Cisco Webex Platform service is the primary source of authentication.
   b. Automatically connects to Cisco Webex Platform Service.
   c. Prompts the user for credentials.
2. If the client discovers that the CAS URL lookup indicates a Webex user, the client does the following:
   a. Determines that the Webex Messenger service is the primary source of authentication.
   b. Automatically connects to the Webex Messenger service.

c. Prompts the user for credentials.

d. Retrieves client and service configuration.

3. If the client discovers a `_cisco-uds` SRV record, the client does the following:

Prompts the user for credentials to authenticate with Cisco Unified Communications Manager.

a. Locates the user's home cluster.

Locating the home cluster enables the client to automatically get the user's device list and register with Cisco Unified Communications Manager.

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

Important See the appropriate version of the *Cisco Unified Communications Manager Features and Services Guide* to learn how to configure ILS.

b. Retrieves the service profile.

The service profile provides the client with the authenticator as well as client and UC service configuration.

The client determines the authenticator from the value of the Product type field in the IM and presence profile, as follows:

- Cisco Unified Communications Manager—Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service is the authenticator.
- Webex (IM and Presence)—Webex Messenger service is the authenticator.

Note As of this release, the client issues an HTTP query in addition to the query for SRV records. The HTTP query allows the client to determine if it should authenticate to the Webex Messenger service.

As a result of the HTTP query, the client connects to the Webex Messenger service in cloud-based deployments. Setting the value of the **Product type** field to Webex does not effect if the client has already discovered the Webex service using a CAS lookup.

- Not set—If the service profile does not contain an IM and Presence Service configuration, the authenticator is Cisco Unified Communications Manager.

c. Sign in to the authenticator.

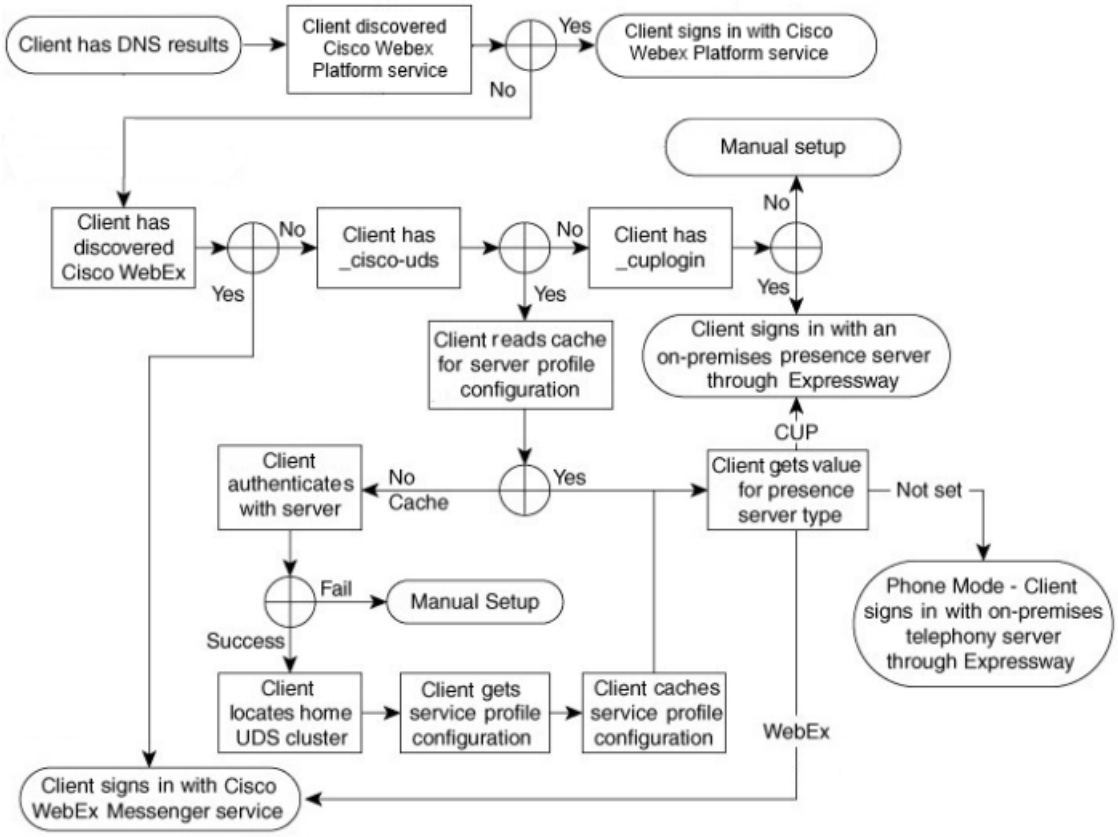
After the client signs in, it can determine the product mode.

