

The background features a vibrant, multi-colored abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of sharp, triangular rays in various colors, including blue, green, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go

#CiscoLiveAPJC



The bridge to possible

Authentication, Authorization and Provision for Cisco Collaboration

Paulo Jorge Correia
Principal Solutions Engineer
@paucorre
BRKCOL-2007

CISCO *Live!*

#CiscoLiveAPJC

Cisco Webex App

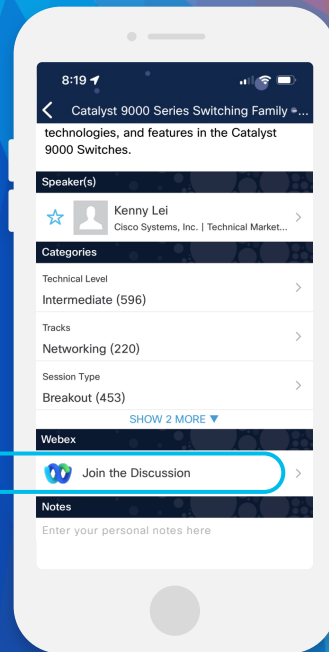
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until December 22, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKCOL-2007>

Agenda

- Introduction
- Webex Provisioning
 - Users Provisioning
 - Groups Provisioning
 - Other Provision Features
 - Microsoft Entra Integration
- OpenID Connect, how does it work?
- Webex AuthN/AuthZ Improvements
- Key Takeaways

Introduction

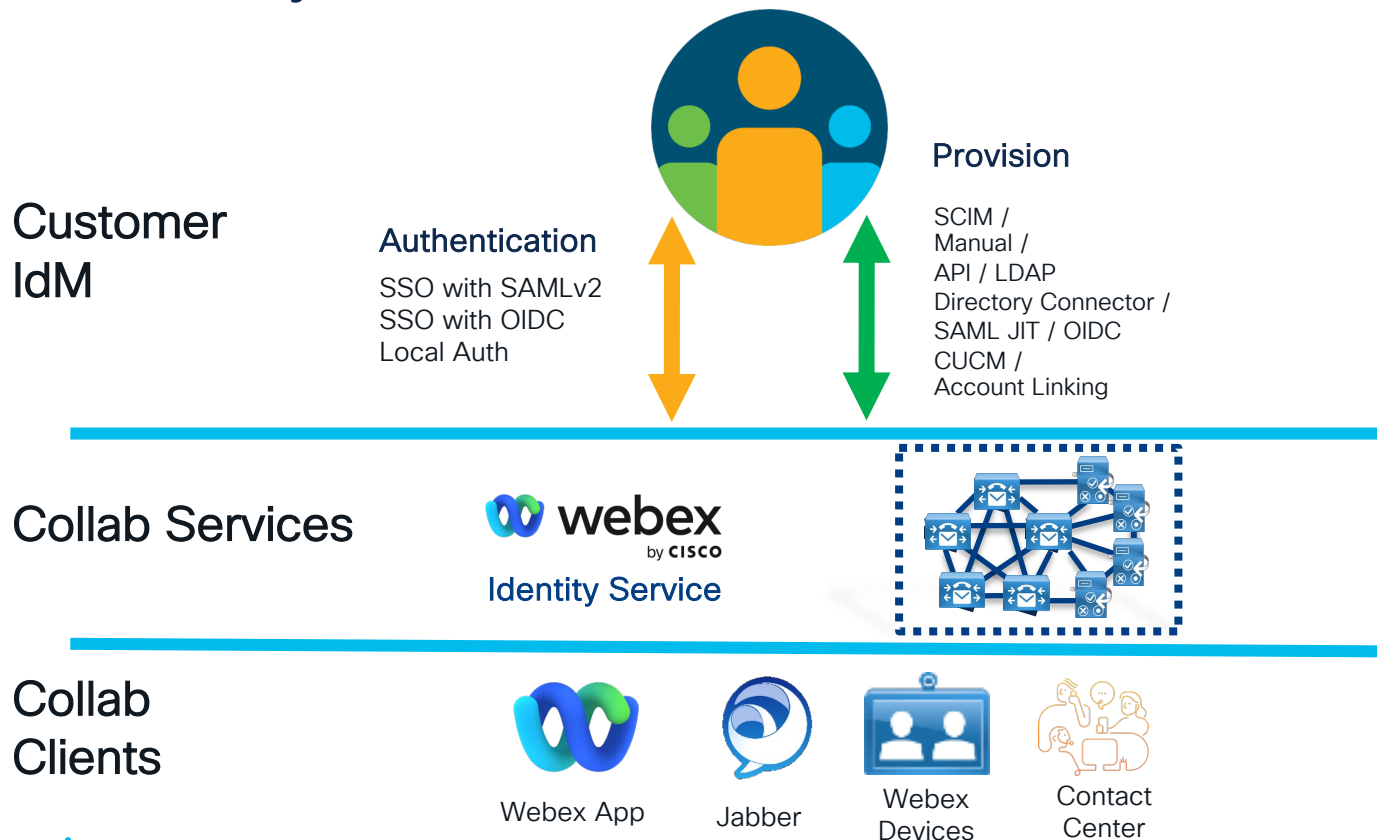
UPDATED: Sep 2022

filter

search...



Cisco Identity Architecture for Collaboration



Which Protocols do we see in Identity Management



SAML Security Assertion Markup Language defined under OASIS Security Services Technical Committee (SSTC) Standards.



OAuth is an Authorization Framework defined by IETF under RFC 6749



SCIM System for Cross-domain Identity Management, 2.0 was release under IETF as RFC 7643 and 7644



OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol.

Webex Provision

Users Provision

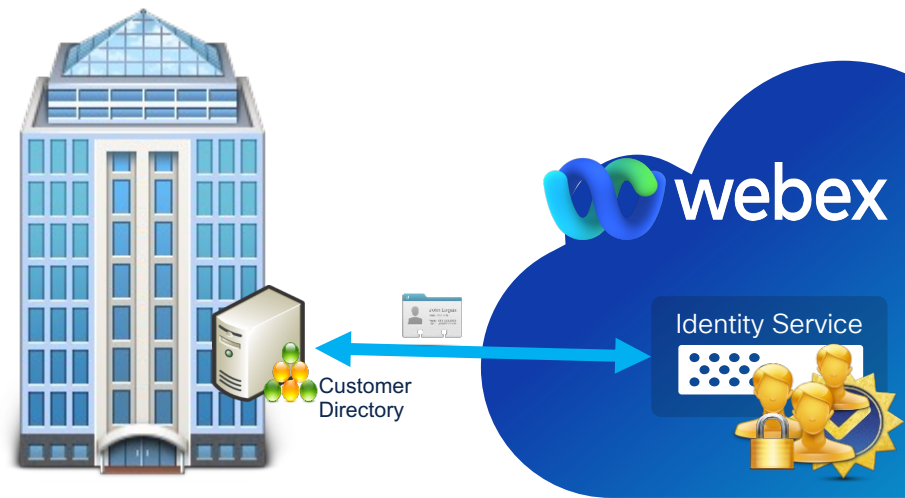
Webex User Account CRUD Operations

Manual or CSV	User Self-Enrollment or Invite	Directory Connector
SCIM Entra Wizard OKTA Synchronization	People API	Account Linking
CUCM Provision	SAML JIT	Social Login

CRUD – Create, Read, Update and Delete

Directory Connector

- Full synchronization and incremental synchronization
- Scheduled synchronization
- Multiple Domains/Forests supported
- LDAP filters
- Dry Run
- User Attribute Mapping and modifications
- Using Service Account or User Account
- Avatar Sync
- Troubleshooting
- Auto-upgrade
- High Availability (HA)



Webex Directory Connector

What is new ?

- Contacts Synchronization
- Uses Edge browser for authentication
- Remove synchronization of Distribution groups, only security groups going to be supported going forward.
- Allows the permanently delete users after soft delete

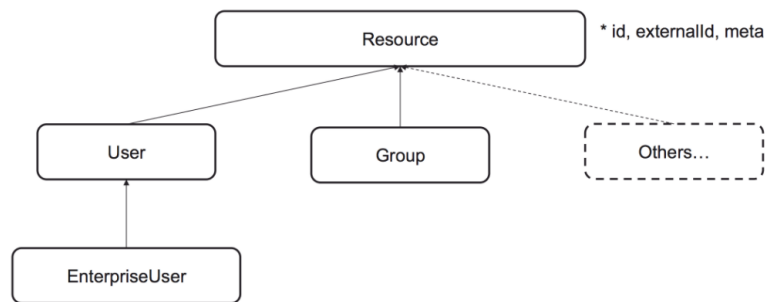


What is SCIM ?

The System for Cross-domain Identity Management (SCIM) specification is designed to **make managing user identities in cloud-based applications and services easier**.

Its intent is to **reduce the cost and complexity** of user management operations by providing a common user schema and extension model, as well as binding documents to provide patterns for exchanging this schema using standard protocols. In essence: make it fast, cheap, and easy to move users in to, out of, and around the cloud.

Normally we will see a Model like :



<http://www.simplecloud.info/>

SCIM

Differences between SCIM 1.1 to SCIM 2.0

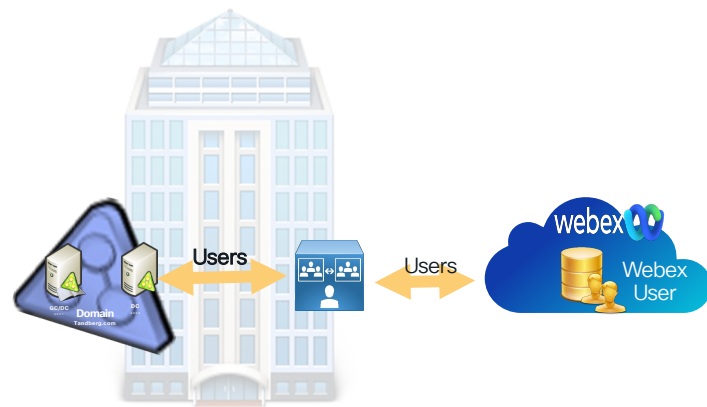
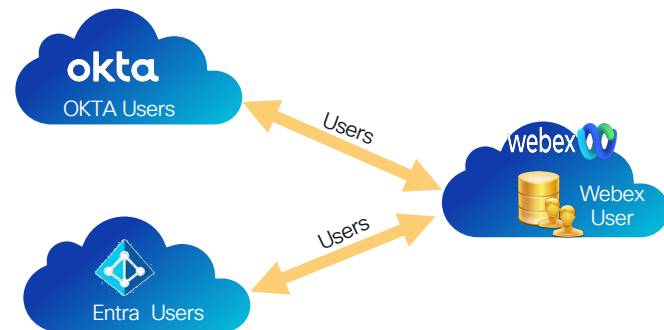
- SCIM 2.0 APIs provide **additional methods** that are not available with SCIM 1.1 (e.g., additional search filters for filtering users).
- The SCIM 2.0 **schema supports more fine-grained requirements**.
- There is more **focus on feature development** for SCIM 2.0 APIs.
- SCIM 2.0 implementation is more **standardize** across different vendors



SCIM

When Comparing with Directory Connector

	SCIM 1.1	Directory Connector
Create, Delete and Update	✓	✓
Allows local Webex Users Creation	✓	✗
Attributes Synchronize	✓ (15)	✓ (27)
Room Systems	✗	✓
Groups	✓	✓
Force re-auth when user change password	✗	✓
Dry-Run	✗	✓
Soft-Delete	✓	✓
Avatars	✗	✓



SCIM 2.0 Users & Groups

Public API

- Implementing the SCIM 2.0 for interoperability with SCIM 2.0. clients, **it allows for better interoperability with external Identity Providers** supporting the SCIM 2.0 standard such as Okta, Microsoft, Oracle, ForgeRock, Ping and others.
- Customers and partners need the ability to automate the provisioning of users and groups from their data stores.
- Using a **standard enables our customers simplifies interoperability** for our customers and customer services already adopting SCIM 2.0 for user management

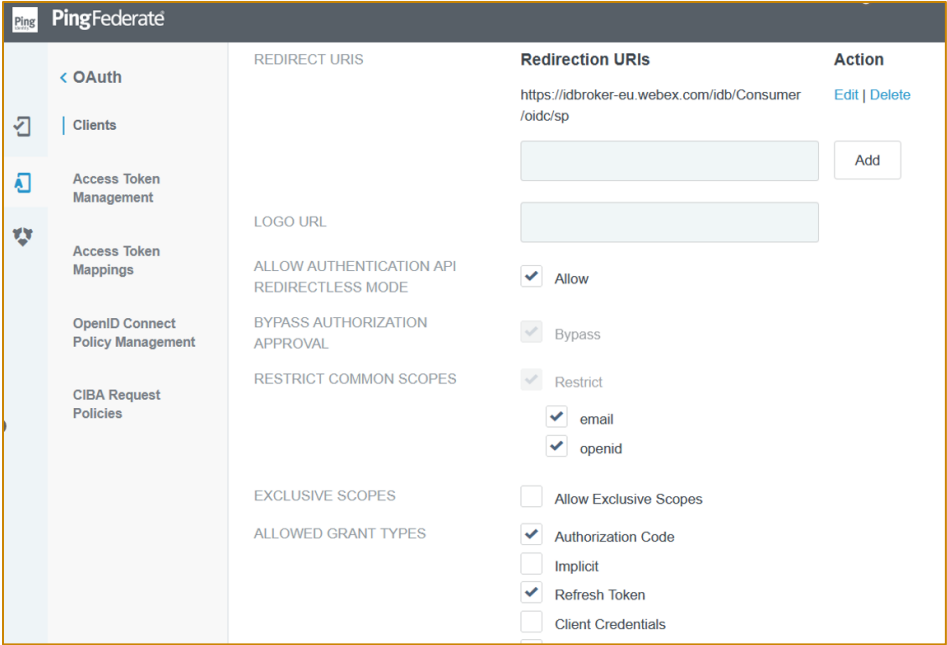
Please also see the SCIM Specification. The schema and API design follows the standard SCIM 2.0 definition with detailed in SCIM 2.0 schema and SCIM 2.0 Protocol.

