cisco Live!

Let’s go

The bridge to possible

Authentication, Authorization and Provision for Cisco Collaboration

Paulo Jorge Correia, Principal Solutions Engineer
@paucorre

Agenda

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

Introduction

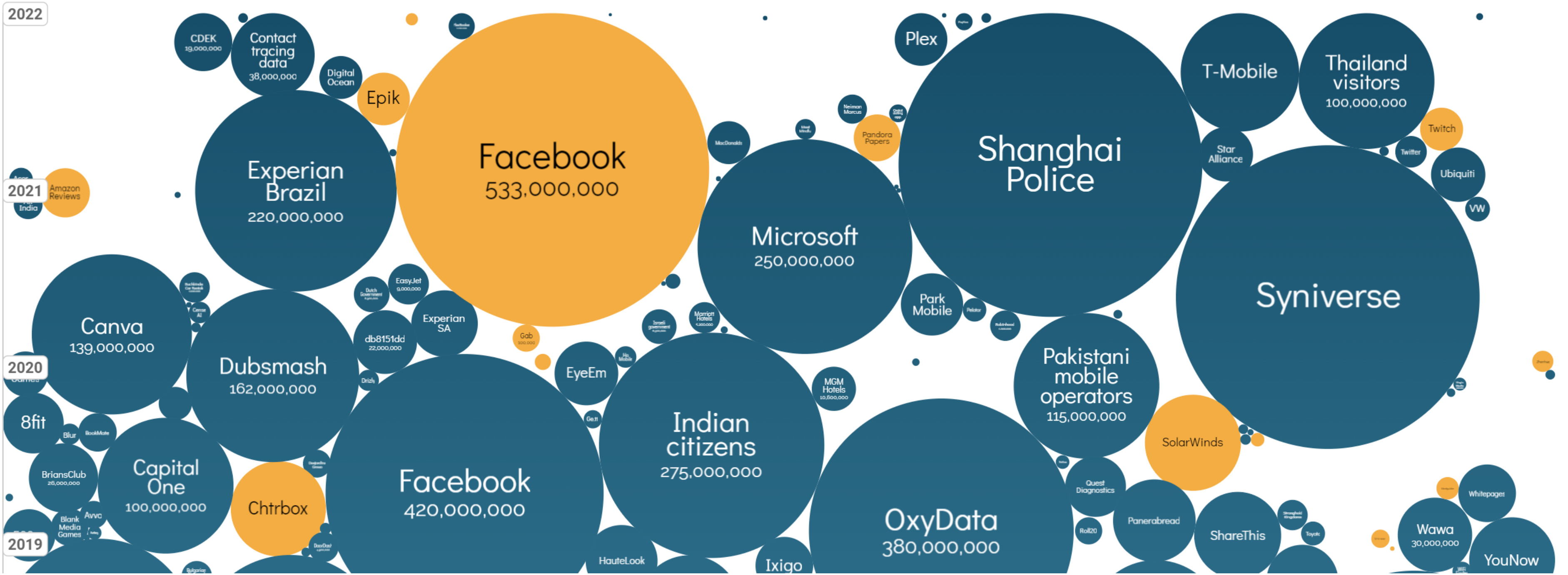
World's Biggest Data Breaches & Hacks

Selected events over 30,000 records

UPDATED: Sep 2022