Client Connects through Expressway for Mobile and Remote Access

If the name server returns the `_collab-edge` SRV record, the client attempts to connect to internal servers through Expressway for Mobile and Remote Access.

The following figure shows how the client connects to internal services when the client is connected to the network through Expressway for Mobile and Remote Access:

Figure 3: Client Connects through Expressway for Mobile and Remote Access



When the name server returns the `_collab-edge` SRV record, the client gets the location of the Cisco Expressway-E server. The Cisco Expressway-E server then provides the client with the results of the query to the internal name server.

Note The Cisco Expressway-C server looks up the internal SRV records and provides the records to the Cisco Expressway-E server.

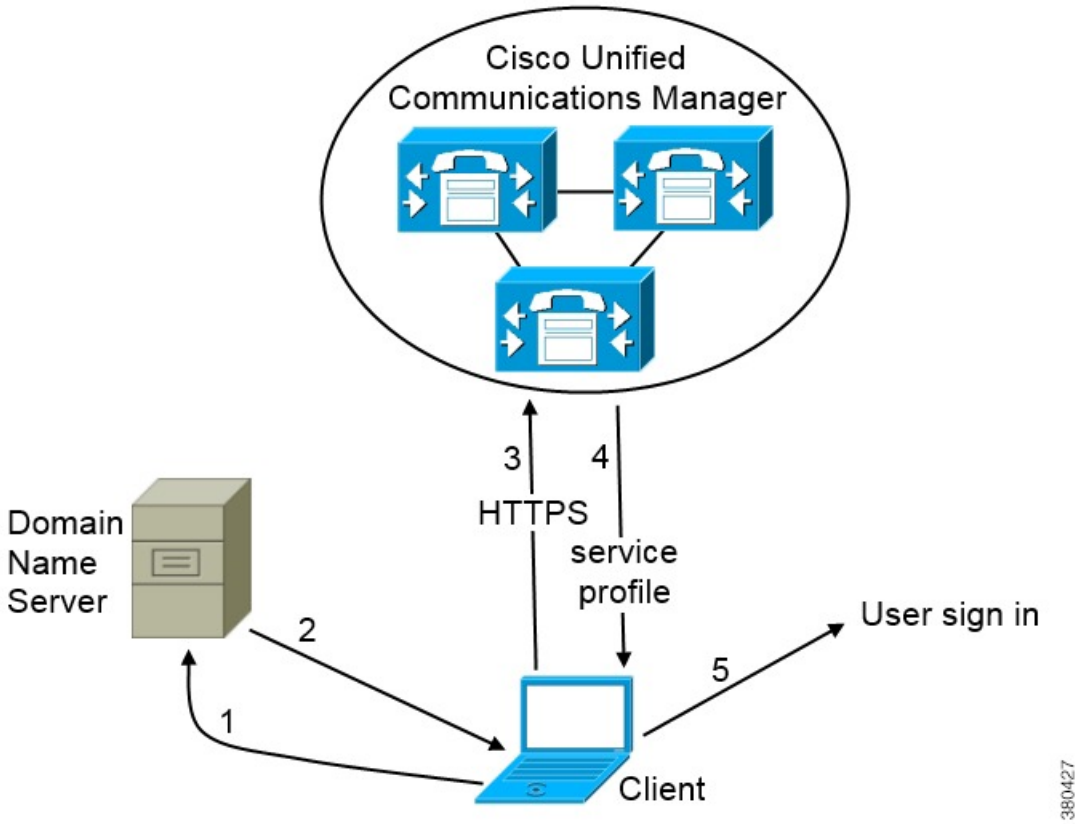
After the client gets the internal SRV records, which must include the `_cisco-uds`SRV record, it retrieves service profiles from Cisco Unified Communications Manager. The service profiles then provide the client with the user's home cluster, the primary source of authentication, and configuration.