Resource Group	Method	Description
Memberships		
Resource Groups		
Roles		
Room Tabs	POST https://webexapis.com/identity/scim/orgid/V2/Users	Create a user
Rooms	GET https://webexapis.com/identity/scim/orgid/V2/Users/{userId}	Get a user
SCIM2-User	GET https://webexapis.com/identity/scim/orgid/V2/Users?filter={filter}&attributes={attributes}&includedAttributes={includedAttributes}&sortBy={sortBy}&sortOrder={sortOrder}&startIndex={startIndex}&count={count}&returnGroups={returnGroups}&includeGroupDetails={includeGroupDetails}&groupUsageTypes={groupUsageTypes}	Search users
	POST Create a user	
	GET Get a user	
	GET Search users	
	PUT Update a user with PUT	
	PATCH Update a user with PATCH	
	DELETE Delete a user	
Session Types		
Site		

SCIM 2.0 Users & Groups

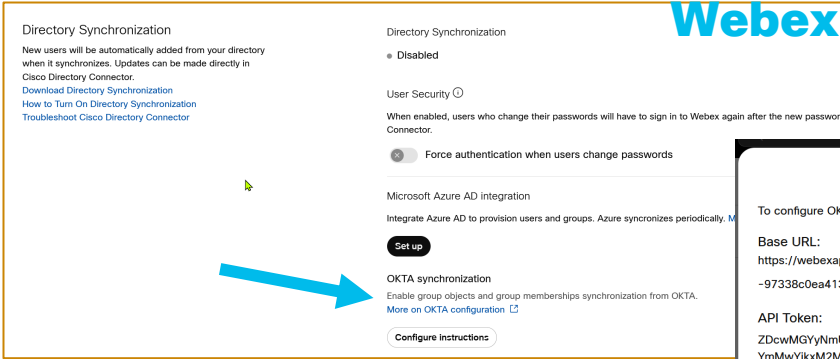
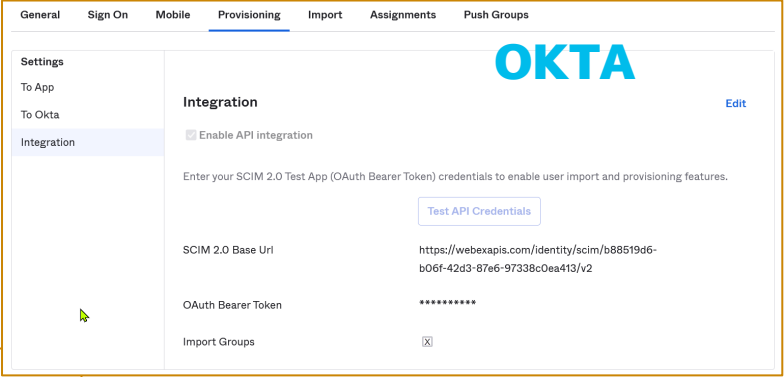
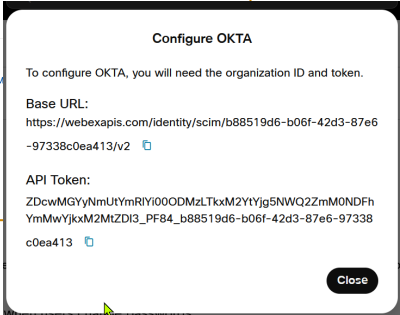
SCIM integration with IdMs

- SCIM 2.0 will allow us to interface with many IDMs available in the market and will allow us to do integration with customer developed Identity Systems.
- Will deliver a much simpler and standardize way of bringing user and group identity objects to Webex platform.



Okta Synchronization

- Simplification the process to obtain **SCIM Server URL in Webex**
- Simplification the process to obtain **API token with the validity of 1 year**
- Okta template for Webex is configure also to **support groups**



Webex Provision

Groups Provision

Webex Groups CRUD Operations

Manual or CSV	Directory Connector
Entra Wizard	Group API
SCIM 2.0	

CRUD – Create, Read, Update and Delete

What is a group?

What's a group?

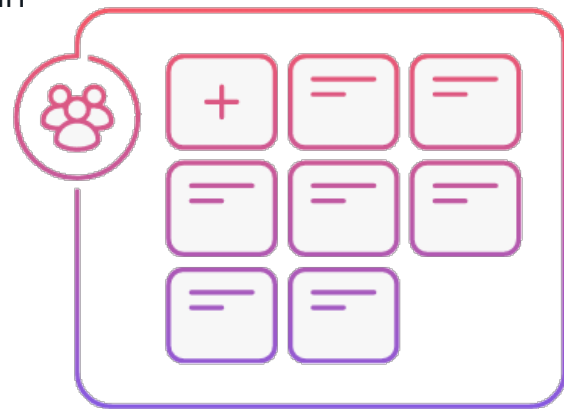
- Use groups to **organise similar users and bulk manage user** assignments, settings templates and resources. For groups based in specific areas (such as physical office buildings and sites), we recommend using locations.

Why use groups?

- Easy bulk management for user assignments (**setting templates, licences and embedded apps**).
- **Automatic assignments** save time, instead of manually editing individual users.

Who can manage groups?

- Full administrators and user administrators can manage groups.



Manage Groups

Using APIs

The screenshot shows the 'webex for Developers' documentation page. The left sidebar lists various API categories: BroadWorks Subscribers with Precheck APIs, BroadWorks Workspaces, Call Controls, Device Configurations, Devices, Events, Groups, and Historical Analytics. The 'Groups' category is selected. The main content area is titled 'Groups' and contains a paragraph explaining that groups contain a collection of members in Webex. Below this, there is a table of API endpoints for managing groups.

Method	Description
POST https://webexapis.com/v1/groups	Create a Group
PATCH https://webexapis.com/v1/groups/{groupId}	Update a Group
GET https://webexapis.com/v1/groups/{groupId}	Get Group Details
GET https://webexapis.com/v1/groups	List and Search Groups
GET https://webexapis.com/v1/groups/{groupId}/members	Get Group Members
DELETE https://webexapis.com/v1/groups/{groupId}	Delete a Group

<https://developer.webex.com/docs/api/v1/groups>

Benefit:

- Manage groups via an API to organize users into containers.

Key Capabilities

- **Create** allow the creation of groups
- **Delete** allow to delete groups
- **Update** allows to update group members
- **List** allows for listing and search for groups
- **Get group** allows to get details of a specific group

Manage Groups

Using Entra Wizard

Configuring Entra Wizard to synchronize **groups and children's groups** from Entra by using the Graph API

Groups updates happen every **12 hours**, since it uses **Graph API**

Microsoft Azure Active Directory Wizard app

Integrate Azure AD to provision users and groups. Azure AD integration requires permission from your Microsoft 365 account. [Learn more about Azure AD set-up](#)



Connector blocks Azure AD. To switch and sync Azure AD, turn off Director... [Show More](#)

Instance name	Job status	Auto sync
> Cisco Webex Identity	● Active	

Microsoft Azure AD integration

Attributes Users Groups **More**

Options

- ☒ Sync user avatars
- ☒ Sync group objects 
- ☒ Activate single sign-on
- ☒ Identify and sync room objects

Groups

 Webex groups  Synchronised groups

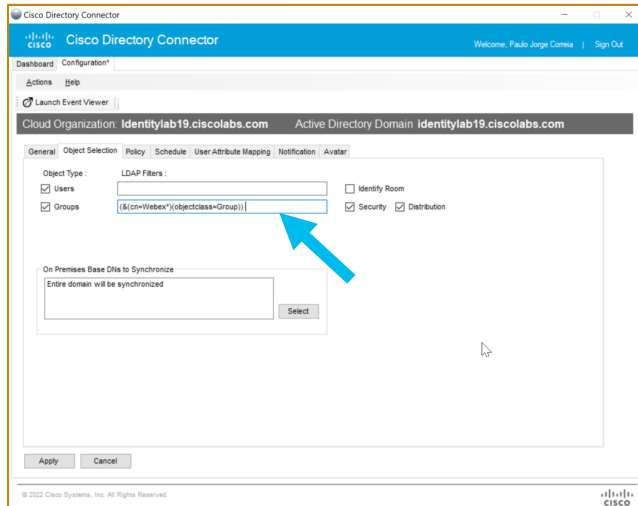
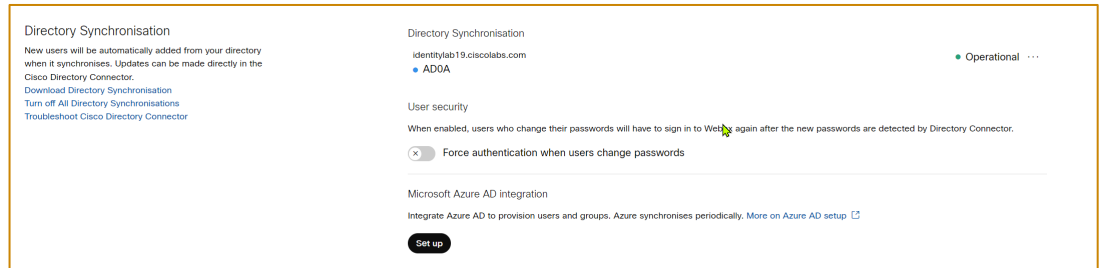
4 groups

Name ↑	Source ⌵	Last Modified ⌵
NewGroup	Azure Active Directory	14/11/2023
Sub_Webex_Users_Azure_group	Azure Active Directory	29/11/2023
Webex_Users_AD_Group	Azure Active Directory	14/11/2023
Webex_Users_Azure_group	Azure Active Directory	24/11/2023

Manage Groups

Using Directory Connector

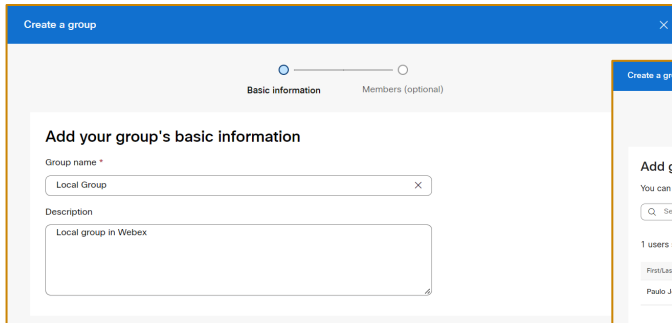
- Deploying Directory Connector in AD Domain to get groups from Active Directory



Manage Groups

Using manual creation

- Groups locally created in Control Hub
- Can be created even if this Webex ORG is using [Entra Wizard](#) or [Directory Connector](#).



Basic information

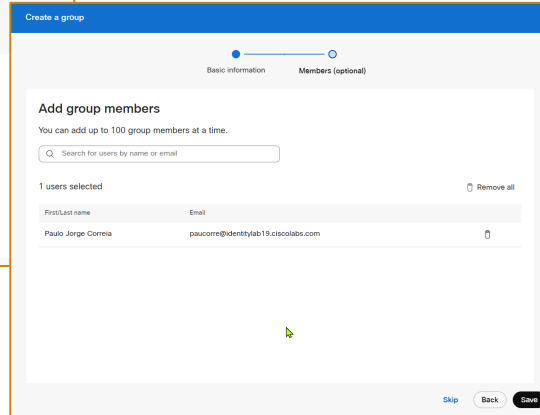
Add your group's basic information

Group name *

Local Group

Description

Local group in Webex



Members (optional)

Add group members

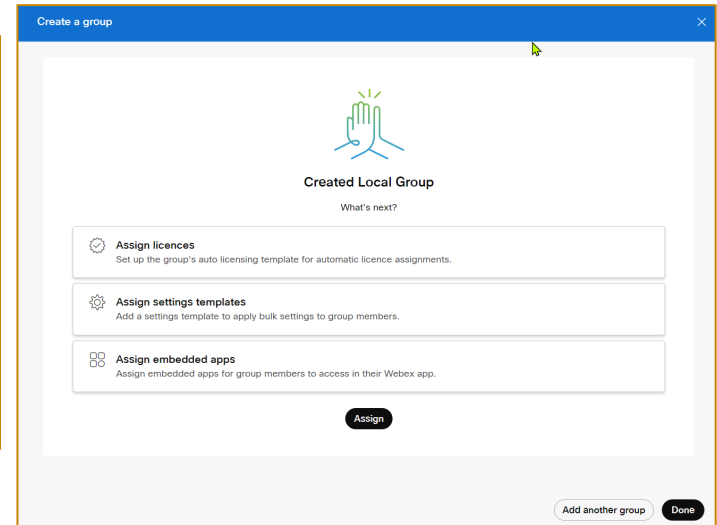
You can add up to 100 group members at a time.

Search for users by name or email

1 users selected

First/Last name	Email
Paulo Jorge Correia	paucoor@identitylab19.ciscolabs.com

Skip Back Save



Created Local Group

What's next?

- Assign licences
Set up the group's auto licensing template for automatic licence assignments.
- Assign settings templates
Add a settings template to apply bulk settings to group members.
- Assign embedded apps
Assign embedded apps for group members to access in their Webex app.

Assign

Add another group Done

Manage Groups

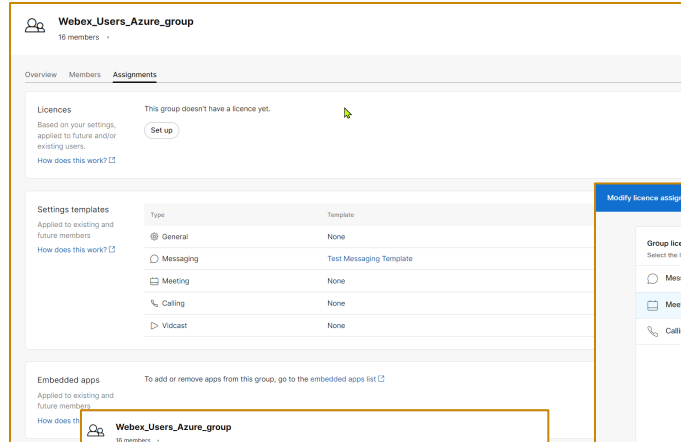
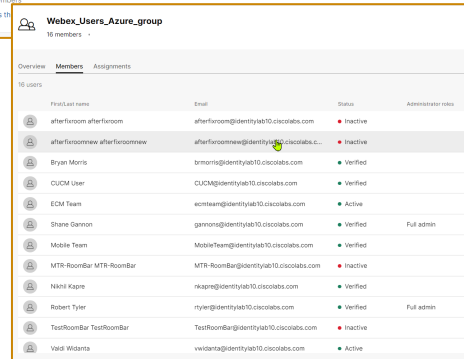
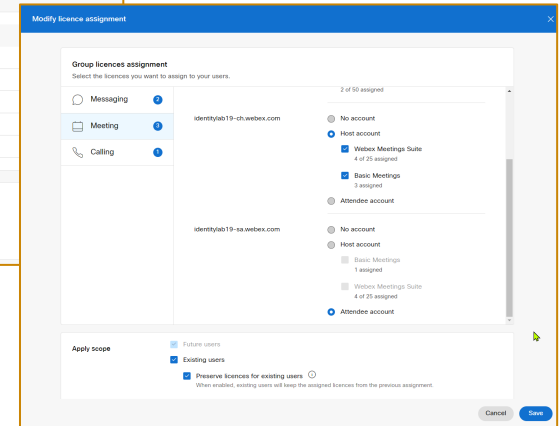
Allows to assign users, Feature template, Licenses and Embedded Apps

No matter how the groups are created, and its members now assign:

- Licenses .
- Feature Templates.
- Embedded Apps

Licenses assignment can apply to future users or also to existent users.

Now it allows admins to set up **both org-level and group-level auto licensing**



Webex Provision

Other Provision Features

Delete inactive users

Inactive users by default are deleted after 30 days.

An inactive user can't login, and all his Access Tokens are not valid.

Default behavior can be changed

First / Last name	Email	Status	Administrator role
A Correia	acorrela@identitylab18.ciscolabs.com	Active	Full admin, Adv
C Correia	ccorreia@identitylab18.ciscolabs.com	Inactive	
Paulo Jorge Correia	pauccorre@identitylab18.ciscolabs.com	Active	Full admin, Adv

Manage inactive user
Customise support information under Support Options in the Webex app.

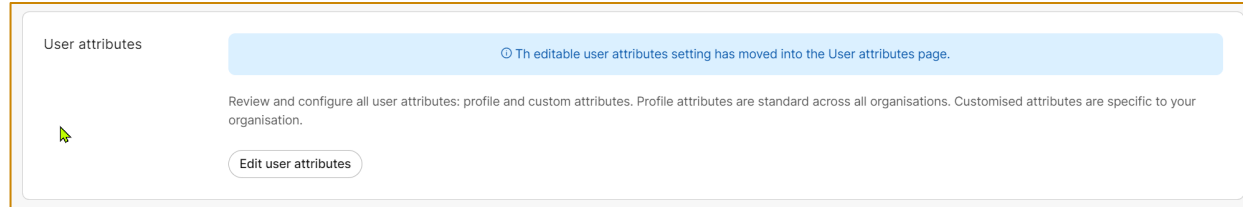
Delete inactive user
After a user is deactivated manually or through directory synchronisation, the user will be deleted from Control Hub after 30 days by default. This feature only works when directory synchronisation is turned off.
 Days

User Attributes

Mandatory attributes

Users attributes can be configured in Webex.