interesting story

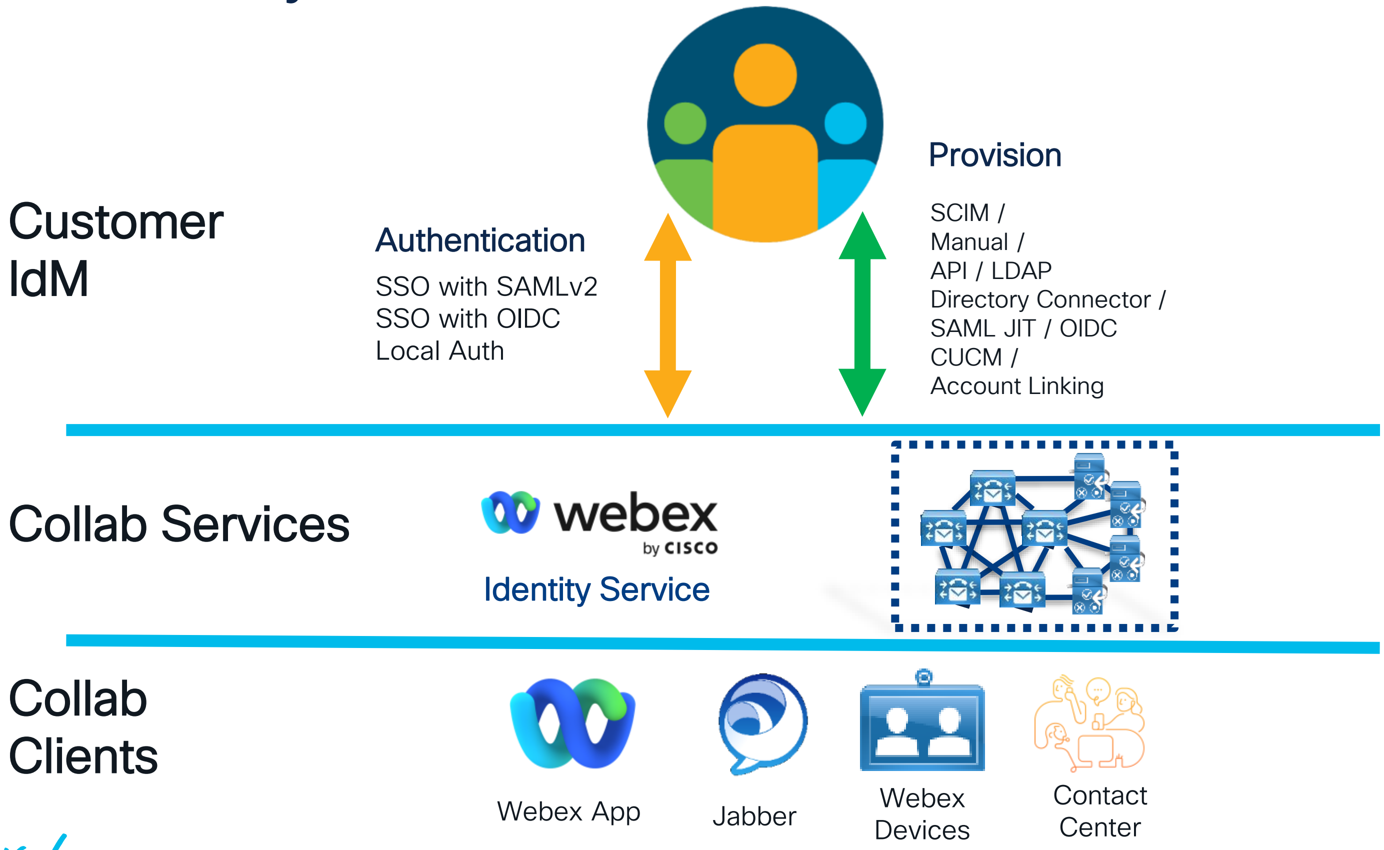
size: records lost | filter | search...



Source: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

cisco Live!

Cisco Identity Architecture for Collaboration



Customer IdM

Authentication

SSO with SAMLv2
SSO with OIDC
Local Auth

Provision

SCIM /
Manual /
API / LDAP
Directory Connector /
SAML JIT / OIDC
CUCM /
Account Linking