Cisco UDS SRV Record

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

The following figure shows how the client uses the `_cisco-uds` SRV record.

Figure 4: UDS SRV Record Login Flow



1. The client queries the domain name server for SRV records.
2. The domain name server returns the `_cisco-uds` SRV record.
3. The client locates the user's home cluster.

   As a result, 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, you must manually configure remote cluster information, similar to the Extension Mobility Cross Cluster (EMCC) remote cluster setup. For more information on remote cluster configurations, 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:

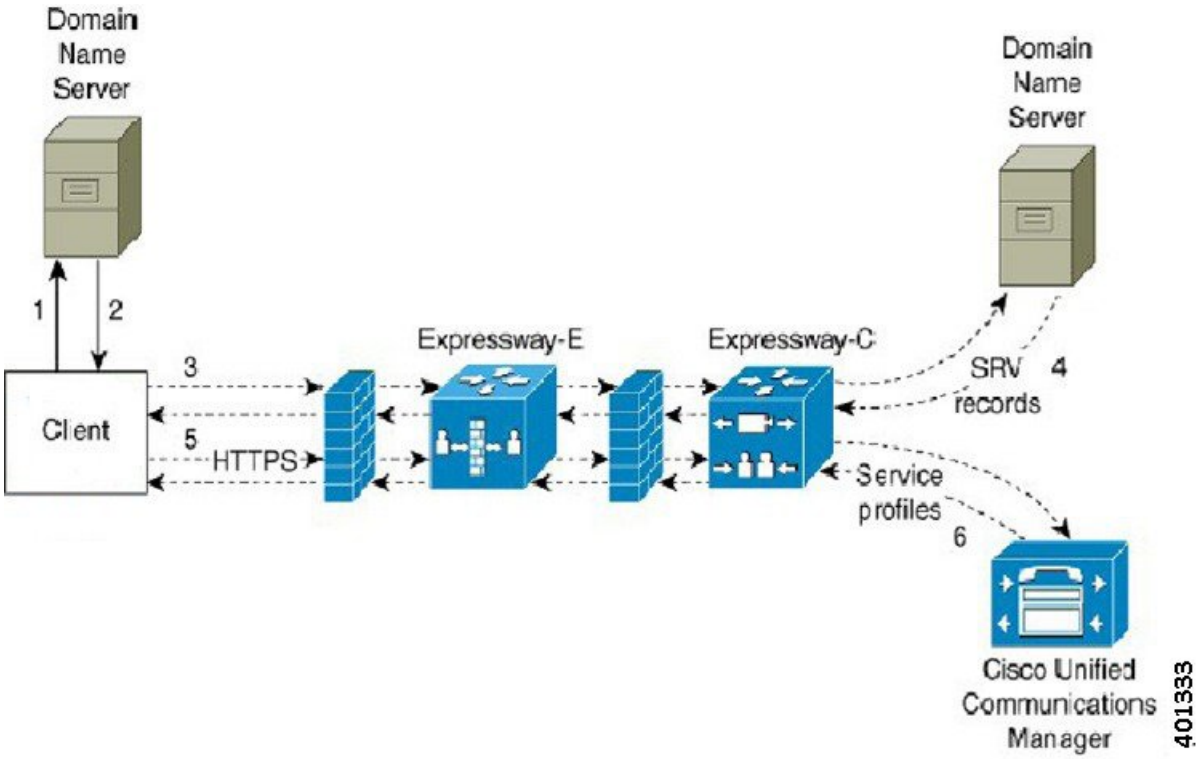
```
_cisco-uds._tcp.example.com     SRV service location:
          priority       = 6
          weight         = 30
          port           = 8443
          svr hostname   = cucm3.example.com
_cisco-uds._tcp.example.com     SRV service location:
          priority       = 2
          weight       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

Collaboration Edge SRV Record

Cisco Jabber can attempt to connect to internal servers through Expressway for Mobile and Remote Access to discover services with the following `_collab-edge` SRV record.

The following figure shows how the client uses the `_collab-edge` SRV record.

Figure 5: Collaboration Edge Record Login Flow



1. The client queries the external domain name server for SRV records.
2. The name server returns the `_collab-edge` SRV record and does not return the `_cuplogin` or `_cisco-uds` SRV records.

As a result, Cisco Jabber can locate the Cisco Expressway-E server.

3. The client requests the internal SRV records (through Expressway) from the internal domain name server.

   These SRV records must include the `_cisco-uds` SRV record.

4. The client obtains the internal SRV records (through Expressway).

   As a result, the client can locate the Cisco Unified Communications Manager server.

5. The client requests the service profiles (through Expressway) from Cisco Unified Communications Manager.

6. The client retrieves the service profiles (through Expressway) from Cisco Unified Communications Manager.

   The service profile contains the user's home cluster, the primary source of authentication, and the client configuration.

DNS Configuration

How the Client Uses DNS

Cisco Jabber uses domain name servers to do the following:

- Determine whether the client is inside or outside the corporate network.
- Automatically discover on-premises servers inside the corporate network.
- Locate access points for Expressway for Mobile and Remote Access on the public Internet.

Note Android OS limitation: Android OS 4.4.2 and 5.0 using the DNS service can resolve only the domain name, but not the hostname.

For more information, see the Android developer link.

How the Client Finds a Name Server

Cisco Jabberlooks for DNS records from:

- Internal name servers inside the corporate network.
- External name servers on the public Internet.

When the client's host computer or device gets a network connection, the host computer or device also gets the address of a DNS name server from the DHCP settings. Depending on the network connection, that name server might be internal or external to the corporate network.

