



How the Client Uses Domain Name Servers

Cisco Jabber uses domain name servers to do the following:

- Automatically discover on-premises servers inside the corporate network.
- Locate access points for Expressway Mobile and Remote Access on the public Internet.
- Determine whether the client is inside or outside the corporate network.
- [How the Client Finds a Name Server, page 1](#)
- [How the Client Gets a Services Domain, page 1](#)
- [How the Client Discovers Available Services, page 2](#)

How the Client Finds a Name Server

Cisco Jabber looks 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 Cisco Jabber 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 version 9.6 or later
 - Cisco Jabber for Mac version 9.6 or later
 - Cisco Jabber for iPhone and iPad version 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 version 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 Cisco WebEx domain through 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 Cisco WebEx and set the VoiceServicesDomain to be the domain where DNS records are deployed. The voice services domain is configured as follows:

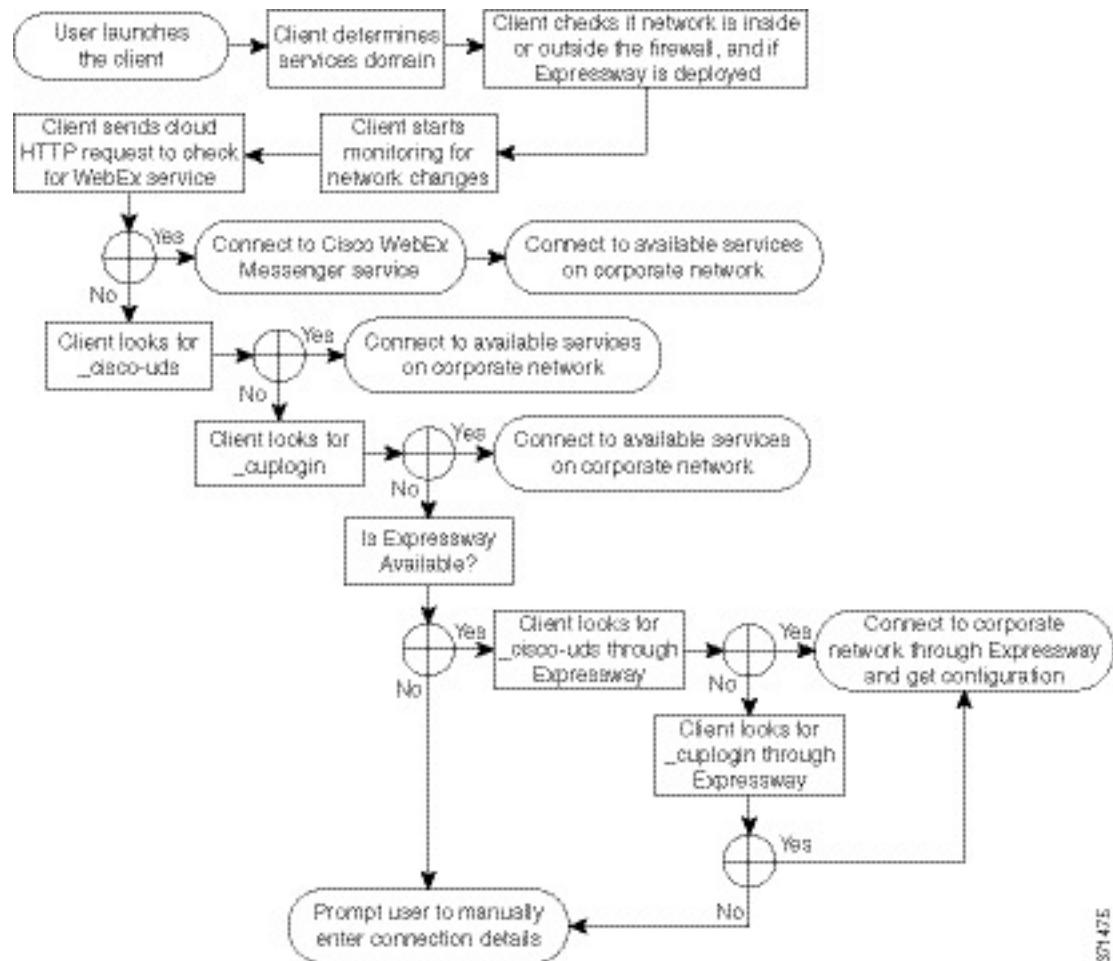
- The client uses the VoiceServicesDomain parameter in the configuration file. This option is available in clients that support the `jabber-config.xml` file.
 - User clicks on a configuration URL that includes the VoiceServicesDomain. This option is available in the following clients:
 - Cisco Jabber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

See the appropriate version of the *Installation and Configuration guide*, for more detailed information.