Collab Services

webex by cisco

Identity Service

Collab Clients

Webex App

Jabber

Webex Devices

Contact Center

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

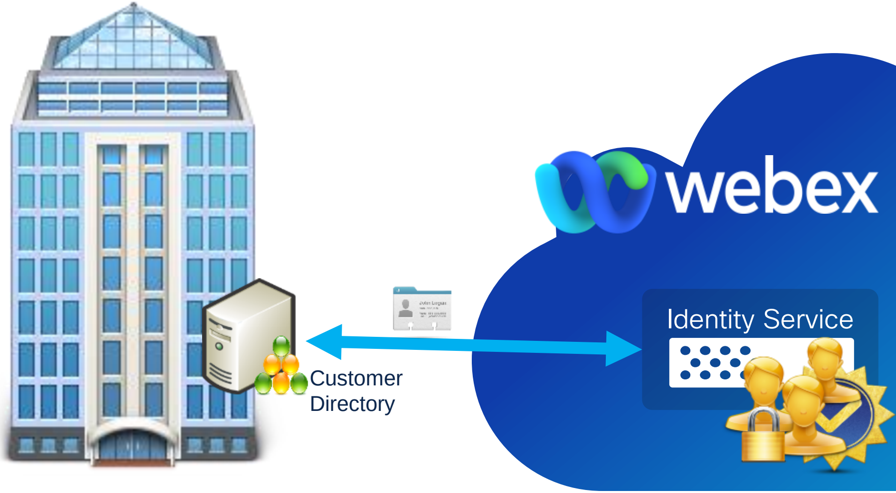
Webex User Account CRUD Operations

Manual or CSV	User Self-Enrollment or Invite	Directory Connector
SCIM Entra ID 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 ?

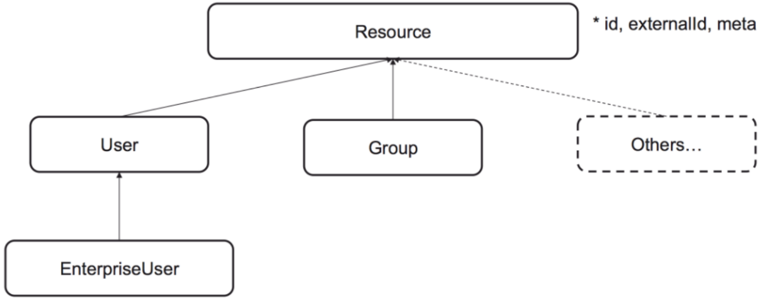
- Contacts Synchronization
- Uses Edge browser for authentication
- Remove synchronization of Distribution groups, only security groups going to be supported going forward.
- Allows the permanently delete users after soft delete
- Synchronizing Workspaces

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 :