Cisco Jabber queries the name server that the host computer or device gets from the DHCP settings.

How the Client Gets a Services Domain

The services domain is discovered by the client in different ways.

New installation:

- User enters an address in the format `username@example.com` in the client user interface.
- User clicks on a configuration URL that includes the service domain. This option is only available in the following versions of the client:
  - Cisco Jabber for Android release 9.6 or later
  - Cisco Jabber for Mac release 9.6 or later
  - Cisco Jabber for iPhone and iPad release 9.6.1 or later
- The client uses installation switches in bootstrap files. This option is only available in the following version of the client:
  - Cisco Jabber for Windows release 9.6 or later

Existing installation:

- The client uses the cached configuration.
- User manually enters an address in the client user interface.

In hybrid deployments the domain required to discover Webex domain through Central Authentication Service (CAS) lookup may be different to the domain where the DNS records are deployed. In this scenario you set the ServicesDomain to be the domain used to discover Webex and set the VoiceServicesDomain to be the domain where DNS records are deployed. The voice services domain is configured as follows:

- The client uses the VoiceServicesDomain parameter in the configuration file. This option is available in clients that support the `jabber-config.xml` file.
- User clicks on a configuration URL that includes the VoiceServicesDomain. This option is available in the following clients:
  - Cisco Jabber for Android release 9.6 or later
  - Cisco Jabber for Mac release 9.6 or later
  - Cisco Jabber for iPhone and iPad release 9.6.1 or later
- The client uses the Voice_Services_Domain installation switch in the bootstrap files. This option is only available in the following version of the client:
  - Cisco Jabber for Windows release 9.6 or later

After Cisco Jabber gets the services domain, it queries the name server that is configured to the client computer or device.

Domain Name System Designs

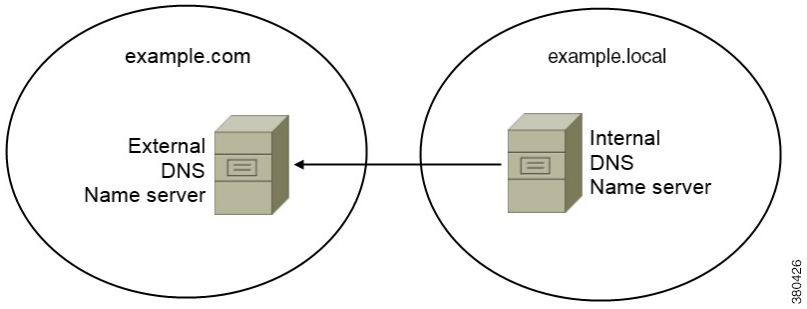
Where you deploy DNS service (SRV) records depends on the design of your DNS namespace. Typically there are two DNS designs:

- Separate domain names outside and inside the corporate network.
- Same domain name outside and inside the corporate network.

Separate Domain Design

The following figure shows a separate domain design:

Figure 6: Separate Domain Design



An example of a separate domain design is one where your organization registers the following external domain with an Internet name authority: `example.com`.

Your company also uses an internal domain that is one of the following:

- A subdomain of the external domain, for example, `example.local`.
- A different domain to the external domain, for example, `exampledomain.com`.

Separate domain designs have the following characteristics:

- The internal name server has zones that contain resource records for internal domains. The internal name server is authoritative for the internal domains.