If you mark custom attributes as **required**, then provision mechanisms need to fill it or the onboarding **will fail**, proceed with caution before marking custom attributes as required.



User attributes

Review and configure all user attributes: profile (standard across all organisations), custom and synced attributes.

Pronouns: If you choose to use it in your organisation, it is your organisation's responsibility to use it in line with your policies and values; to educate your users on those policies and to provide the necessary safeguards for its use, such as a channel for users to report abuse.

Profile attributes

Customised attributes

Required user attributes	Identity	Address	Phone
Tick the box to make optional user attributes required.	☒ Email	☐ Address	☐ Work phone
	☐ First name	☐ Town/City	☐ Mobile phone
	☐ Last name	☐ Country/region	☐ Alternative phone 1
	☐ Display name	☐ Postcode	☐ Alternative phone 2
	☐ Title	☐ Country	
	☐ Department	☐ Time zone	

User Attributes

User Editable and Pronouns

Allowing users to change its attributes.

Note: might create conflict with SCIM sources

Allowing pronouns either **created** or **select from a list** by users

Editable user attributes

Your users can edit and populate these profile attributes.

[More on editable user attributes](#)

☒ First and last name

☒ Display name

☒ Profile picture

Pronouns

Please read the [Legal notice about pronouns in Webex](#) and share it with Webex users in your organisation.

[More on admin instructions and the pronouns we support](#)

☒ Allow pronouns

Pronouns are available for both English and non-English users. Note that while users may be able to use the Webex app in Catalan (Spain) and Indonesian, the help page explaining how users can set their pronouns and the external legal notice is not available in these languages. We recommend that you advise these users to not select or input their pronouns and leave the visibility setting as 'Hidden'. [Instructions for how your users can set their pronouns](#)

☒ Selectable by users

Users can select their pronouns via a drop-down menu

☐ Customisable by users

Users can choose to enter customised pronouns via a text field or select their pronouns via a drop-down menu

User Attributes

Custom Attributes

Custom attributes are organization-specific user attributes that you can set up and define for your organization.

You can add custom attributes up to **15 custom attributes**.

< Organisation settings

User attributes

Review and configure all user attributes: profile (standard across all organisations), custom and synced attributes.

Pronouns: If you choose to use it in your organisation, it is your organisation's responsibility to use it in line with your policies and values; to educate your users on those policies and to ensure safeguards for its use, such as a channel for users to report abuse.

Profile attributes Customised attributes

Customised attributes are exclusive to your organisation, and can be configured with specific names and properties. Each attribute name is unique and can't be duplicated for other organisations. You can also assign customised attributes to external users. For more information, see [how to configure customised attributes](#).

⚠ Changes to the customised attributes will affect the meeting site's mapped attributes.

Identifier	Display Name	Required	Locked	Input type	Value list
extensionAttribute1	ca01- Project	☐	☐	Text field	
extensionAttribute2	ca02- Division	☐	☐	Text field	

+ Add a custom attribute

User Attributes

Custom Attributes mapping to tracking codes

In the Webex Meeting configuration, you can map the custom attributes to the tracking codes.

Map tracking code to user attributes

Map this site's tracking codes to user attributes

When mapping tracking codes to user attributes, you can select both custom and profile attributes. You can also edit the scheduling for Webex services (such as meetings and events) after the site's tracking code migration.

Tracking code index	Select attributes for host profile
1	ca01-Division
2	ca02-Project
3	Department
4	Select an attribute
5	Select an attribute
6	Select an attribute
7	Select an attribute
8	Select an attribute
9	Select an attribute
10	Select an attribute

webex Control Hub

Meeting

identitylab10c.webex.com

Sub-prod090822ciscolabs • Control Hub [Delete Site](#)

Settings Site Information

Common Settings

- Account management
- Company Addresses
- Collaboration Meeting Rooms (CMR)
- Site Options
- Disclaimers
- Email Template
- Mobile
- Navigation Customisation
- Audio Settings
- Desktop Application
- Scheduler
- Security
- Session Types
- Branding
- Tracking Codes
- User Privileges
- Personal Meeting Room

Site info

Licences and Users Licences [Redistribute](#)

Meeting

identitylab9.webex.com

trialSub.ae9bc22c-c703-4176-ab85-b7dee93047aa • Control Hub

[Email All Hosts](#)

Settings Site Information **Tracking Codes**

Map tracking codes to user attributes

 **Introducing the new user attribute mapping**

For a more flexible way of specifying tracking codes with user attributes (profile and custom). This also enables **required** tracking codes for new users. For more help, see [how to map tracking codes to user attributes](#).

[Map to user attributes](#)

Alternative email addresses for AuthN and Calendar

Allows that alternative email addresses be use for **Authentication and for Calendar**.

Alternative email address need to have the email domain verified by the Webex ORG in CH

The screenshot shows the 'Users' management interface in the Cisco Webex Admin Center. The user profile for 'identitylab6@identitylab6.ciscolabs.com' is displayed, marked as 'Not Verified'. The 'Profile' tab is active, showing fields for Identity and Address. The Identity section includes First name (Paulo), Last name (Identitylab6), Display name (Paulo at Identitylab6), Primary email (identitylab6@identitylab6.ciscolabs.com), and Alternative emails (Paulo.Correia@identitylab10.ciscolabs.com). The Address section includes Address, Town/City, and Postcode fields.

Identity	
First name	<input type="text" value="Paulo"/>
Last name	<input type="text" value="Identitylab6"/>
Display name	<input type="text" value="Paulo at Identitylab6"/>
Primary email *	<input type="text" value="identitylab6@identitylab6.ciscolabs.com"/>
Alternative emails ⓘ	<input type="text" value="Paulo.Correia@identitylab10.ciscolabs.com"/> ⓘ
+ Add email	
Title	<input type="text" value="Enter a title"/>
Department	<input type="text" value="Enter a department"/>

Address	
Address	<input type="text" value="Enter an address"/>
Town/City	<input type="text" value="Enter a town/city"/>
Postcode	<input type="text" value="Enter a postcode"/>

Hide highly sensitive users from directory

When Turn on, the User and their registered device can't be searched in the Webex App

The screenshot displays the Cisco Webex Admin Center interface for a user named Paulo Jorge Correia. The top navigation bar includes tabs for Summary, Profile, General, Meetings, Calling, Messaging, Hybrid Services, Devices, and Vidcast. The 'Summary' tab is active, showing a list of services and their configurations:

- Calling:** Register to Unified Communications Manager (UCM)
- Contact Centre:** Contact Centre admin
- Edit licences:** A button to manage licenses.
- Administrator roles:** Full admin, Advanced troubleshooting access, Webex site admin
- Security:** Includes a 'Reset Access' button and a description: 'Revoke user-access tokens for the Webex app on desktop, web and mobile. This deletes any cached content and prompts the user to sign in again. [Learn more.](#)'
- Hide from search:** A toggle switch that is currently turned on (blue), indicating the user is hidden from the directory search.

Choose which kind of OS to allow to connect to Webex

Specify which OS where the user can run the Webex App, this allow us to block for example the Web app client.

Configure token policy

Configure token policy for all the Webex clients

Client type	Client access	Refresh token TTL	Max. num of refresh tokens	Access token TTL
IOS	☒ Allowed	<input type="text" value="1440"/> hour(s)	<input type="text" value="100"/> token(s)	<input type="text" value="1080"/> minute(s)
Android	☒ Allowed	<input type="text" value="1440"/> hour(s)	<input type="text" value="100"/> token(s)	<input type="text" value="1080"/> minute(s)
MAC	☒ Allowed	<input type="text" value="1440"/> hour(s)	<input type="text" value="100"/> token(s)	<input type="text" value="720"/> minute(s)
Windows	☒ Allowed	<input type="text" value="1440"/> hour(s)	<input type="text" value="100"/> token(s)	<input type="text" value="720"/> minute(s)
Web Client	☒ Denied	<input type="text" value="1440"/> hour(s)	<input type="text" value="100"/> token(s)	<input type="text" value="720"/> minute(s)

Webex Provision

Entra Wizard

Microsoft Entra

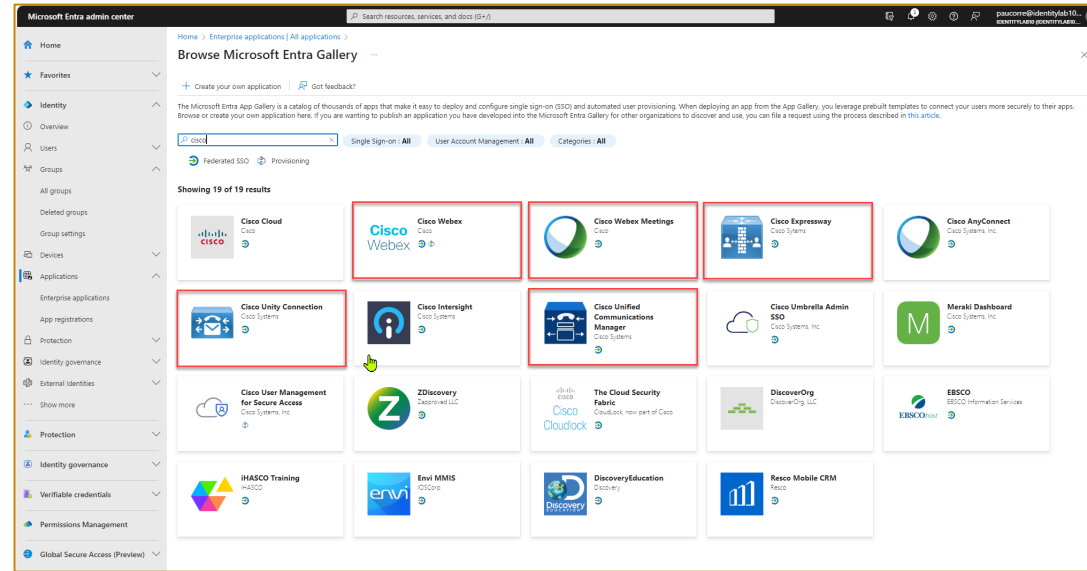
Cisco Applications in Entra



Today when we **manually add a new application** from the Entra Enterprise Application catalogue we see 5 Cisco Collaboration Application.

But this doesn't mean that we only have this applications in Entra Enterprise Applications.

These are the application that **can be manually added** by the system administrator to the Entra Enterprise Applications.





Microsoft Entra

Cisco Applications in Entra

The other application from Cisco Collaboration are created when our **developers use the MS Graph API** and automatically added in the Entra Enterprise Applications catalogue.

Name	Object ID	Application ID	Homepage URL	Created on
EPCS	0d3a64b0-9b78-4838-82...	0126c03c-3f55-41fe-9a6...	https://account.activedir...	26/02/2021
Cisco Unified Communications Manager	103e0258-c244-4edc-a1f...	177805c-ee27-4e0a-a7b...	https://FQDN/CUCMmode...	15/02/2023
Cisco Webex Video Integration for Microsoft Teams	16966c08-7a1e-4b5f-96a...	98a39cf3-3a89-4856-91b...	https://cisco.com/go/web...	25/04/2022
Webex Enterprise Content Management	26ca9837-a70d-4ae4-b6...	40830e92-8323-4b43-ab...	https://www.webex.com/...	26/04/2022
Microsoft Photos	42c0f78b-e419-42be-86...	0ec20138-5a70-4a33-b2c...	https://www.microsoft.co...	01/02/2022
Cisco Webex Office 365 Groups	471f0699-ee0f-4473-a245...	c48a08e1-ee3e-47f5-851...	https://www.webex.com	09/09/2021
Jabber	575281b0-8494-43f2-b8...	223864e0-6b61-4867-ac7...		25/04/2022
Cisco Webex for Intune	62d0f9e6-8389-43a6-99b...	ee0f98b0-011c-4d44-9ac...	https://help.webex.com/...	19/07/2022
Cisco Webex Meetings	7990f5d9-f0f3-4aee-994e...	80f9c320-e55f-434f-99e...		03/11/2020
Cisco Webex Teams	854ae259-ac9a-47f5-66...	1121e43c-95eb-4070-b3...	https://www.webex.com	19/07/2022
Webex Calendar Service	859462bd-00aa-4ee9-bd...	1a3fa2f3-d202-456a-9e3...	http://www.cisco.com/go...	25/04/2022
ExpiCQ Identitylab10 Cluster	8af27b56-2699-441e-9c4...	87592270-f171-4339-ba7...	https://account.activedir...	10/11/2020
Cisco Webex Identity	8e514701-b3c4-40a5-998...	75969e8b-8b47-4c13-9d...	https://ldbroker.webex.co...	03/07/2023
Lync/Outlook Identitylab10 Cluster	8e077e8b-04c5-4e41-b1...	229c434c-e991-4ae0-835...	https://account.activedir...	10/11/2020
Cisco Webex Identity Integration	a46b0eac-61fe-4999-b46...	90b9942a-c1eb-4e8d-92...	http://webex.com	03/07/2023
Cisco Unified Communications Manager	bbba046c-ea99-4015-81...	a2100f41-7af3-41b3-9a2...	https://FQDN/CUCMmode...	08/05/2023
Graph explorer (official site)	c3758733-7c0b-4b68-86...	d8b0c8b5-d9f9-48b1-a8a...	https://developer.micros...	15/12/2020
Webex Call	c8d9c8d2-4b42-42c0-ba...	9a7ce614-bdcd-4640-aa...		08/09/2021
Cisco Webex Meetings uc5devlab13	f449d8cd-0ffc-4765-6290...	b885526a-f113-4660-a7...	https://www.webex.com/...	25/04/2022
Cisco Webex Scheduler	fa282b0b-00ba-4509-9aa...	7a91a319-a65d-4a0b-90...	https://webex.com	26/04/2022
EPCS @ Microsoft	fbaa6d67-bda7-490f-b2b...	a9a0b19a-0128-4d6f-924...		26/02/2021
Cisco Webex Connect Your Calendar	feaf2a22-480d-48da-8d7...	98204440-5d81-4ab6-83...	https://webex.com	25/04/2022

Microsoft Entra

Cisco Applications in Entra



Application
created
using MS
Graph API

Entra Enterprise application	App ID
Webex Teams Enterprise Content Management	40830e92-8323-4b43-abd5-ca6b81d39b75
Cisco Webex Office 365 Groups	c4a8d8e1-ee3e-47f3-8514-2a4e6fea5b5c
Webex Calendar Service (Admin Consent)	1e3faf23-d2d2-456a-9e3e-55db63b869b0 189ea49b-75a4-4e53-a013-2aed74803405
Cisco Webex Connect Your Calendar (User Consent)	98204440-5c81-4ab6-8353-ef68d1b53ee3
Cisco Webex Meetings (for MS Teams)	80f3c320-e55f-434f-98e8-d798dfcbe182
Cisco Webex Scheduler (Meetings scheduler for Outlook)	7a91e319-a65d-4ceb-909b-12203561dbf5
Cisco Webex Social Login	280851f2-bc68-4362-91e9-3c44b3a29049
Webex Call (for MS Teams)	9a7ce614-bdc8-4640-aaea-d8c626c58966
Jabber (for MS Teams)	223b6ef0-6b61-4867-ac7f-9eccc7413b46
Cisco Webex Identity (CH Entra Wizard)	f6016c4c-c015-453c-8ea6-dfc146f7eb7f
Cisco Webex Identity Synchronization (CH Entra Wizard)	90db942a-c1eb-4e8d-82e4-eebf64a7e2ae
Cisco Webex Identity Integration for Migration (CH Entra Wizard)	fd578ab1-1f5b-49c9-8d3d-b5ffee28d187
Cisco Webex for Intune	ee0f8f6b-011c-4d44-9cac-bb042de0ab18
Cisco Webex Video Integration for MS Teams (CVI)	7968d647-6a0f-4476-8931-206eff6c4d55