Resource

* id, externalId, meta

User

Group

Others…

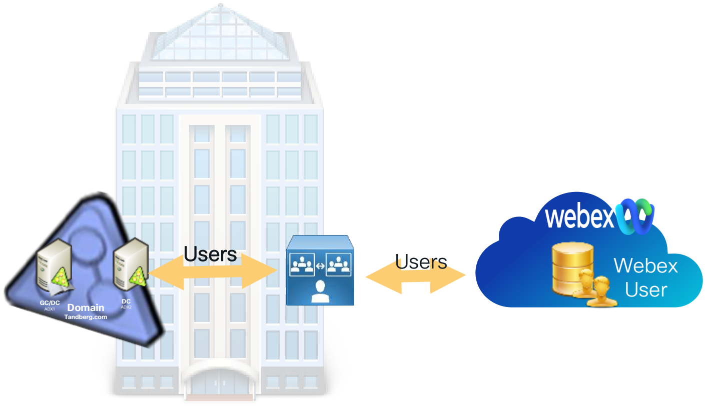
EnterpriseUser

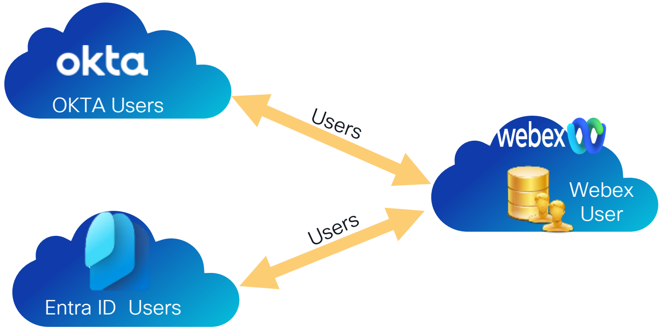
http://www.simplecloud.info/

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	✗	✓





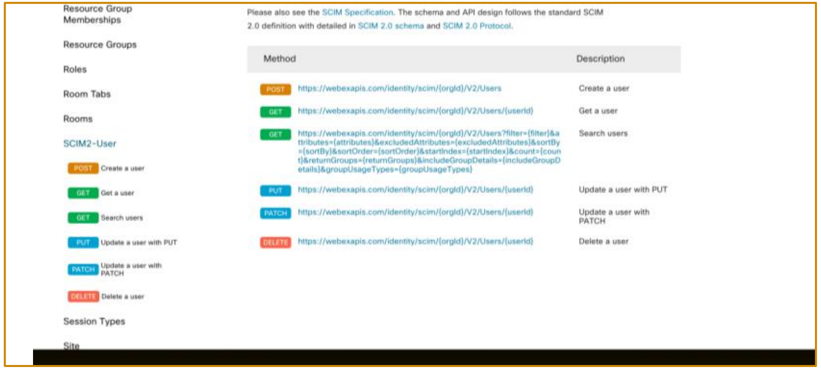
SCIM 2.0 Users & Groups

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



Resource Group Memberships

Resource Groups

Roles

Room Tabs

Rooms

SCIM2-User

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

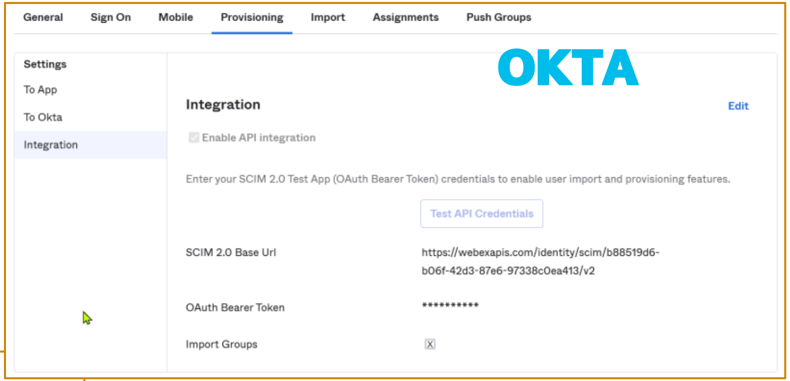
Please also see the SCIM Specification. The schema and API design follows the standard SCIM 2.0 definition with detailed in SCIM 2.0 schema and SCIM 2.0 Protocol.

Method	Description
POST https://webexapis.com/identity/scim/{orgId}/V2/Users	Create a user
GET https://webexapis.com/identity/scim/{orgId}/V2/Users/{userId}	Get a user
GET https://webexapis.com/identity/scim/{orgId}/V2/Users?filter={filter}&attributes={attributes}&excludedAttributes={excludedAttributes}&sortBy={sortBy}&sortOrder={sortOrder}&startIndex={startIndex}&count={count}&returnGroups={returnGroups}&includeGroupDetails={includeGroupDetails}&groupUsageTypes={groupUsageTypes}	Search users
PUT https://webexapis.com/identity/scim/{orgId}/V2/Users/{userId}	Update a user with PUT
PATCH https://webexapis.com/identity/scim/{orgId}/V2/Users/{userId}	Update a user with PATCH
DELETE https://webexapis.com/identity/scim/{orgId}/V2/Users/{userId}	Delete a user

Future

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



OKTA

Integration

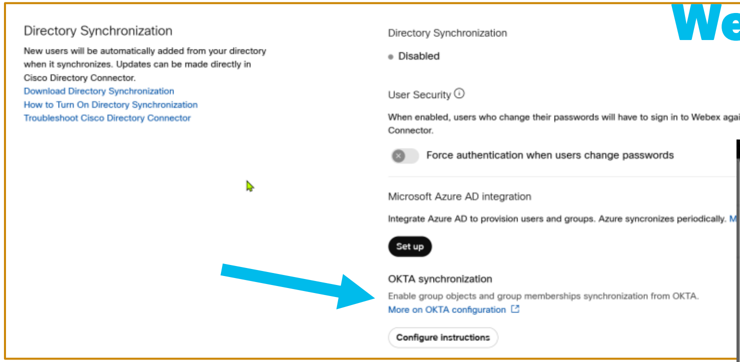
☑ Enable API integration

Enter your SCIM 2.0 Test App (OAuth Bearer Token) credentials to enable user import and provisioning features.