- The internal name server forwards requests to the external name server when a DNS client queries for external domains.
- The external name server has a zone that contains resource records for your organization's external domain. The external name server is authoritative for that domain.
- The external name server can forward requests to other external name servers. However, the external name server cannot forward requests to the internal name server.

Deploy SRV Records in a Separate Domain Structure

In a separate name design there are two domains, an internal domain and an external domain. The client queries for SRV records in the services domain. The internal name server must serve records for the services domain. However in a separate name design, a zone for the services domain might not exist on the internal name server.

If the services domain is not currently served by the internal name server, you can:

- Deploy records within an internal zone for the services domain.
- Deploy records within a pinpoint subdomain zone on the internal name server.

Use an Internal Zone for a Services Domain

If you do not already have a zone for the services domain on the internal name server, you can create one. This method makes the internal name server authoritative for the services domain. Because it is authoritative, the internal name server does not forward queries to any other name server.

This method changes the forwarding relationship for the entire domain and has the potential to disrupt your internal DNS structure. If you cannot create an internal zone for the services domain, you can create a pinpoint subdomain zone on the internal name server.

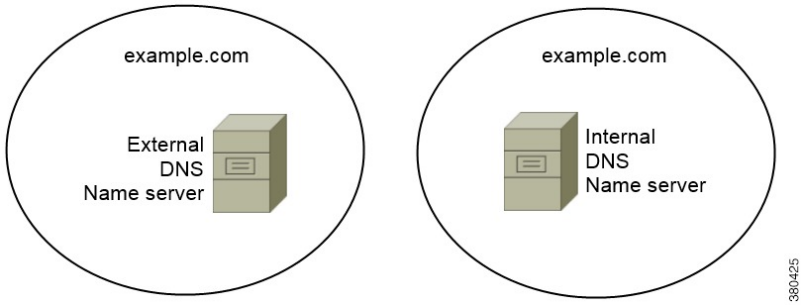
Same Domain Design

An example of a same domain design is one where your organization registers `example.com` as an external domain with an Internet name authority. Your organization also uses `example.com` as the name of the internal domain.

Single Domain, Split-Brain

The following figure shows a single domain with a split-brain domain design.

Figure 7: Single Domain, Split-Brain



Two DNS zones represent the single domain; one DNS zone in the internal name server and one DNS zone in the external name server.

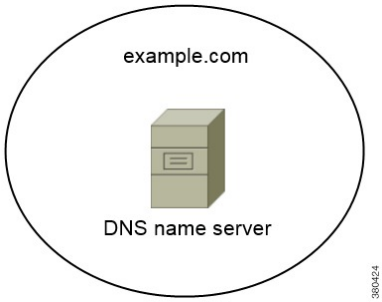
Both the internal name server and the external name server are authoritative for the single domain but serve different communities of hosts.

- Hosts inside the corporate network access only the internal name server.
- Hosts on the public Internet access only the external name server.
- Hosts that move between the corporate network and the public Internet access different name servers at different times.

Single Domain, Not Split-Brain

The following figure shows a single domain that does not have a split-brain domain design.

Figure 8: Single Domain, Not Split-Brain



In the single domain, not split-brain design, internal and external hosts are served by one set of name servers and can access the same DNS information.

Important This design is not common because it exposes more information about the internal network to potential attackers.

Method 2: Customization

You can customize service discovery by using installation parameters, URL configuration, or Enterprise Mobility Management.