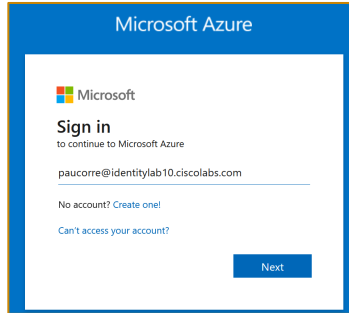
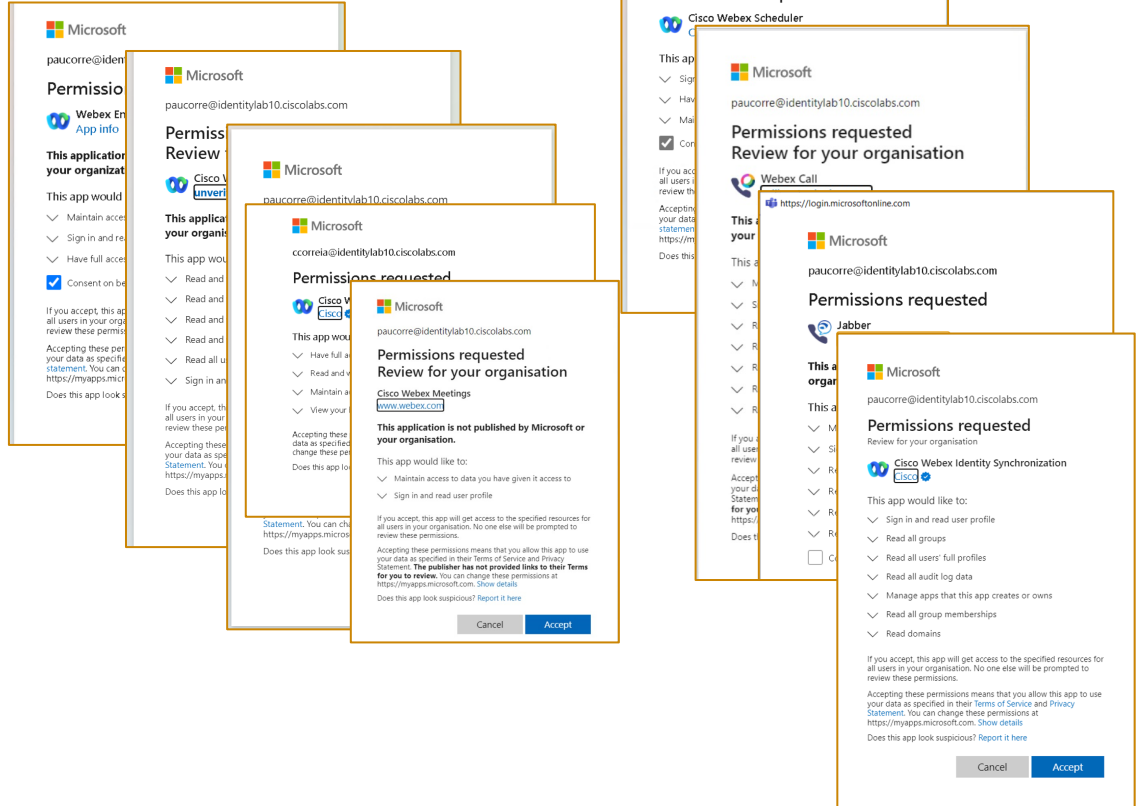


Microsoft Entra

Consent given by Administrators or Users

Those applications require that the **Administrator or Users to authenticate in Entra.**

Consent to have access to specific information will be request before the application is created in the catalogue.





Microsoft Entra

Consent given by Administrators or Users

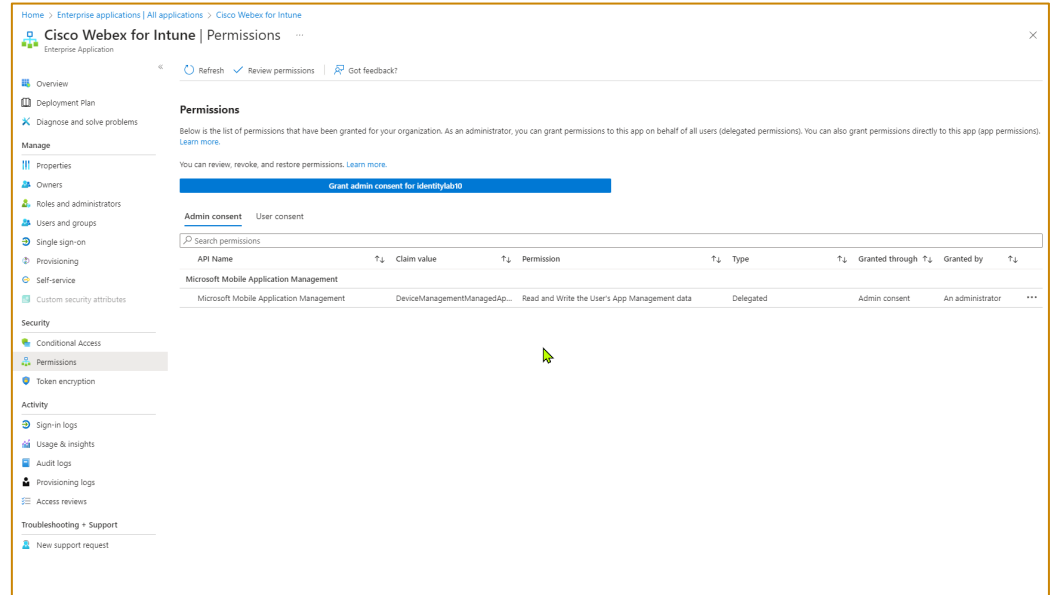
Sometimes the users in Webex **doesn't has permission to allow consent as an administrator** in Entra.

It is possible in the desktop of the Entra admin to allow consent to application that is not created yet.

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent>

We can grant manually the admin consent for an application

https://login.microsoftonline.com/organizations/v2.0/adminconsent?client_id=ee0f8f6b-011c-4d44-9cac-bb042de0ab18&redirect_uri=ms.com.aksc.teams://auth&scope=https://wip.mam.manage.microsoft.us//DeviceManagementManagedApps.ReadWrite



Microsoft Entra

Entra Wizard



Cisco Wizard from Control Hub that will configure the [Webex Identity integration in Entra Portal](#).

Bring additional functionalities to what SCIM protocol can deliver.

[Doesn't require any knowledge](#) on Entra configuration, and providing a straightforward integration for [Provision](#) and [Single Sign-On](#)

Microsoft Azure Active Directory Wizard app

Integrate Azure AD to provision users and groups. Azure AD integration requires permission from your Microsoft 365 account. [Learn more about Azure AD set-up](#)

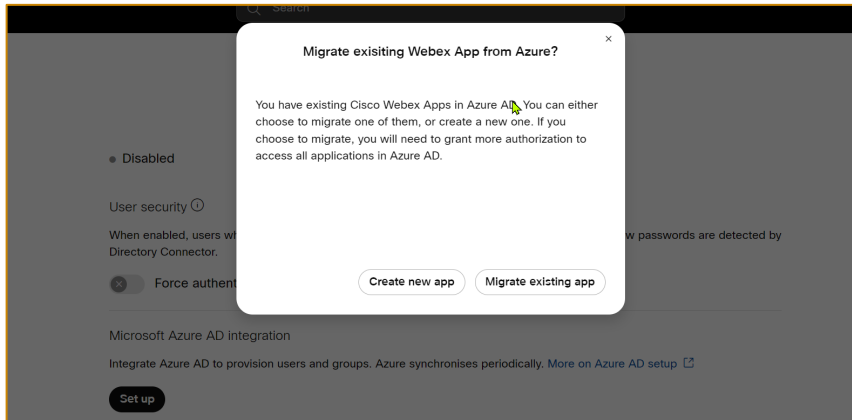
☒

Connector blocks Azure AD. To switch and sync Azure AD, turn off Director... [Show More](#)

Instance name	Job status	Auto sync	
> Cisco Webex Identity	● Active	☒	⋮

Microsoft Entra

Entra Wizard



Entra Wizard allow us to **migrate** existent application that does User Provision using SCIM and SSO using SAML or **create a new integration**.

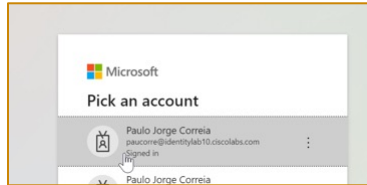
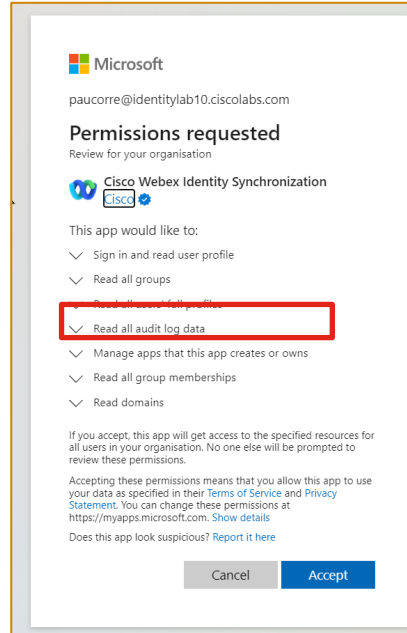
When doing the migration, **we add the benefits of MS Graph APIs** (Avatar, dry run, provision on demand, groups, Etc.) to the SCIM provision

Microsoft Entra

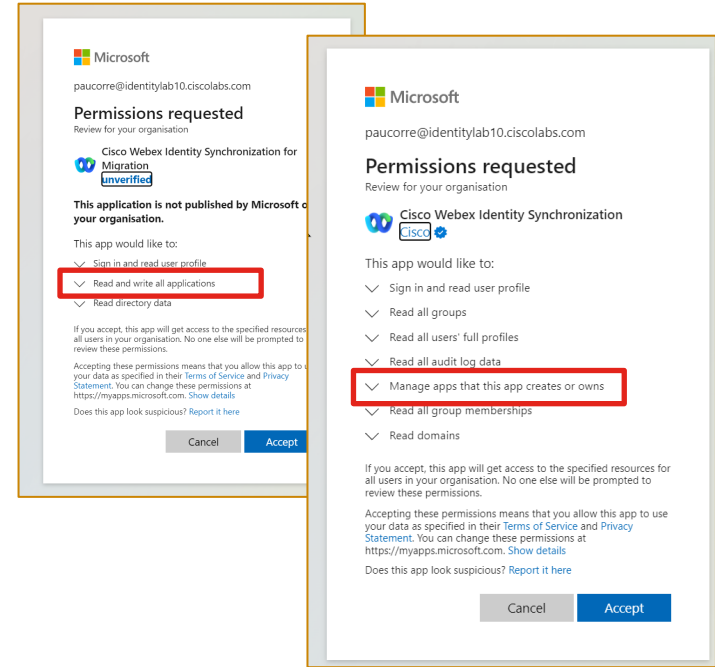
Entra Wizard



Uses Graph API to
configure Entra
portal, and for that
requires permissions



Permission to create
a **new application**



Permission for **Migration of
an existent application** in
Entra Enterprise Applications

Microsoft Entra

Entra Wizard



Attributes Users Groups More

displayName	▼	displayName
givenName	▼	name.givenName
surname	▼	name.familyName
jobTitle	▼	title
objectId	▼	externalId
telephoneNumber	▼	phoneNumbers[type eq "work"].value
mobile	▼	phoneNumbers[type eq "mobile"].value
facsimileTelephoneNumber	▼	phoneNumbers[type eq "fax"].value
streetAddress	▼	addresses[type eq "work"].streetAddress
postalCode	▼	addresses[type eq "work"].postalCode
usageLocation	▼	addresses[type eq "work"].usageLocation
state	▼	addresses[type eq "work"].state
city	▼	addresses[type eq "work"].city
manager	▼	manager

Microsoft Azure AD integration

Attributes Users **Groups** More

Select groups

Sync group members Sync children groups

Webex will sync these child groups and the members.

Search Select groups 1 groups selected

Group name	Group type	Group object ID
Webex_Users_Azure_group	Security	51a0a6dc-0c8e-420d-b832-293e5289ed61
Hide groups		
Sub_Webex_Users_Azure_group	Security	0629a802-9428-4660-85a6-f543f5744427

Microsoft Azure AD integration

Attributes **Users** Groups More

Select users

Search Select users Select all users 0 users selected



You haven't added any users yet

Use the search bar to select individual users, or sync all users.

Cancel Save

Allow us to map attributes.

Select the users or groups of users that you want to synchronize with Webex.

Manager attribute is possible now

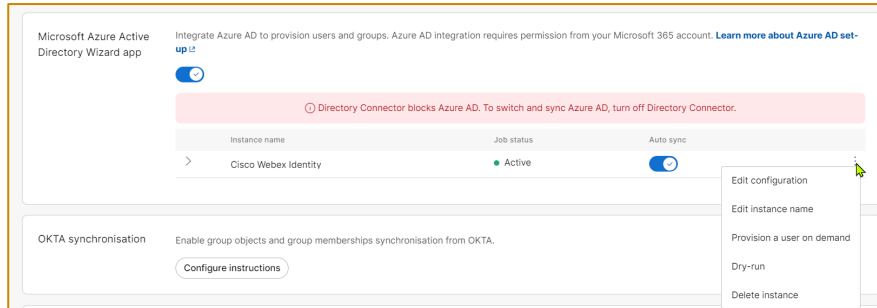
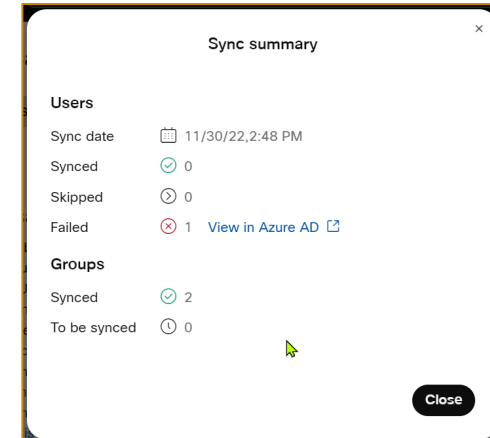
Microsoft Entra

Entra Wizard



Wizard has many capabilities that allows administrators to control the integration from Webex Control Hub:

- Allows us to define the name of the Entra application
- Provision Users on-demand
- Dry-run
- Delete integration
- Check Sync Summary



Microsoft Entra

Entra Wizard



Domains

Domains

Add, verify, or claim domains for added security in your organisation. Add them manually or with Azure AD. Azure AD has already verified the domains.

Learn more about the [add, verify and claim domain process](#).

Domain	Status	
identitylab10.cis...	● claimed	...