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

How the Client Discovers Available Services

The following diagram illustrates the flow that the client uses to connect to services:



To discover available services, the client:

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

When Expressway 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 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.
- 4 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 Mobile and Remote Access.

**Note**

Refer to the latest version of your *Cisco Jabber client Installation and Configuration Guide* for further information on configuring available services.

Client Issues HTTP Query

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 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 services 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 services 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 services domain is a valid Cisco WebEx domain.

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

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

**Note**

When the client sends the HTTP request to the CAS URL, it uses any configured system proxies. The following limitations apply when using a proxy for these HTTP requests:

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

Client Queries 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`
- `_cuplogin`
- `_collab-edge`

If the name server returns:

_cisco-uds or _cuplogin

The client detects it is inside the corporate network and connects to one of the following:

Cisco Unified Communications Manager

If the name server returns `_cisco-uds`.

Cisco Unified Presence

If the name server returns `_cuplogin`.

_collab-edge

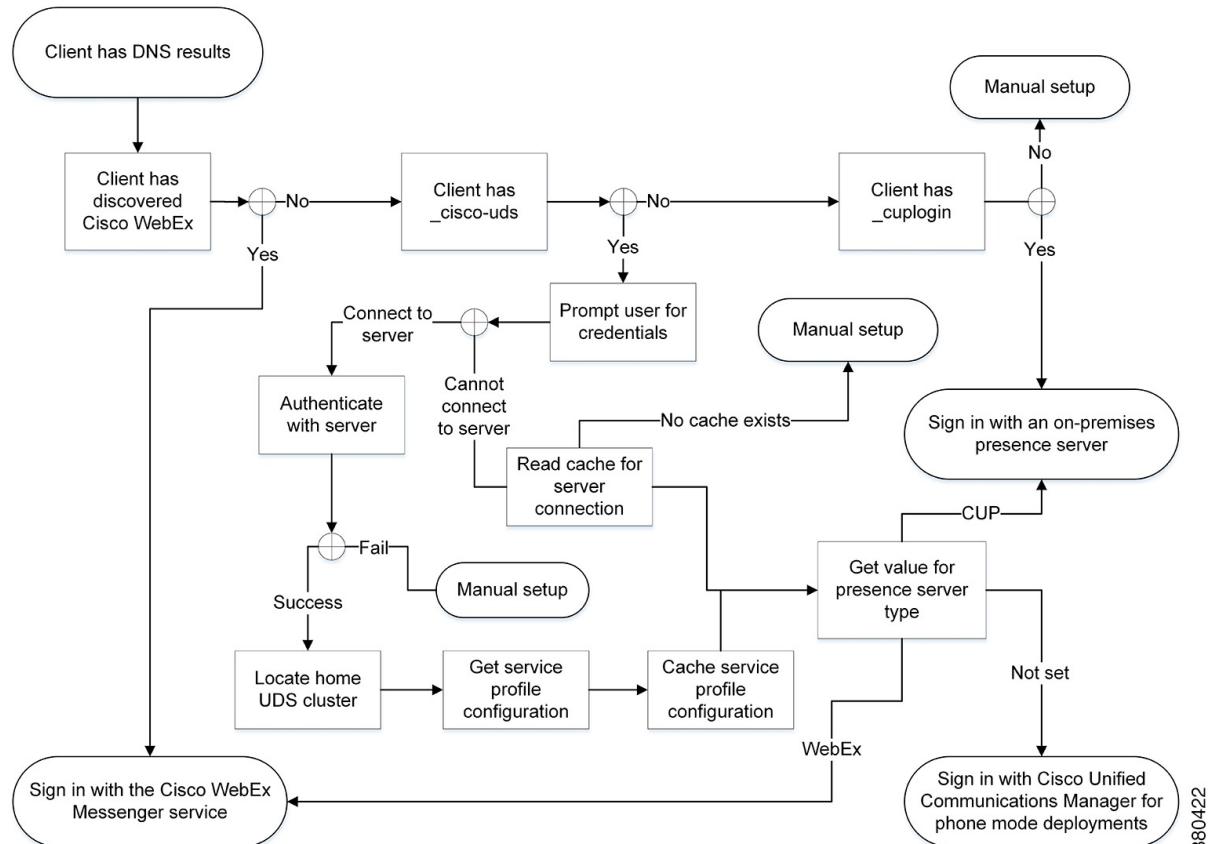
The client attempts to connect to the internal network through Expressway Mobile and Remote Access and discover services.