Service Discovery Customization

Custom Installations for Cisco Jabber for Windows

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

- Use the Command Line—You can specify arguments in a command line window to set installation properties.

  Choose this option if you plan to install multiple instances.

- Run the MSI Manually—Run the MSI manually on the file system of the client workstation and then specify connection properties when you start the client.

  Choose this option if you plan to install a single instance for testing or evaluation purposes.

- Create a Custom Installer—Open the default installation package, specify the required installation properties, and then save a custom installation package.

  Choose this option if you plan to distribute an installation package with the same installation properties.

- Deploy with Group Policy—Install the client on multiple computers in the same domain.

Installer Switches: Cisco Jabber for Windows

When you install Cisco Jabber, you can specify the authenticator and server addresses. The installer saves these details to a bootstrap file. When users launch the client for the first time, it reads the bootstrap file. The bootstrap file takes priority if service discovery is deployed.

Bootstrap files provide a fallback mechanism for service discovery in situations where service discovery has not been deployed and where you do not want users to manually specify their connection settings.

The client only reads the bootstrap file on the initial launch. After the initial launch, the client caches the server addresses and configuration, and then loads from the cache on subsequent launches.

We recommend that you do not use a bootstrap file, and instead use service discovery, in on-premises deployments with Cisco Unified Communications Manager release 9.x and later.

Custom Installations for Cisco Jabber for Mac, iPhone and iPad, and Android

You can create customized installations of Cisco Jabber for Mac or mobile clients by using URL Configuration. For mobile clients you can also use Enterprise Mobility Management. These custom installations depend on installation parameters that enable services.

URL Configuration

To enable users launch Cisco Jabber without having to manually enter service discovery information, provide a configuration URL link to users to install the client.

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

Mobile Configuration Using Enterprise Mobility Management

You can configure Cisco Jabber using Enterprise Mobility Management (EMM) on Cisco Jabber for Android and Cisco Jabber for iPhone and iPad. For more information on setting up EMM, refer to the instructions for administrators provided by the EMM provider.

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

For more information about how to deploy EMM, see the section on *Deploy Cisco Jabber Applications* in the *On-Premises Deployment for Cisco Jabber* or in the *Cloud and Hybrid Deployments for Cisco Jabber*.

Method 3: Manual Installations

As an advanced option, users can manually connect to services at the sign in screen.

High Availability

High Availability for Instant Messaging and Presence