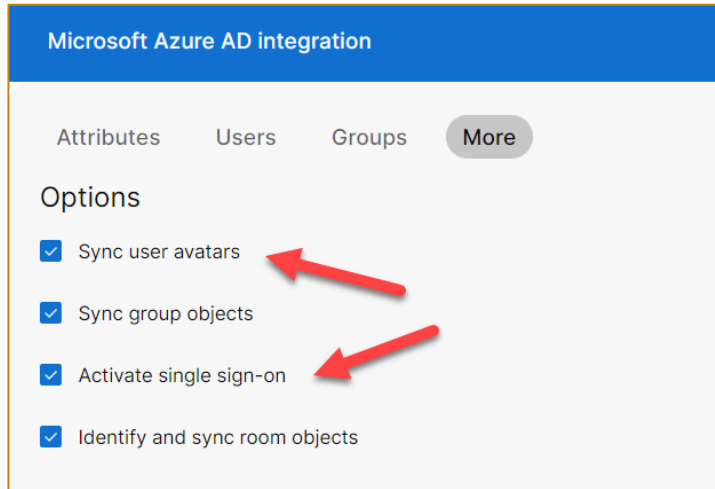
Add manually

Add with Azure AD

Allow us to import domain verified already in Entra as verified in Webex, with no need to create the DNS SRV record for validation.

Microsoft Entra

Entra Wizard



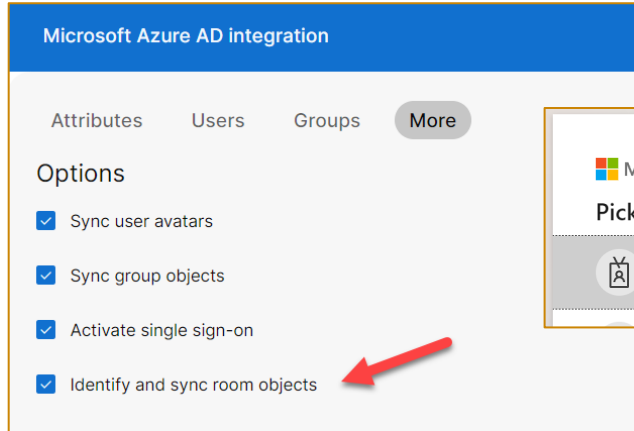
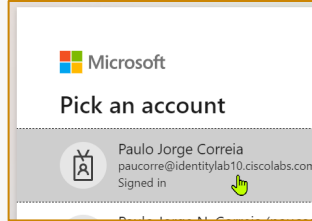
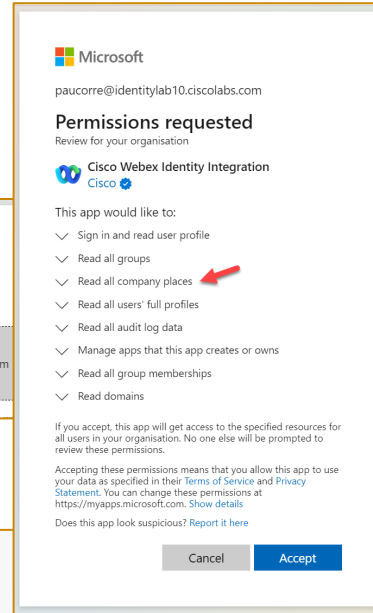
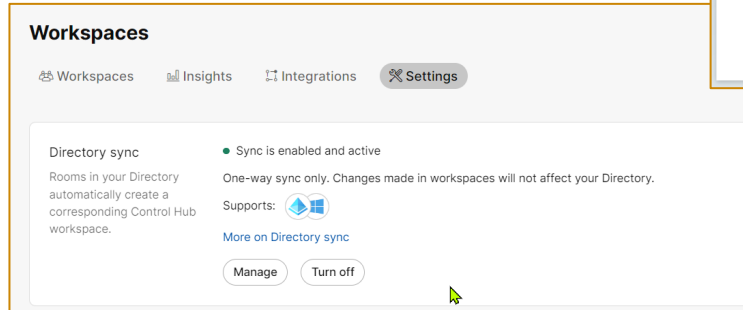
Allow us to sync Avatars.

Can also configure the **SSO integration with Entra using OIDC**, but will be only available for the option of new application.

All the options in **More** tab are achieved using **Graph API**

Microsoft Entra

Workspace synchronization



To allow for Microsoft Rooms objects to be imported, an extension of permission will be needed to accept to **Company places in Entra**

They will be created in CH as **Workspaces**

Microsoft Entra

Entra Wizard



What to see in Entra Enterprise Applications

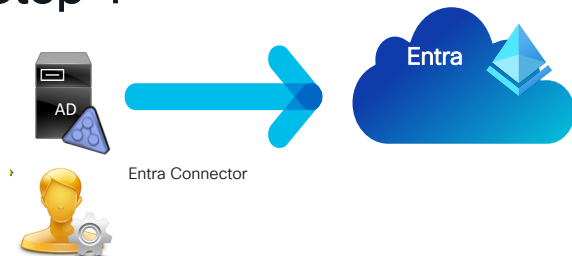
The screenshot displays the Microsoft Azure portal interface, specifically the 'Enterprise applications' section. The left sidebar shows the navigation menu with 'Permissions' selected. The main content area shows a list of applications, with 'Cisco Webex Identity Integration' highlighted. A red arrow points to the 'Provision' button, and another red arrow points to the 'Graph API/OIDC' button. The 'Permissions' tab is active, showing a table of permissions granted to the application.

API Name	Claim value	Permission	Type	Granted through	Granted by
Microsoft Graph	User.Read	Sign in and read user profile	Delegated	Admin consent	An administrator
Microsoft Graph	Application.ReadWrite.OwnedBy	Manage apps that this app creates or owns	Application	Admin consent	An administrator
Microsoft Graph	Group.Read.All	Read all groups	Application	Admin consent	An administrator
Microsoft Graph	User.Read.All	Read all users' full profiles	Application	Admin consent	An administrator
Microsoft Graph	Domain.Read.All	Read domains	Application	Admin consent	An administrator
Microsoft Graph	GroupMember.Read.All	Read all group memberships	Application	Admin consent	An administrator
Microsoft Graph	AuditLog.Read.All	Read all audit log data	Application	Admin consent	An administrator

Where Customers do the Identity Management from Microsoft perspective?

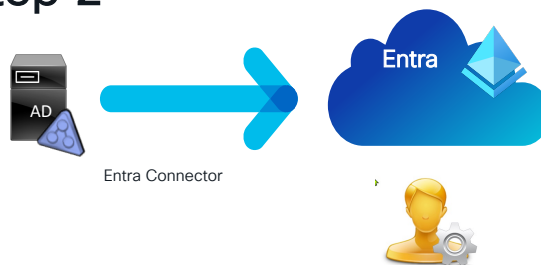


Step 1



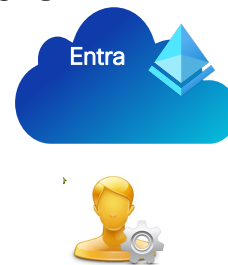
Initially all the Create, Replace, Update and Delete Operations (CRUD) will be done in AD.

Step 2



At some point they will migrate the CRUD operation to Entra and at that point AD is only for Legacy applications, and there will be users in the cloud that no longer exist on-premise

Step 3

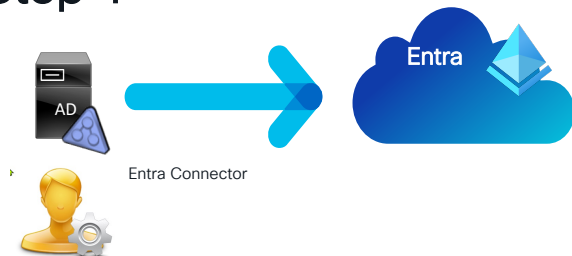


There isn't any longer any AD on-premise

What is Cisco recommendation for each Customer step?

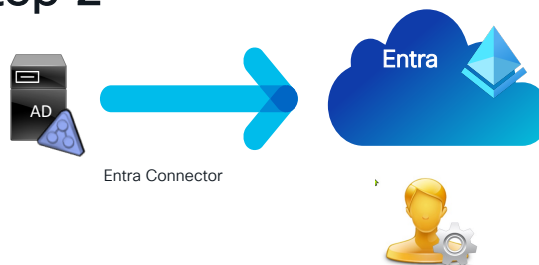


Step 1



Cisco Directory Connector

Step 2



Cisco Entra Wizard
SCIM Manual Configuration

Step 3



Cisco Entra Wizard
SCIM Manual Configuration

How do we Migrate from one to the other ?



- Disable Directory Connector in Webex CH
- Follow instructions in <https://help.webex.com/en-us/article/6ta3gz/Synchronize-Entra-Active-Directory-users-into-Control-Hub>
- When follow the above article make sure that userName is mapped to the same attribute value that was before Directory Connector to uid.



- Disable Directory Connector in Webex CH
- Follow instructions in <https://help.webex.com/en-us/article/heaubez/Set-up-Entra-AD-Wizard-App-in-Control-Hub>
- When follow the above article make sure that userName is mapped to the same attribute value that was before Directory Connector to uid.



Cisco Directory Connector



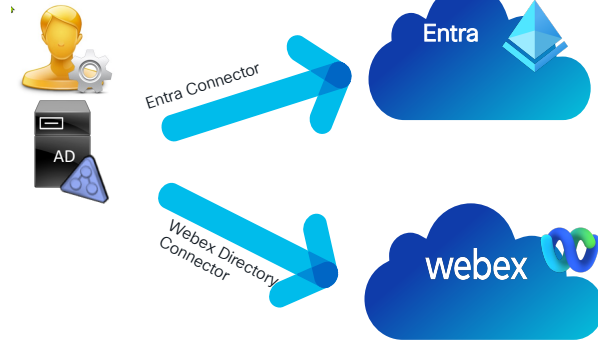
- Follow instructions in <https://help.webex.com/en-us/article/heaubez/Set-up-Entra-AD-Wizard-App-in-Control-Hub>
- You will be given an option to :
 - Migrate Existing Application (SSO using SAML) Entra Wizard
 - Create new Application (SSO using OIDC)
- When follow the above article make sure that userName is mapped to the same attribute value that was before Directory Connector to uid.



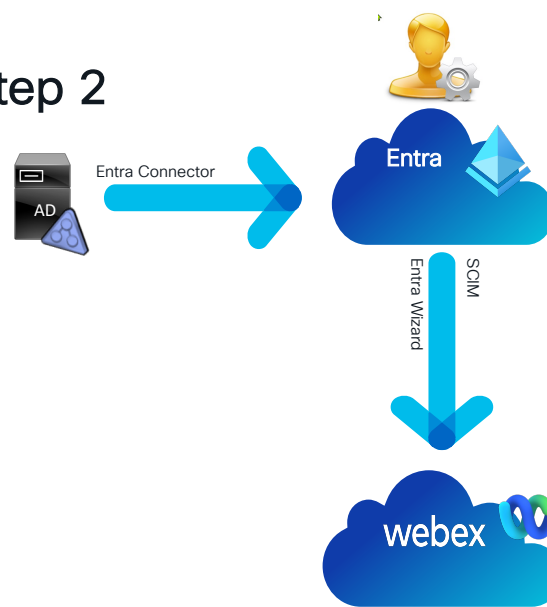
Webex Integration for each step recommendation



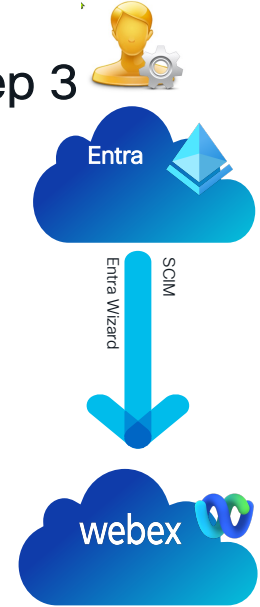
Step 1



Step 2



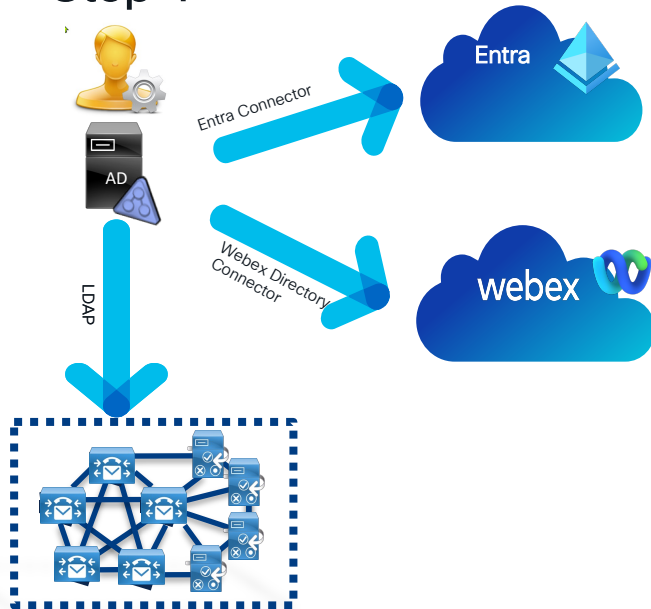
Step 3



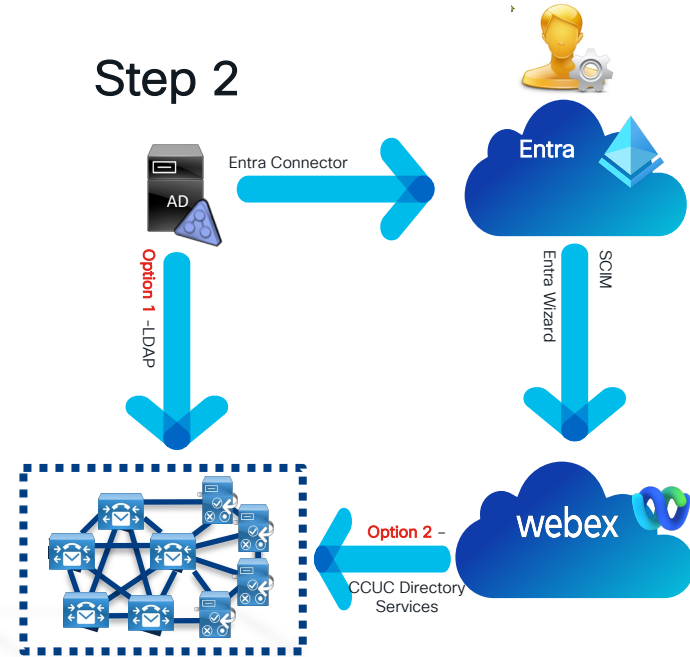
And if the customer still has CUCM and other on-premise services?



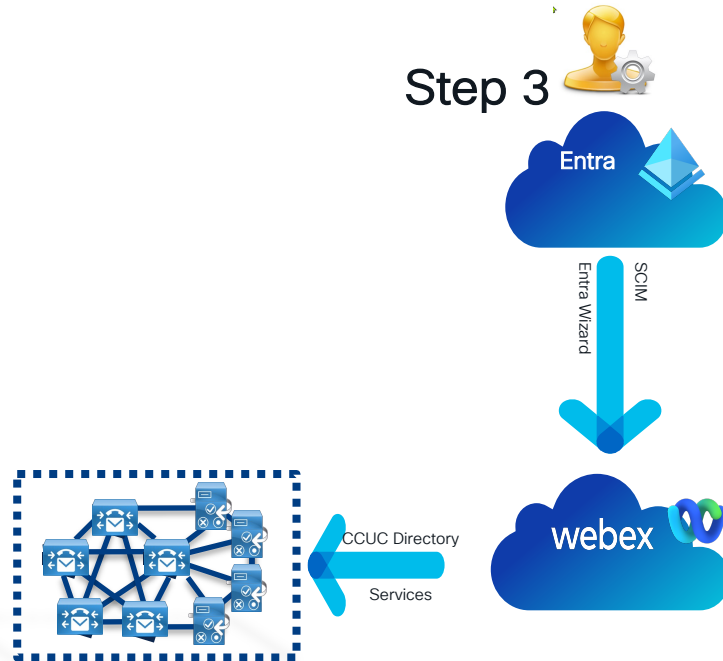
Step 1



Step 2



And if the customer still has CUCM and other on-premise services?

