User management

Jabber IDs

Cisco Jabber uses a Jabber ID to identify the contact information in the contact source.

The default Jabber ID is created using the user ID and the presence domain.

For example, Adam McKenzie has a user ID of `amckenzie`, his domain is `example.com` and his Jabber ID is `amckenzie@example.com`.

The following characters are supported in a Cisco Jabber user ID or email address:

- Uppercase characters (A to Z)
- Lowercase characters (a to z)
- Numbers (0-9)
- Period (.)
- Hyphen (-)
- Underscore (_)
- Tilde (~)
- Hashtag (#)

When populating the contact list the client will search the contact source using the Jabber IDs to resolve the contacts and display the firstname, lastname, and any other contact information.

IM Address Scheme

Cisco Jabber 10.6 and later supports multiple presence domain architecture models for on premises deployments when the domains are on the same presence architecture, for example users in example-us.com and example-uk.com. Cisco Jabber supports flexible IM Address Scheme using Cisco Unified Communications Manager IM and Presence 10.x or later. The IM Address scheme is the Jabber ID that identifies the Cisco Jabber users.

To support multi domain models, all components of the deployment require the following versions:

- Cisco Unified Communications IM and Presence server nodes and call control nodes version 10.x or later.
- All clients running on Windows, Mac, IOS and Android version 10.6 or later.

Only deploy Cisco Jabber with multiple domain architecture in the following scenarios:

- Cisco Jabber 10.6 or later is deployed as a new installation to all users in your organization on all platforms (Windows, Mac, IOS and Android, including Android based IP Phones such as the DX series).
- Before making any domain or IM address changes on the presence server, Cisco Jabber is upgraded to version 10.6 or later for all users on all platforms (Windows, Mac, IOS and Android, including Android based IP Phones such as the DX series).

The available IM address schemes in the Advanced Presence Settings are:

- UserID@[Default Domain]
- Directory URI

UserID@[Default Domain]

The User ID field is mapped to an LDAP field. This is the default IM Address Scheme.

For example, user Anita Perez has an account name aperez and the User ID field is mapped to the sAMAccountName LDAP field. The address scheme used is aperez@example.com.

Directory URI

The Directory URI is mapped to the **mail** or **msRTCSIP-primaryuseraddress** LDAP fields. This option provides a scheme that is independent of the user ID for authentication.

For example, user Anita Perez has an account name aperez, the mail field is Anita.Perez@domain.com, the address scheme used is Anita.Perez@domain.com.

Service Discovery using Jabber IDs

Service discovery takes the Jabber ID entered in the format `[userid]@[domain.com]` and by default, extracts the `domain.com` portion of the Jabber ID to discover the services available. For a deployment where the presence domain is not the same as the service discovery domain, you can include the service discovery domain information during installation as follows:

- In Cisco Jabber for Windows this is done using the `SERVICES_DOMAIN` command line argument.

- In Cisco Jabber for Mac, Cisco Jabber for Android, or Cisco Jabber for iPhone and iPad the service discovery domain can be set using the `ServicesDomain` parameter used with URL configuration.

.

SIP URI

A SIP URI is associated with each user. The SIP URI can be an email address, an IMAddress, or a UPN.

The SIP URI is configured using the Directory URI field in Cisco Unified Communications Manager. These are the available options:

- mail
- msRTCSIP-primaryuseraddress

Users can search for contacts and dial contacts by entering a SIP URI.

LDAP User ID

When you synchronize from your directory source to Cisco Unified Communications Manager, the user ID is populated from an attribute in the directory. The default attribute that holds the user ID is `sAMAccountName`.

User ID Planning for Federation

For federation, Cisco Jabber requires the contact ID or user ID for each user to resolve contacts during contact searches.

Set the attribute for the user ID in the SipUri parameter. The default value is `msRTCSIP-PrimaryUserAddress`. If there is a prefix to remove from your user ID you can set a value in the UriPrefix parameter, see the latest version of the *Parameters Reference Guide for Cisco Jabber*.

Proxy Addresses for User Contact Photos

Cisco Jabber accesses the photo server to retrieve contact photos. If your network configuration contains a Web Proxy, you need to ensure that Cisco Jabber can access the Photo Server.