High availability refers to an environment in which multiple nodes exist in a subcluster to provide failover capabilities for instant messaging and presence services. If one node in a subcluster becomes unavailable, the

instant messaging and presence services from that node failover to another node in the subcluster. In this way, high availability ensures reliable continuity of instant messaging and presence services for Cisco Jabber.

High availability is supported for LDAP. High availability is not supported when using UDS contact source.

Cisco Jabber supports high availability with the following servers:

Cisco Unified Communications Manager IM and Presence Service release 9.0 and higher

Use the following Cisco Unified Communications Manager IM and Presence Service documentation for more information about high availability.

Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager

`High Availability Client Login Profiles`

`Troubleshooting High Availability`

Active Calls on Hold During Failover

You cannot place an active call on hold if failover occurs from the primary instance of Cisco Unified Communications Manager to the secondary instance.

High Availability in the Client

Client Behavior During Failover

If high availability is configured on the server, then after the primary server fails over to the secondary server, the client temporarily loses presence states for up to one minute. Configure the re-login parameters to define how long the client waits before attempting to re-login to the server.

Configure Login Parameters

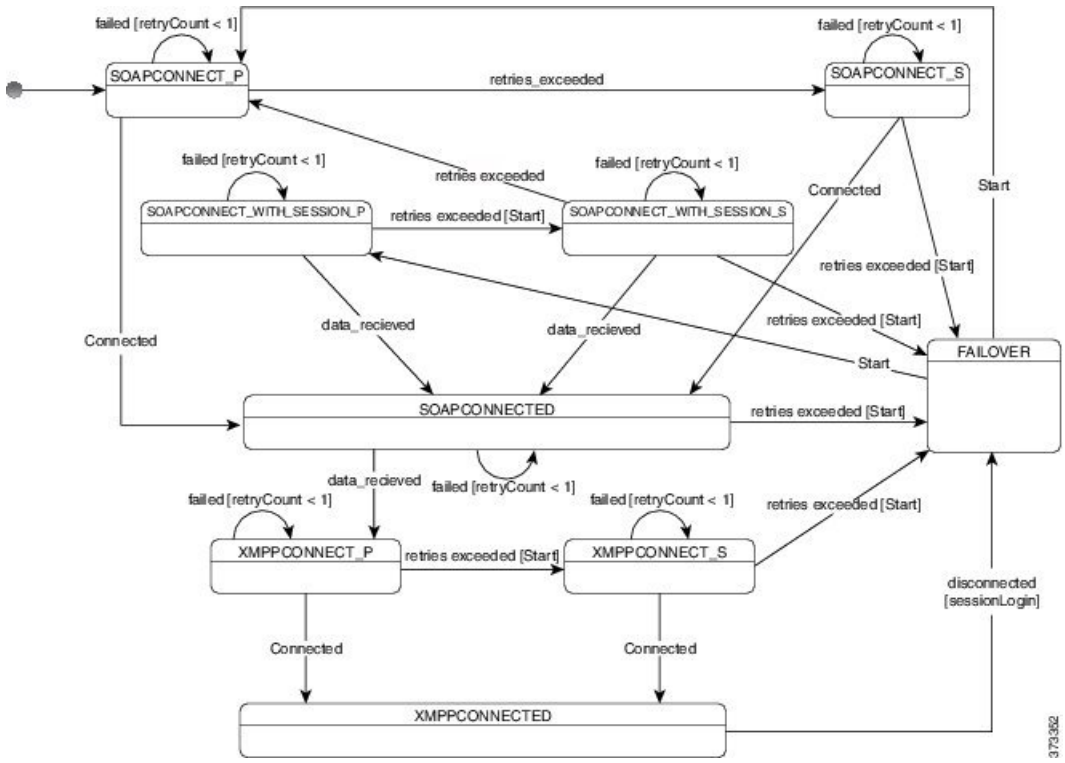
In Cisco Unified Communications Manager IM and Presence Service, you can configure the maximum and minimum number of seconds that Cisco Jabber waits before attempting to re-login to the server. On the server, you specify the re-login parameters in the following fields:

- **Client Re-Login Lower Limit**
- **Client Re-Login Upper Limit**

Client Behavior During a Failover

The following figure shows the client's behavior when the Cisco Unified Communications Manager IM and Presence service during a failover.

Figure 9: Client Behavior During a Failover



1. When the client is disconnected from its active server, the client goes from XMPPCONNECTED state to a FAILOVER state.
2. From a FAILOVER state, the client tries to attain a SOAPCONNECTED state by attempting SOAPCONNECT_SESSION_P (as the primary server), and if that fails, attempts SOAPCONNECT_SESSION_S (as the secondary server).
   - If it is unable to attain SOAPCONNECT_SESSION_P or SOAPCONNECT_SESSION_S, the client re-enters into the FAILOVER state.
   - From a FAILOVER state, the clients attempts to attain a SOAPCONNECT_P state, and if that fails, attempts to reach a SOAPCONNECT_S state.
   - If the client cannot reach the SOAPCONNECT_P or SOAPCONNECT_S state, then the client does not attempt any more automatic connections to the IM&P server until a user initiates a login attempt.
3. From a SOAPCONNECT_SESSION_P, SOAPCONNECT_SESSION_S, SOAPCONNECT_P, or SOAPCONNECT_S state, the client retrieves its current primary secondary XMPP server address. This address changes during a failover.