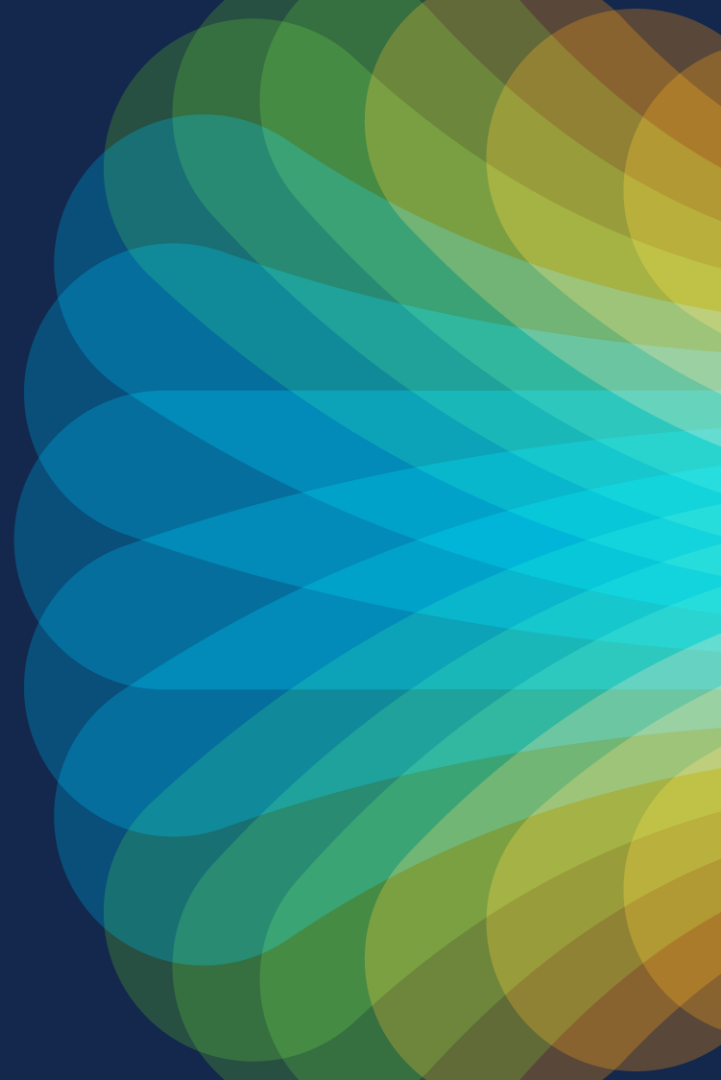


Comparing SCIM, Entra Wizard and Directory Connector

	SCIM 1.1	SCIM 2.0	Entra Wizard	Directory Connector
Create, Delete and Update	✓	✓	✓	✓
Allows local Webex Users Creation	✓	✓	✓	✗
Attributes Synchronize	✓ (15)	✓ (27)	✓ (15)	✓ (27)
Room Systems	✗	✗	✓ *	✓
Groups	✗	✓	✓	✓
Force re-auth when users change password	✗	✗	✓ *	✓
Dry-Run	✗	✗	✓	✓
Soft-Delete	✓	✓	✓	✓
Avatars	✗	✗	✓	✓
Domain Verification	✗	✗	✓	✓
SSO Configuration	✗	✗	✓	✗
On-demand provision	✗	✗	✓	✓
Manager Attribute	✗	✗	✓	✓
Synchronize Contacts	✗	✗	✗	✓

OpenID Connect

how does it work?



What is OpenID Connect ?

OpenID Connect 1.0 is a **simple identity layer on top of the OAuth 2.0** protocol.

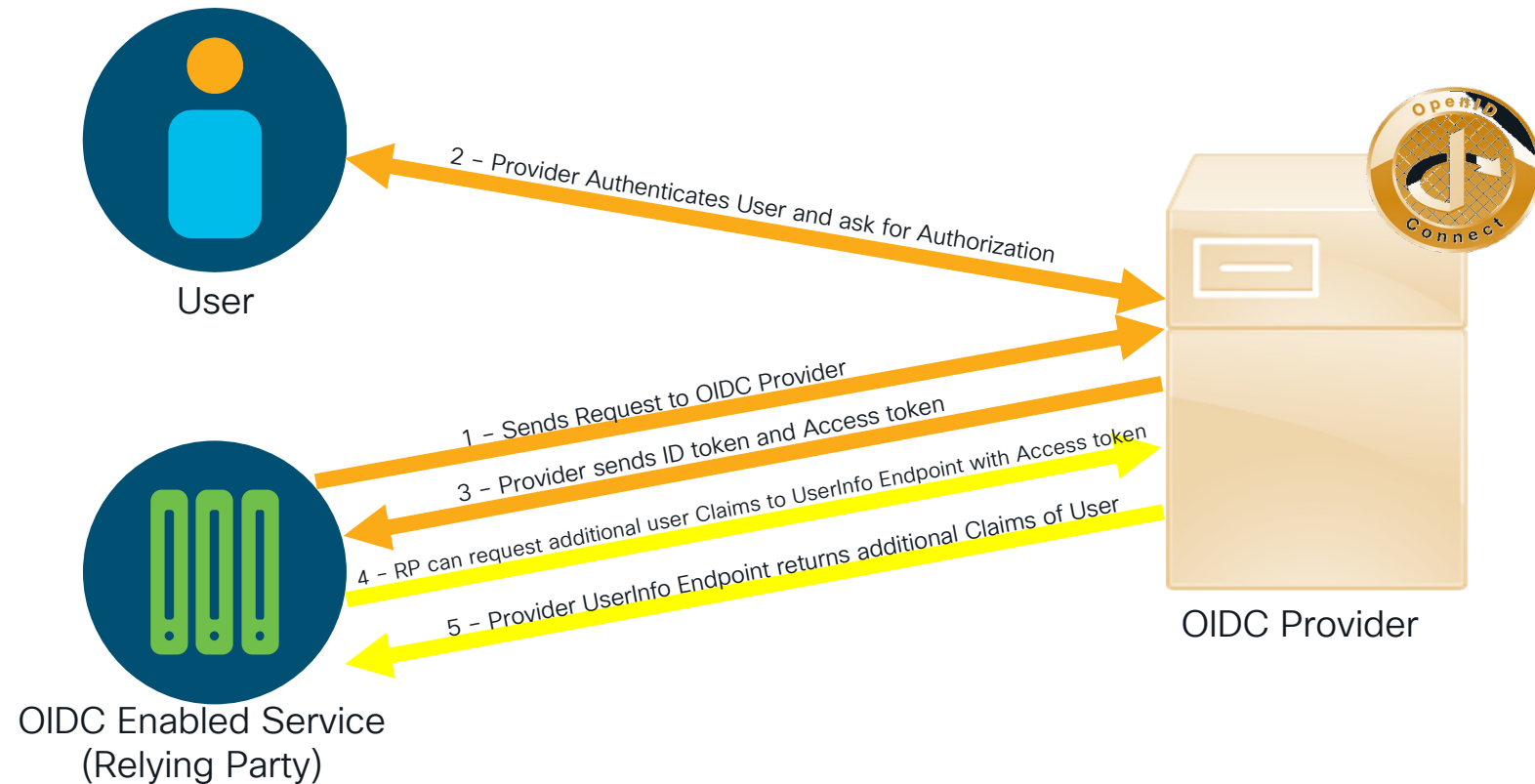
It allows Clients to **verify the identity of the End-User** based on the authentication performed by an Authorization Server.

It allows to **obtain basic profile information** about the End-User in an interoperable and REST-like manner.

The specification suite is extensible, allowing participants to use optional features such as **encryption of identity data, discovery of OpenID Providers, and session management**, when it makes sense for them.



OpenID Connect Flow



CISCO *Live!*

#CiscoLiveAPJC

BRKCOL-2007

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

61

Claims

It also defines a standard set of basic profile Claims.

Pre-defined sets of Claims can be requested using specific scope values or individual Claims can be requested using the claims request parameter.

The Claims can come directly from the OpenID Provider or from distributed sources as well.

More information in

https://openid.net/specs/openid-connect-core-1_0.html#Claims

Example of UserInfo Response

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "sub": "248289761001",
  "name": "Jane Doe",
  "given_name": "Jane",
  "family_name": "Doe",
  "preferred_username": "j.doe",
  "email": "janedoe@example.com",
  "picture": "http://example.com/janedoe/me.jpg"
}
```

Standard Claims

Member	Type	Description
sub	string	Subject - Identifier for the End-User at the Issuer.
name	string	End-User's full name in displayable form including all name parts, possibly including titles and suffixes, ordered according to the End-User's locale and preferences.
given_name	string	Given name(s) or first name(s) of the End-User. Note that in some cultures, people can have multiple given names; all can be present, with the names being separated by space characters.
family_name	string	Surname(s) or last name(s) of the End-User. Note that in some cultures, people can have multiple family names or no family name; all can be present, with the names being separated by space characters.
middle_name	string	Middle name(s) of the End-User. Note that in some cultures, people can have multiple middle names; all can be present, with the names being separated by space characters. Also note that in some cultures, middle names are not used.
nickname	string	Casual name of the End-User that may or may not be the same as the given_name. For instance, a nickname value of Mike might be returned alongside a given_name value of Michael.
preferred_username	string	Shorthand name by which the End-User wishes to be referred to at the RP, such as janedoe or j.doe. This value MAY be any valid JSON string including special characters such as @, /, or whitespace. The RP MUST NOT rely upon this value being unique, as discussed in Section 5.7 .
profile	string	URL of the End-User's profile page. The contents of this Web page SHOULD be about the End-User.
picture	string	URL of the End-User's profile picture. This URL MUST refer to an image file (for example, a PNG, JPEG, or GIF image file), rather than to a Web page containing an image. Note that this URL SHOULD specifically reference a profile photo of the End-User suitable for displaying when describing the End-User, rather than an arbitrary photo taken by the End-User.
website	string	URL of the End-User's Web page or blog. This Web page SHOULD contain information published by the End-User or an organization that the End-User is affiliated with.
email	string	End-User's preferred e-mail address. Its value MUST conform to the RFC 5322 [RFC5322] addr-spec syntax. The RP MUST NOT rely upon this value being unique, as discussed in Section 5.7 .
email_verified	boolean	True if the End-User's e-mail address has been verified; otherwise false. When this Claim Value is true, this means that the OP took affirmative steps to ensure that this e-mail address was controlled by the End-User at the time the verification was performed. The means by which an e-mail address is verified is context-specific, and dependent upon the trust framework or contractual agreements within which the parties are operating.
gender	string	End-User's gender. Values defined by this specification are female and male. Other values MAY be used when neither of the defined values are applicable.
birthdate	string	End-User's birthday, represented as an ISO 8601:2004 [ISO8601-2004] YYYY-MM-DD format. The year MAY be 0000, indicating that it is omitted. To represent only the year, YYYY format is allowed. Note that depending on the underlying platform's date related function, providing just year can result in varying month and day, so the implementers need to take this factor into account to correctly process the dates.
zoneinfo	string	String from zoneinfo [zoneinfo] time zone database representing the End-User's time zone. For example, Europe/Paris or America/Los_Angeles.
language	string	End-User's locale, represented as a BCP47 [RFC5646] language tag. This is typically an ISO 639-1 Alpha-2 [ISO639-1] language code in lowercase and an ISO 3166-1 Alpha-2 [ISO3166-1] country code in uppercase, separated by a dash. For example, en-US or fr-FR. As a compatibility note, some implementations have used an

Example of OpenID Connect flow for Webex Entra Social Login

(AuthN & Provision)

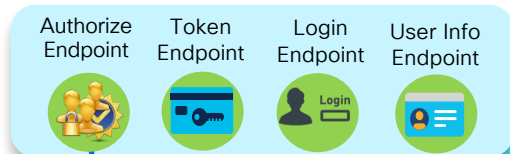
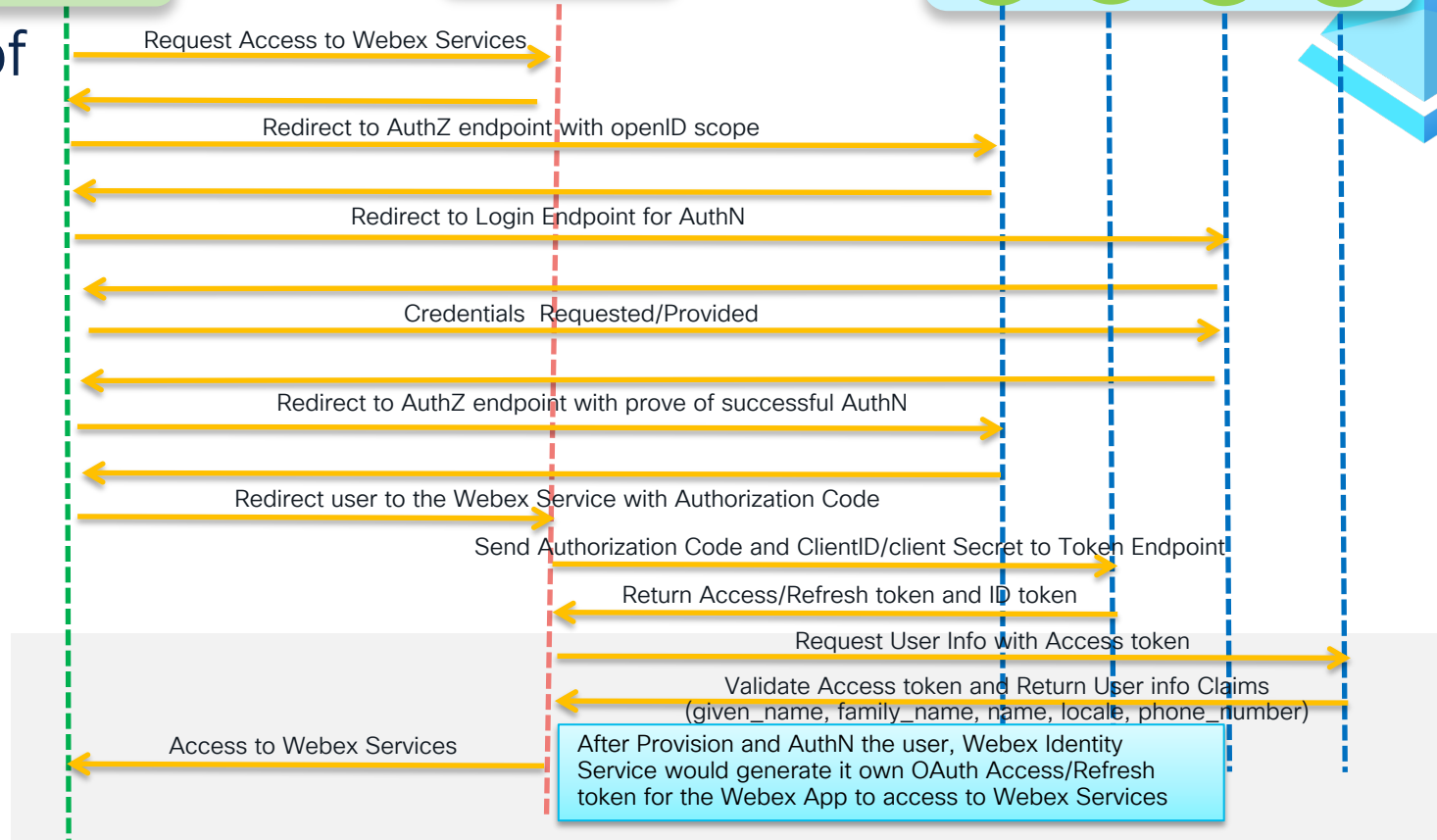
User/Webex App



Webex Service



Entra OIDC Services



OpenID Connect Discovery

As we saw before in OpenID Connect there are multiple endpoints that need to be target to get different results (Token, UserInfo, Authorization, etc.)

So the configuration can be request according to Discovery extensions

https://openid.net/specs/openid-connect-discovery-1_0.html, in the end we just need to know the hostname for the service.

OpenID Provider Configuration Request