None of the SRV records

The client prompts users to manually enter setup and sign-in details.

Client Connects to Internal Services

The following diagram illustrates how the client connects to internal services:



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

There are three possible authenticators that can get users past the sign in screen, as follows:

Cisco WebEx Messenger Service

Cloud-based or hybrid cloud-based deployments.

Cisco Unified Presence

On-premises deployments in the default product mode. The default product mode can be either full UC or IM only.

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 CAS URL lookup indicates a Cisco WebEx user, the client:
 - a Determines that the Cisco WebEx Messenger service is the primary source of authentication.
 - b Automatically connects to the Cisco WebEx Messenger service.
 - c Prompts the user for credentials.
 - d Retrieves client and service configuration.
- 2 If the client discovers a `_cisco-uds` record, then the client:
 - 1 Prompts the user for credentials to authenticate with Cisco Unified Communications Manager.
 - 2 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.



Important

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.

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

-
- 3 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:

Unified CM (IM and Presence)

Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence is the authenticator.

WebEx (IM and Presence)

The Cisco 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 Cisco WebEx Messenger service.

As a result of the HTTP query, the client connects to the Cisco WebEx Messenger service in cloud-based deployments. Setting the value of the **Product type** field to **WebEx** may have no practical effect if the client 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.

- 4 Sign in to the authenticator.

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

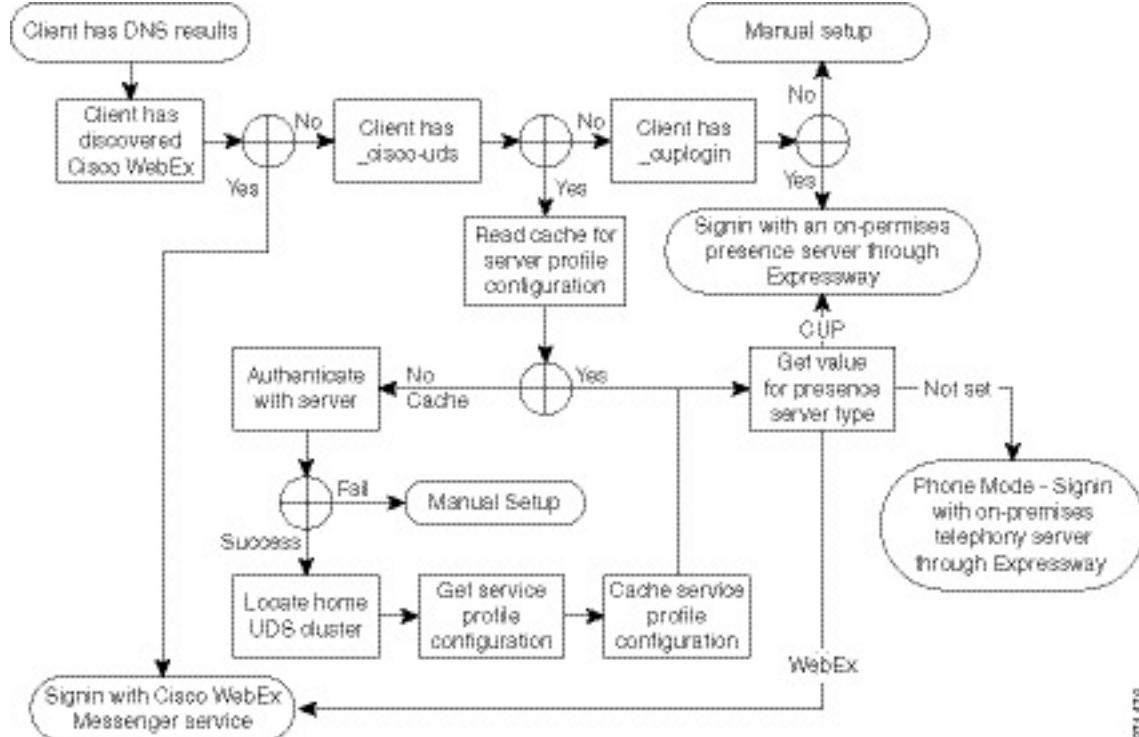
- 3 If the client discovers a `_cuplogin` record, the client:

- 1 Determines that Cisco Unified Presence is the primary source of authentication.
- 2 Automatically connects to the server.
- 3 Prompts the user for credentials.
- 4 Retrieves client and service configuration.

Client Connects through Expressway Mobile and Remote Access

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

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



37478

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



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

After the client gets the internal SRV records, which must include `_cisco-uds`, 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.