Authentication and Authorization

Cisco Unified Communications Manager LDAP Authentication

LDAP authentication is configured on Cisco Unified Communications Manager to authenticate with the directory server.

When users sign in to the client, the presence server routes that authentication to Cisco Unified Communications Manager. Cisco Unified Communications Manager then proxies that authentication to the directory server.

Webex Messenger Login Authentication

Webex Messenger authentication is configured using the Webex Administration tool.

When users sign in to the client, the information is sent to the Webex Messenger and an authentication token is sent back to the client.

Single Sign-On Authentication

Single Sign on authentication is configured using an Identity Provider (IdP) and services.

When users sign in to the client, the information is sent to the IdP and once the credentials are accepted an authentication token is sent back to Cisco Jabber.

Certificate-Based Authentication for Cisco Jabber for iPhone and iPad

Cisco Jabber authenticates on the IdP server through a client certificate. This certificate authentication allows users to sign in to the servers without entering user credentials. The client uses the Safari framework to implement this feature.

Requirements

- Cisco Unified Communications Manager 11.5, IM and Presence Service 11.5, Cisco Unity Connection 11.5 and above.
- Expressway for Mobile and Remote Access server 8.9 and later.
- SSO enabled for the Unified Communications infrastructure.
- All server certificates are CA signed including Cisco Unified Communications Manager, IM and Presence Service, Cisco Unity Connection and IdP server. If the iOS device does use a trusted authority of OS, install the CA certificate before installing the Cisco Jabber app.
- Configure Native browser (embedded Safari) for SSO in Cisco Unified Communications Manager. For more information, refer to the section on certificate-based SSO authentication in *On-Premises Deployment for Cisco Jabber*.
- Configure Native browser (embedded Safari) for SSO in Expressway for Mobile and Remote Access server. For more information, see the Cisco Expressway installation guides at https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-guides-list.html.

You can deploy Cisco certificates on iOS devices through the EMM solution.

Recommendation—Cisco recommends using the EMM solution for deploying the certificate on iOS devices.

Certificate-Based Authentication for Cisco Jabber for Android

Cisco Jabber uses a client certificate to sign into single sign-on servers (Webex Messenger and on-premises).

Requirements

- Android OS 5.0 or later

- Single Sign-On is enabled
- Jabber client is supported over Mobile and Remote Access (MRA) and non-MRA deployment mode.
- Jabber always displays notifications for invalid certificates on Android 7.0 and later, even for installed custom CA-signed certificates on the Android OS. Apps that target Android 7.0 only trust system-provided certificates and no longer trust user-added Certificate Authorities.

Certificate Deployment

Cisco recommends using an EMM solution for deploying the certificate on an Android device.

Voicemail Authentication

Users need to exist on Cisco Unity Connection. Cisco Unity Connection supports multiple authentication types. If Cisco Unified Communications Manager and Cisco Unity Connection use the same authentication then we recommend that Cisco Jabber is configured to use the same credentials.

OAuth

You can set up Cisco Jabber to use the OAuth protocol to authorize users' access rights to services. If the user signs in to an OAuth-enabled environment, then there is no need to enter the credentials every time the user signs in. However, if the servers are not OAuth-enabled, then Jabber may not function appropriately.

If you're using Cisco Unified Communication Manager 12.5 or later, you can also enable SIP OAuth. It allows Jabber to authorize itself to SIP, which allows Jabber to connect to SIP service over TLS. It also allows Jabber to send media over a secure connection (sRTP). SIP OAuth means that CAPF enrollment is no longer necessary to enable secure SIP and media.

Prerequisites:

- OAuth Refresh tokens must be turned on across all of these components if deployed to be functional
- Cisco Unified Communication Manager, Cisco Unified Communication Manager Instant Messaging and Presence, and Cisco Unity Connection must be of version 11.5(SU3) or 12.0
- Cisco Expressway for Mobile and Remote Access version X8.10 or later
- For SIP OAuth: Cisco Unified Communication Manager 12.5 or later, Cisco Expressway for Mobile and Remote Access version X12.5 or later.