```
GET /.well-known/openid-configuration HTTP/1.1
Host: example.com
```

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "issuer":
    "https://server.example.com",
  "authorization_endpoint":
    "https://server.example.com/connect/authorize",
  "token_endpoint":
    "https://server.example.com/connect/token",
  "token_endpoint_auth_methods_supported":
    ["client_secret_basic", "private_key_jwt"],
  "token_endpoint_auth_signing_alg_values_supported":
    ["RS256", "ES256"],
  "userinfo_endpoint":
    "https://server.example.com/connect/userinfo",
  "check_session_iframe":
    "https://server.example.com/connect/check_session",
  "end_session_endpoint":
    "https://server.example.com/connect/end_session",
  "jwks_uri":
    "https://server.example.com/jwks.json",
  "registration_endpoint":
    "https://server.example.com/connect/register",
  "scopes_supported":
    ["openid", "profile", "email", "address",
     "phone", "offline_access"],
  "response_types_supported":
    ["code", "code id_token", "id_token", "token id_token"],
  "acr_values_supported":
    [{"urn:mace:incommon:iap:silver",
     "urn:mace:incommon:iap:bronze"}],
  "subject_types_supported":
    ["public", "pairwise"],
  "userinfo_signing_alg_values_supported":
    ["RS256", "ES256", "HS256"],
  "userinfo_encryption_alg_values_supported":
    ["RSA1_5", "A128KW"],
  "userinfo_encryption_enc_values_supported":
    ["A128CBC-HS256", "A128GCM"],
  "id_token_signing_alg_values_supported":
    ["RS256", "ES256", "HS256"],
  "id_token_encryption_alg_values_supported":
    ["RSA1_5", "A128KW"],
  "id_token_encryption_enc_values_supported":
    ["A128CBC-HS256", "A128GCM"],
  "request_object_signing_alg_values_supported":
    ["none", "RS256", "ES256"],
  "display_values_supported":
    ["page", "popup"],
  "claim_types_supported":
    ["normal", "distributed"],
  "claims_supported":
    ["sub", "iss", "auth_time", "acr",
     "name", "given_name", "family_name", "nickname",
     "profile", "picture", "website",
     "email", "email_verified", "locale", "zoneinfo",
     "http://example.info/claims/groups"],
  "claims_parameter_supported":
    true,
  "service_documentation":
    "http://server.example.com/connect/service_documentation.html",
  "ui_locales_supported":
    ["en-US", "en-GB", "en-CA", "fr-FR", "fr-CA"]
}
```

Webex AuthN/AuthZ improvements

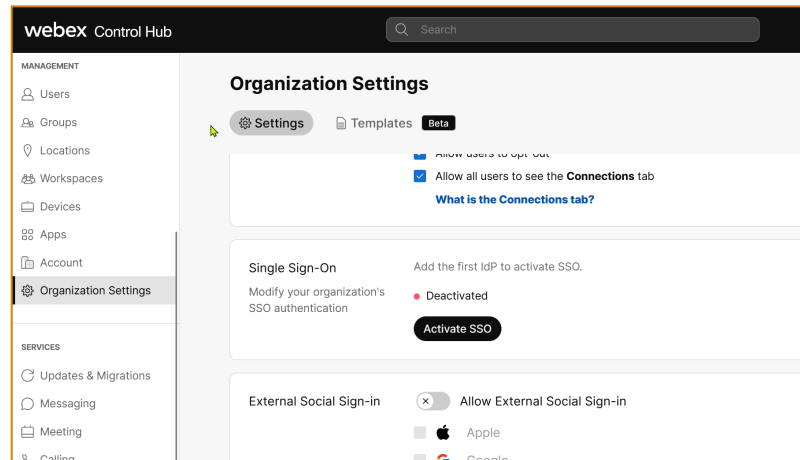
Authentication

Single Sign-On

Webex normally only allows 1 IdP, but with the [Webex Extended Security Pack](#) multiple IdPs will be possible,

Single Sign-On will be enable when [first/single](#) IdP will be configured.

Very Important : Having multiple IdP's for a single SSO enable Application (Webex), is not a common practice in the market. It can bring [security vulnerabilities](#), the Collaboration Administrator can re-define the Corporate Authentication policies and impersonate any user in the organization.

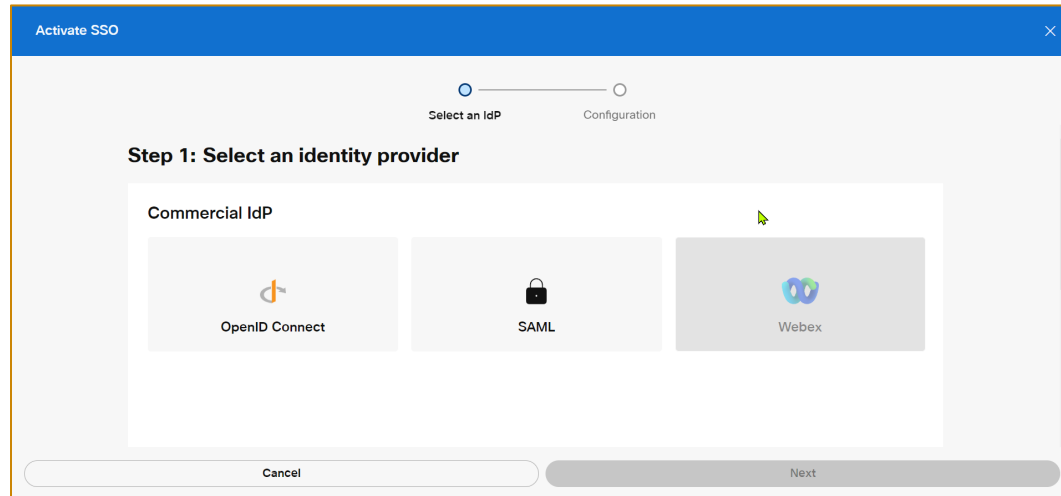


Single Sign-On

New Wizard

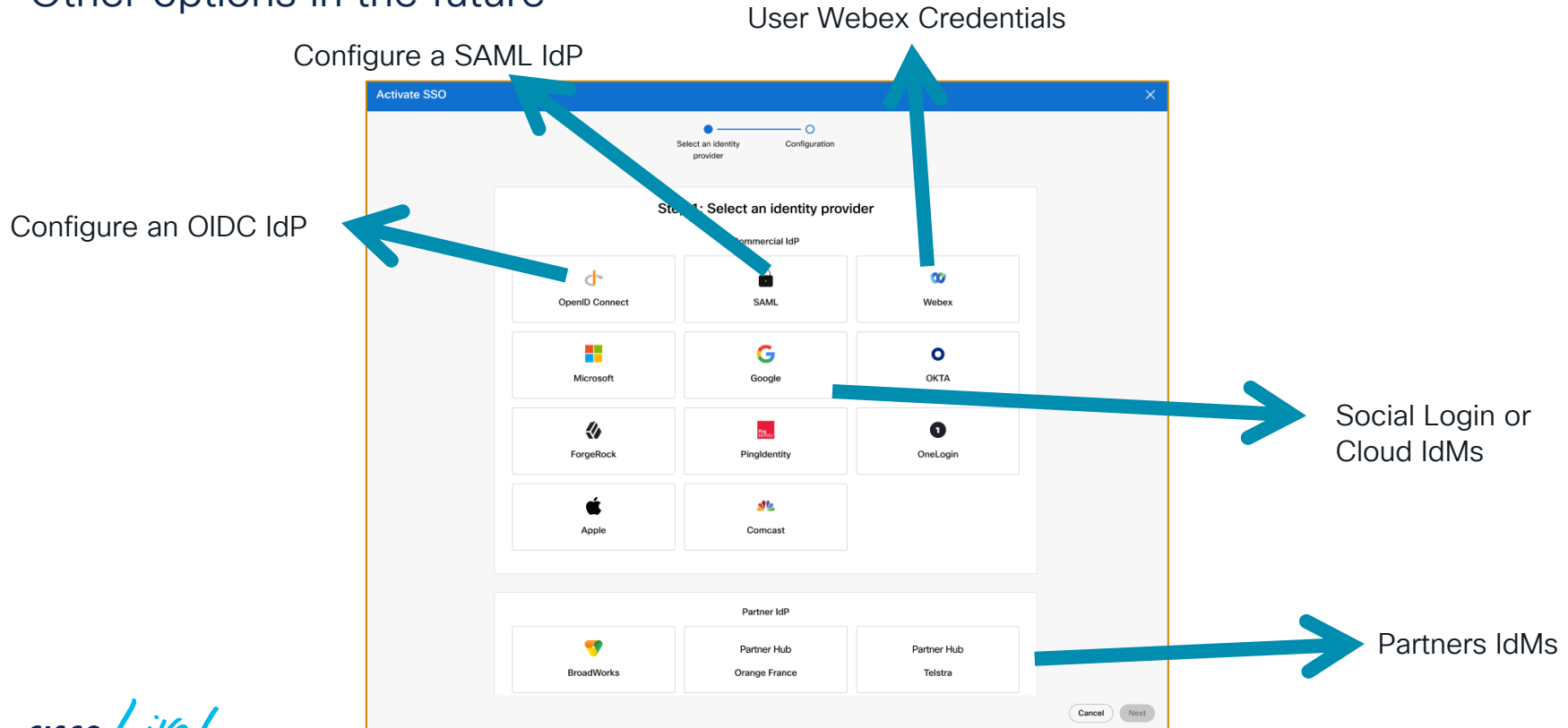
Today we will allow OIDC and SAML IdPs.

The option for Webex is only available in the multiple IdPs scenarios, after the first IdP.



Single Sign-On

Other options in the future



Options for each protocol

New Wizard will have the options of automatic configuration by using metadata or Discovery URL.

Will also allow for manual configuration.

SAML

OIDC

Single Sign-On

SAML IdPs

Step 2 – Export metadata to configure the IDP

Step 3 – Configure Webex with IdP metadata file or manually by providing the SAML details (entityID, Single Sign-On URL, Binding,)

The screenshot shows the 'Activate SSO' wizard at Step 2: 'Select and export a certificate'. The progress bar at the top indicates the current step. The main content area has a heading 'Select a certificate' and two options:

- Self-signed by Cisco (recommended)**: Valid for 4 years. Less secure but you'll only update Cisco metadata every 4-5 years. Your identity provider (IdP) vendor must support self-signed certificates in metadata.
- Signed by a public certificate authority**: Valid for 1 years. More secure, but you'll need to frequently update metadata (unless your IdP vendor supports trust anchors).

Below these options is a 'Download the certificate's metadata' section with instructions: 'Download the metadata from the directory certificate. You'll upload this to your identity provider for SAML authentication.' and a 'Download metadata' button.

At the bottom right are 'Previous' and 'Next' buttons.

The screenshot shows the 'Activate SSO' wizard at Step 3: 'Configure IdP metadata'. The progress bar at the top indicates the current step. The main content area has a heading 'Step 3: Configure IdP metadata' and a sub-heading 'Select how to connect your identity provider (IdP) to the Webex cloud:'. There are two options:

- Upload your IdP's metadata**: Represented by a document icon.
- Fill in the configuration form**: Represented by a document icon with a plus sign.

Below these options is the 'Add IdP information' section with the following fields and options:

- Entity ID (SAML Identifier) ***: Enter an ID.
- Single sign-on URL ***: Enter a URL.
- Binding**: Radio buttons for HTTP-Post (selected) and HTTP-Redirect.
- Single sign-out URL (recommended)**: Enter a URL.
- Binding**: Radio buttons for HTTP-Post (selected) and HTTP-Redirect.
- Features**: A checkbox for 'Sign SAML request' is unchecked.
- NameIDFormat**: Three radio buttons: 'urn:oasis:names:tc:SAML:2.0:nameid-format:transient' (selected), 'urn:oasis:names:tc:SAML:2.0:nameid-format:persistent', and 'urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified'.
- IdP certificate files (supported file types: *.pem, *.cer) up to 2 (if your idp supports multiple certificates)**: A 'Select file' button.

At the bottom right are 'Previous' and 'Next' buttons.

Single Sign-On

SAML IdPs

Step 4 – SAML mappings and JIT

The screenshot shows the 'Activate SSO' wizard at Step 4. The progress bar at the top indicates the following steps: Select an IdP, Select certificate, Configure metadata, **JIT & SAML configuration**, Test SSO setup, and Activate SSO. The main content area is titled 'Step 4: Just-in-Time (JIT) & SAML mapping configuration'.

Just-in-Time (JIT) settings

To create and activate JIT user accounts, configure Domain Claim to add your organisation's users.

- ☐ Create or activate user: if no active user is found
- ☐ Update user with attributes: if a user with email address is found

SAML mapping required attributes

SAML attribute name	Webex identity attribute name	Attribute description
<input type="text" value="uid"/>	Username / Primary email address *	Map the UID attribute to the provisioned user's email, UPN or edupersonprincipalname.

Linking attribute

SAML attribute name	Webex identity attribute name	Attribute description
<input type="text" value="Sync/map the name after selection"/>	<input type="text" value="Select an attribute"/>	This should be an attribute that is unique to the user. It will be used to look up a user so that Webex can update all profile attributes including email for a user.

[Show optional attributes](#)

At the bottom, there are 'Previous' and 'Next' buttons.

Step 5 – Test Configuration

Step 6 – Enable or Disable SSO

The top screenshot shows Step 5: 'Test your SSO setup'. The progress bar highlights 'Test SSO setup'. The main content area contains instructions to check the SSO configuration and a 'Test SSO setup' button. Below the instructions, there is a 'Copy the URL to the clipboard' button.

The bottom screenshot shows Step 6: 'Activate SSO with a successful test'. The progress bar highlights 'Activate SSO'. The main content area contains instructions to turn on SSO and a 'Turn on SSO' button. Below the instructions, there are radio buttons for 'Successful test. Activate SSO and IdP' and 'Unsuccessful test. Go back to previous steps to fix errors'.