4. From a SOAPCONNECTED state, the client tries to attain an XMPPCONNECTED state by attempting to connect to the XMPPCONNECT_P state, and if that fails, attempts XMPPCONNECT_S state.
   - If client cannot reach XMPPCONNECT_P or XMPPCONNECT_S state, then the client does not attempt any more automatic connections to the IM&P server until a user initiates a login attempt.
5. After the client is in an XMPPCONNECTED state, then the client has IM&P capability.

High Availability for Voice and Video

If one node in a subcluster becomes unavailable, voice and video failover to another node in the subcluster.

By default, it takes up to 120 seconds for a software phone device or desk phone to register with another node. If this timeout period is too long, adjust the value of the SIP Station KeepAlive Interval service parameter for your node. The SIP Station KeepAlive Interval service parameter modifies all phone devices on Cisco Unified Communications Manager. Before you adjust the interval, analyze the impact on the Cisco Unified Communications Manager servers.

To configure service parameters for the node, in Cisco Unified Communications Manager Administration, select **System** > **Service Parameters**.

For a phone mode deployment using the non-DNS SRV record method, failover isn't possible for Voice and Video, as there is only one Cisco Unified Communications Manager node specified.

High Availability for Persistent Chat

There is high availability support for persistent chat. During the failover window, users may be prompted that they can't send messages. When the node has failed over, users automatically rejoin the chat room and can send messages again.

High Availability for Contact Search and Contact Resolution

High availability is supported for contact search and contact resolution, which are provided by the Cisco Unified Communications Manager User Data Service (UDS). If the primary UDS server is unavailable, Jabber automatically fails over to a second UDS server, or to a third UDS server, if configured.

High Availability for Voicemail

If a secondary voicemail server is configured, then all clients automatically failover to the secondary voicemail server if the primary server becomes unavailable or unreachable.

Configuration Priorities

When both a service profile and a configuration file are present, the following table describes which parameter value takes precedence.

Service Profile	Configuration File	Which Parameter Value Takes Precedence?
Parameter value is set	Parameter value is set	Service profile
Parameter value is set	Parameter value is blank	Service profile
Parameter value is blank	Parameter value is set	Configuration file
Parameter value is blank	Parameter value is blank	Service profile blank (default) value

Group Configurations Using Cisco Support Field

Group configuration files apply to a subset of users. If you provision users with CSF devices, you can specify the group configuration file names in the **Cisco Support Field** field on the device configuration. If users do not have CSF devices, you can set a unique configuration file name for each group during installation with the TFTP_FILE_NAME argument.

Group configuration is supported on TCT and BOT with COP file later than 14122 version.