Before you configure OAuth, check the type of the deployment you have:

- If you have local authentication deployment, then IdP server is not required, and Cisco Unified Communication Manager is responsible for authentication.
- You can set up OAuth with or without SSO configured. If you're using SSO, ensure it is enabled for all services. If you have an SSO-enabled deployment, then deploy an IdP server, and IdP server is responsible for authentication.

You can enable OAuth on the following services for your users:

- Cisco Unified Communications Manager
- Cisco Expressway

- Cisco Unity Connection

By default, OAuth is disabled on these servers. To enable OAuth on these servers:

- For Cisco Unified Communications Manager and Cisco Unity Connection Servers, go to **Enterprise Parameter configuration** > **OAuth with refresh Login Flow**.
- For Cisco Expressway-C, go to **Configuration Unified Communication** > **Configuration Authorized by OAuth token with refresh**.

When OAuth is enabled or disabled on any of these servers, Jabber identifies it during configuration re-fetch interval, and lets the user sign out and sign in to Jabber.

During sign out, Jabber deletes user credentials stored in the cache, and then lets user sign in with regular sign-in flow, where Jabber fetches all the configuration information first, and then lets the user access Jabber services.

To configure OAuth on Cisco Unified Communication Manager:

1. Go to **Cisco Unified Communication Manager Admin** > **System** > **Enterprise Parameters** > **SSO Configuration**.
2. Set **O-Auth Access Token Expiry Timer(minutes)** to desired value.
3. Set **O-Auth Refresh Token Expiry Timer(days)** to desired value.
4. Click **Save** button.

To configure OAuth on Cisco Expressway:

1. Go to **Configuration** > **Unified Communications** > **Configuration** > **MRA Access Control**.
2. Set **O-Auth local authentication** to **On**.

To configure OAuth on Cisco Unity:

1. Go to **AuthZ Servers** and select **Add New**.
2. Enter the details in the all fields and select **Ignore Certificate Errors**.
3. Click **Save**.

Limitation

Jabber triggers automated intrusion protection

Conditions:

- Your Expressway for Mobile and Remote Access deployment is configured for authorization by OAuth token (with or without Refresh token).
- The Jabber user's access token is expired.

Jabber does one of these:

- Resumes from desktop hibernate
- Recovers network connection

- Attempts fast sign-in after it is signed out for several hours

Behavior:

- Some Jabber modules attempt to authorize at Expressway-E using the expired access token.
- The Expressway-E (correctly) denies these requests.
- If there are more than five such requests from a particular Jabber client, the Expressway-E blocks that IP address for ten minutes (by default).

Symptoms:

The affected Jabber clients' IP addresses are added to the blocked addresses list of Expressway-E, in the HTTP proxy authorization failure category. You can see these on **System** > **Protection** > **Automated detection** > **Blocked addresses.**.

Workaround:

There are two ways you can work around this issue; you can increase the detection threshold for that particular category, or you can create an exemption for the affected clients. We describe the threshold option here because the exemptions may be impractical in your environment.

1. Go to **System** > **Protection** > **Automated detection** > **Configuration**.
2. Click **HTTP proxy authorization failure**.
3. Change the **Trigger level** from 5 to 10. 10 must be enough to tolerate the Jabber modules that present expired tokens.
4. Save the configuration, which takes effect immediately.
5. Unblock any affected clients.

Multiple Resource Login

All Cisco Jabber clients register with one of the following central IM and Presence Service nodes when a user logs in to the system. This node tracks availability, contact lists, and other aspects of the IM and Presence Service environment.

- On-Premises Deployments: Cisco Unified Communications Manager IM and Presence Service.
- Cloud Deployments: Webex.

This IM and Presence Service node tracks all of the registered clients associated with each unique network user in the following order:

1. When a new IM session is initiated between two users, the first incoming message is broadcast to all of the registered clients of the receiving user.
2. The IM and Presence Service node waits for the first response from one of the registered clients.
3. The first client to respond then receives the remainder of the incoming messages until the user starts responding using another registered client.
4. The node then reroutes subsequent messages to this new client.

Note If there is no active resource when a user is logged into multiple devices, then priority is given to the client with the highest presence priority. If the presence priority is the same on all devices, then priority is given to the latest client the user logged in to.