Single Sign-On

OIDC IdPs

Step 2 – Agreement Name, Client ID, Client Secret and Discovery URL or Manual Endpoint configuration

Activate SSO

Progress: Select an IdP, **Configure metadata**, Test SSO setup, Activate SSO

Step 2: Configure OpenID Connect metadata

Add identity provider information

Name *

Enter the IdP name

Client ID *

Enter the client ID

Configure the client's redirect URL: <https://idbroker.webex.com/IdP/Consumer/redirect?as...> [Learn more](#)

Client Secret *

Enter the client secret

Scopes *

☐ email ☐ openid ☒ address ☒ phone ☒ profile

Endpoints

Select how to enter all endpoints:

☒ Use the discovery URL

☐ Manually add endpoint information

Discovery URL *

Enter the URL

Just in Time (JIT) settings

☐ Update user with attributes: if a user with email address is found

Previous Next

Activate SSO

Progress: Select an IdP, **Configure metadata**, Test SSO setup, Activate SSO

Step 2: Configure OpenID Connect metadata

Add identity provider information

Name *

Enter the IdP name

Client ID *

Enter the client ID

Configure the client's redirect URL: <https://idbroker.webex.com/IdP/Consumer/redirect?as...> [Learn more](#)

Client Secret *

Enter the client secret

Scopes *

☒ email ☐ openid ☒ address ☒ phone ☒ profile

Endpoints

Select how to enter all endpoints:

☐ Use the discovery URL

☒ Manually add endpoint information

Issuer *

Enter an issuer

Authorization endpoint *

Enter your authorisation endpoint

Token endpoint *

Enter token endpoint

JWKS endpoint *

Enter your JWKS endpoint

User info endpoint *

Enter user info endpoint

Just in Time (JIT) settings

☐ Update user with attributes: if a user with email address is found

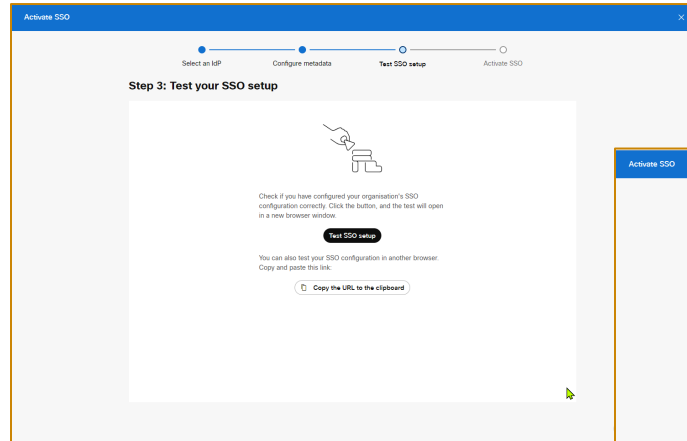
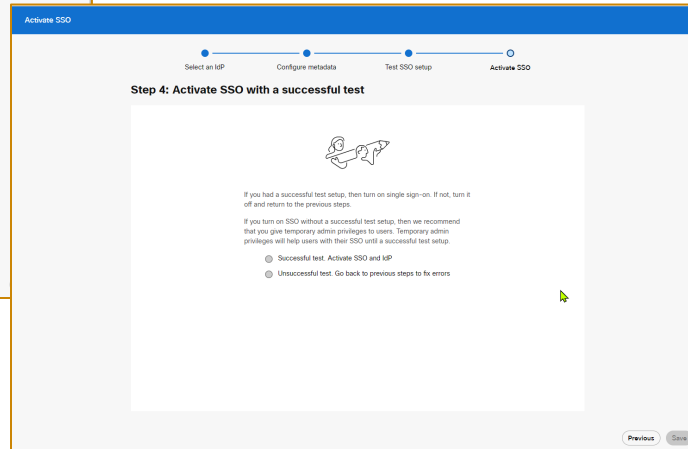
Previous Next

Single Sign-On

OIDC IdPs

Step 3 – Test SSO

Step 4 – Activate or deactivate SSO



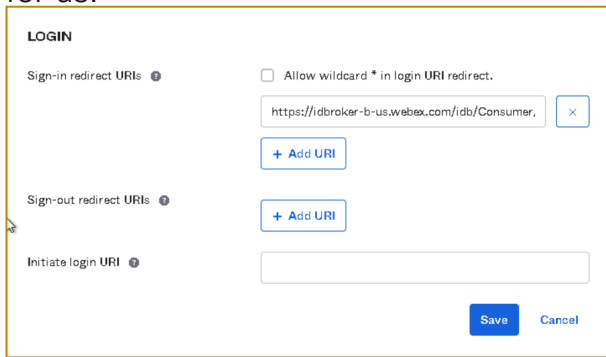
Cloud OIDC IdP

Where do we get that information on Okta ?

When configuring the OIDC application in Okta, we need to provide the Sign-In URL in Webex

<https://idbroker-b-us.webex.com/idb/Consumer/oidc/sp>

And then it allow us to create a Client Secret for the dynamic Client ID created for us.



LOGIN

Sign-in redirect URIs ⓘ ☐ Allow wildcard * in login URI redirect.

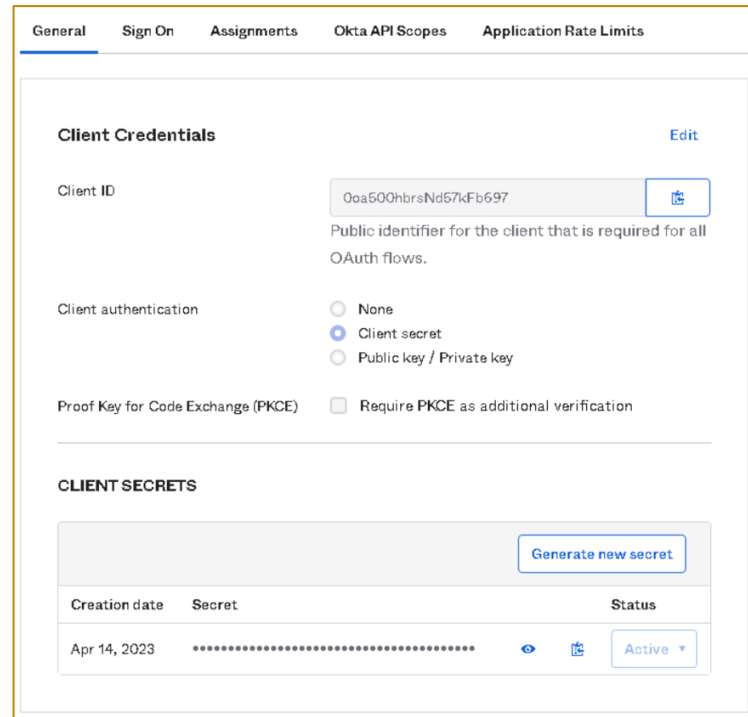
<https://idbroker-b-us.webex.com/idb/Consumer,> ✕

[+ Add URI](#)

Sign-out redirect URIs ⓘ [+ Add URI](#)

Initiate login URI ⓘ

[Save](#) [Cancel](#)



General **Sign On** **Assignments** **Okta API Scopes** **Application Rate Limits**

Client Credentials [Edit](#)

Client ID [✕](#)

Public identifier for the client that is required for all OAuth flows.

Client authentication ☐ None ☒ Client secret ☐ Public key / Private key

Proof Key for Code Exchange (PKCE) ☐ Require PKCE as additional verification

CLIENT SECRETS

[Generate new secret](#)

Creation date	Secret	Status
Apr 14, 2023	 👁 🔗	Active ▼

Discover URL is the Okta tenant name, as we saw before, we add .well-known/openid-configuration.

Something like <https://trial-1234044-admin.okta.com/.well-known/openid-configuration>

On-Premise OIDC IdP

Where do we get that information on PingFederate ?

When configuring the OIDC application in Okta, we need to provide the Sign-In URL in Webex

<https://idbroker-b-us.webex.com/idb/Consumer/oidc/sp>

Allow us to create a Client ID and Secret.

The screenshot shows the PingFederate console with the 'Clients' tab selected. The 'REDIRECT URIS' section is active, showing a list of URIs with an 'Add' button. The 'ALLOW AUTHENTICATION API REDIRECTLESS MODE' is checked. The 'RESTRICT COMMON SCOPES' section is expanded, showing 'email' and 'openid' scopes. The 'EXCLUSIVE SCOPES' section is also expanded, showing 'Allow Exclusive Scopes' and 'Authorization Code' options. The 'ALLOWED GRANT TYPES' section is expanded, showing 'Implicit', 'Refresh Token', 'Client Credentials', 'Device Authorization Grant', 'CIBA', 'Token Exchange', 'Resource Owner Password Credentials', 'Assertion Grants', and 'Access Token Validation (Client is a Resource Server)'. The 'RESTRICT RESPONSE TYPES' section is expanded, showing 'Restrict'.

The screenshot shows the PingFederate console with the 'Clients' tab selected. The 'Clients | Client' section is active, showing the configuration for a new client. The 'CLIENT ID' is 'Webex'. The 'NAME' is 'Webex'. The 'DESCRIPTION' is 'OIDC Client for Webex'. The 'CLIENT AUTHENTICATION' section is expanded, showing 'NONE', 'CLIENT SECRET' (selected), 'CLIENT TLS CERTIFICATE', and 'PRIVATE KEY JWT'. The 'CLIENT SECRET' is '.....'. The 'CHANGE SECRET' button is visible.

Discover URL is the PingFederate FQDN, as we saw before,
we add .well-known/openid-configuration.

Something like <https://ping8a.identitylab9.ciscolabs.com/.well-known/openid-configuration>

Single Sign-On

How to configure each detail on OIDC and/or SAML

We will have the same controls as we had before with SAML SSO configuration, but now we can manage multiple IDPs and also local authentication

OIDC

SAML

Local

Organization Settings

Single sign-on & multiple identity providers

Identity provider **Relaying rules**

Search IdP 3 IdP [Activate SSO](#) [Add identity provider](#)

Name	Type	Provisioning mode	Expiration date
▼ PingIdentityOIDC	OpenID Connect	JIT creation & ...	N/A
Client ID	Webex		
Scopes	openid email profile		
Discovery URL	https://ping0a.identitylab9.cisco.com:9031/.well-known/openid-configuration		
Redirect URI	https://idbroker-eu.webex.com/idb/Consumer/oidc/sp		
▼ http://ads0a.identitylab1.cisco.com/ads/services/trust	SAML	N/A	10/07/2023, 12:09:10 PM
Entity ID (SAML identifier)	http://ads0a.identitylab1.cisco.com/ads/services/trust		
Service Provider (SP)	Review certificates and expiration date		
SP Certificate usage	Logout request		
Webex			

[Edit IdP](#) [Test IdP](#) [Delete](#)

[Download IdP metadata](#) [Upload IdP metadata](#) [Download SP metadata](#) [Test IdP](#) [Edit SAML mapping](#) [Delete](#)

Review and edit Service Provider (SP) certificates

Service Provider (SP) certificates

Service Provider (SP) certificate is shared across all SAML IdP. Once a SP is renewed, all related SAML SP's metadata will need to be updated to make sure all IdPs are still working as expected.

Status	Expiration date	Serial number
Primary	09/13/2026, 03:40:55 AM	1173874692439297210885754160434 25224810773970695

[Cancel](#) [Renew certificate](#)

Multiple IdP Single Sign-On

How to associate each user to a different IdP

The association of Users to a specific IDP is defined in the [Routing Rules](#).

We can create the association based on [Groups](#) or [Domains](#)

If routing is based on DNS Domains, then the [domain needs to be verified](#)

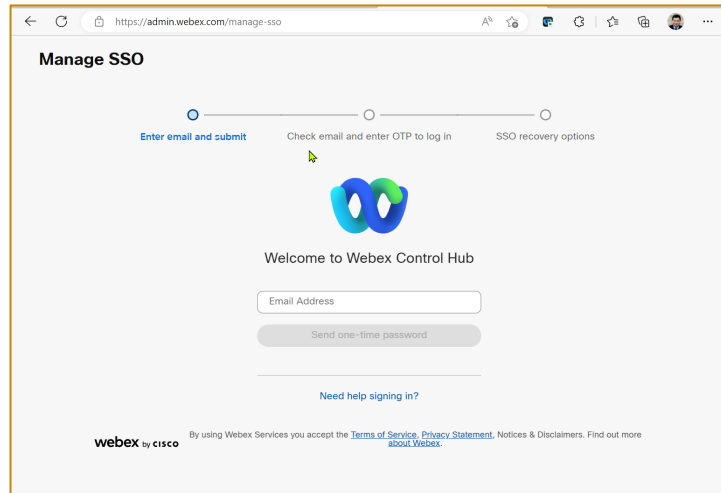
There is an [order of search](#) in the routing to the right IdP, so when a user goes through the rules, the first that match is picked.

The screenshot shows the 'Organization Settings' page for 'Single sign-on & multiple identity providers'. The 'Routing rules' tab is selected. On the left, a list of rules is shown with an 'Add new routing rule' button. The rules are: 1. OIDC_user_Group (Active), 2. SAML_user_Group (Active), 3. Identity9Domain (Active and selected), 4. Identitylab1Domain (Active), and 5. DefaultRule (Active). On the right, the configuration for the selected 'Identity9Domain' rule is shown. It includes a 'Select a routing type' dropdown set to 'domain'. Below this, there is a section 'If these are your domains' with a text input field containing 'identitylab9.cisco.com' and a 'Clear All' button. At the bottom, there is a 'Then use this identity provider' dropdown set to 'PingIdentityOIDC', and 'Deactivate' and 'Delete' buttons.

SSO recover process

How to fix SSO process if IDP break

- If SSO no longer works and User and Administrator can't login to Webex, Administrators can initiate recover process by navigating to <https://admin.webex.com/manage-ssu>.
- This will allow them to provide the Administrator ID to receive an OTP code



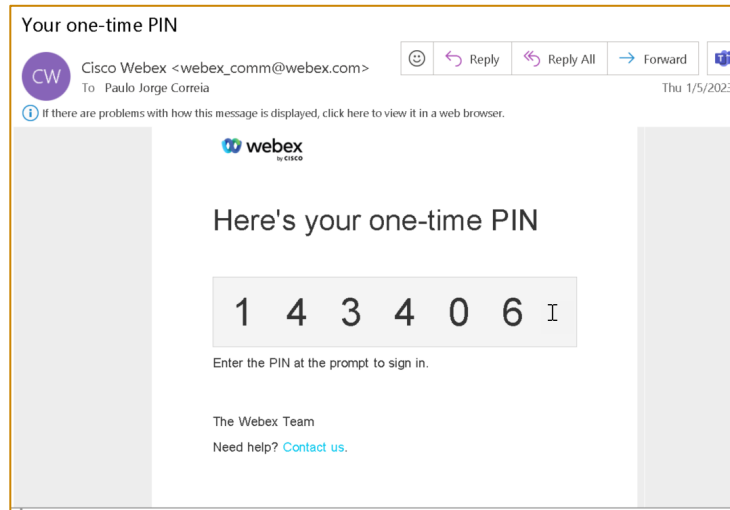
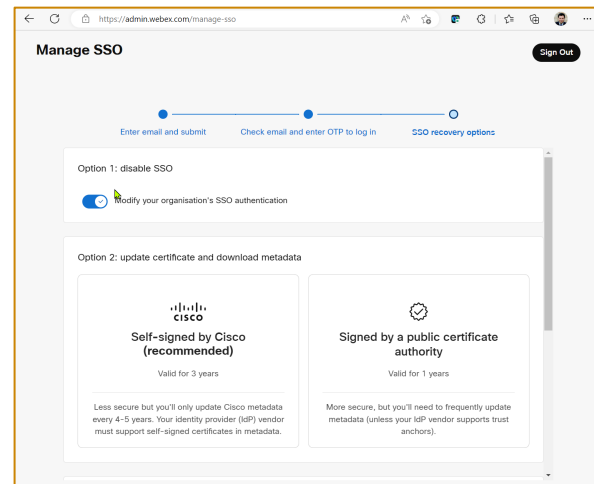
SSO recover process

How to fix SSO process if IDP break

After providing the OTP 6 digit code then have two options:

- Disable SSO
- Upload certificate and download metadata (rebuild SSO)

If they choose to rebuild, they have the option to test the new agreement.



Key Takeaways

- Cisco has a Webex **Provision solution for any stage** in the Identity journey of our Customers to the Cloud.
- Latest's protocol like OIDC make our customer **Authentication/Provision challenges easier to take.**
- Cisco has the best Identity architecture for Collaboration applications in the market, **deliver all possible combinations for any customer Identity Architecture.**



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLiveAPJC

Session

The background features a vibrant, multi-colored abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, green, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go

#CiscoLiveAPJC