SCIM 2.0 Base Url https://webexapis.com/identity/scim/b88519d6-b06f-42d3-87e6-97338c0ea413/v2

OAuth Bearer Token **********

Import Groups ☒



Webex

Directory Synchronization

New users will be automatically added from your directory when it synchronizes. Updates can be made directly in Cisco Directory Connector.

Download Directory Synchronization

How to Turn On Directory Synchronization

Troubleshoot Cisco Directory Connector

Directory Synchronization

● Disabled

User Security

When enabled, users who change their passwords will have to sign in to Webex again after the new passwords are detected by Directory Connector.

Force authentication when users change passwords

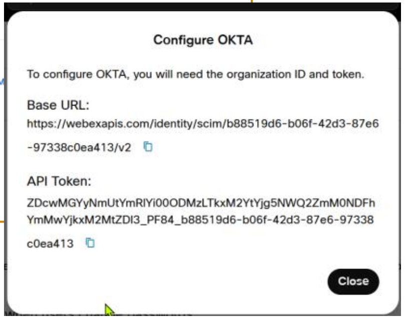
Microsoft Azure AD integration

Integrate Azure AD to provision users and groups. Azure syncronizes periodically. M

OKTA synchronization

Enable group objects and group memberships synchronization from OKTA.

More on OKTA configuration



Configure OKTA

To configure OKTA, you will need the organization ID and token.

Base URL:
https://webexapis.com/identity/scim/b88519d6-b06f-42d3-87e6-97338c0ea413/v2

API Token:
ZDcwMGYyNmUtYmRlYi00ODMzLTkxM2YtYjg5NWQ2ZmM0NDFhYmMwYjkxM2MtZDI3_PF84_b88519d6-b06f-42d3-87e6-97338c0ea413

Comparing SCIM & Directory Connector

	SCIM 1.1	SCIM 2.0	Directory Connector
Create, Delete and Update	✓	✓	✓
Allows local Webex Users Creation	✓	✓	✗
Attributes Synchronize	✓ (15)	✓ (27)	✓ (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	✗	✗	✓

Webex Provision

Groups Provision

Webex Groups CRUD Operations

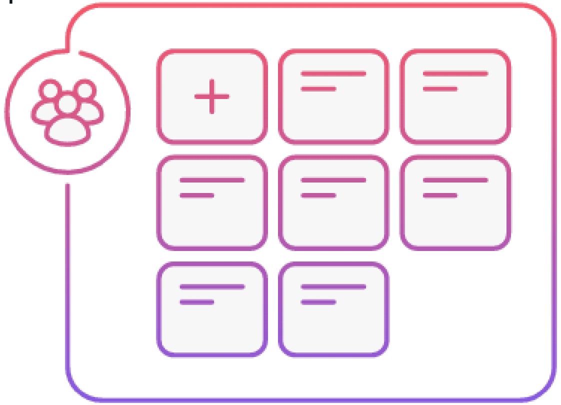
Manual or CSV	Directory Connector
Entra ID Wizard	Group API
SCIM 2.0	

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.

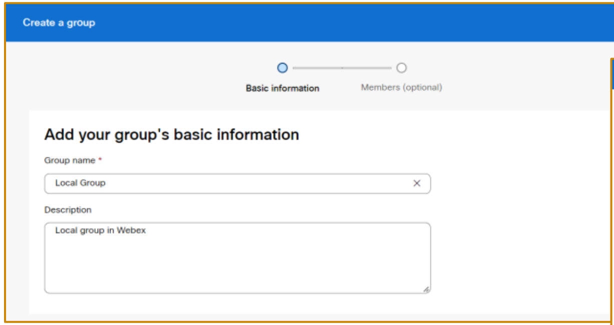
Who can manage groups?

- Full administrators and user administrators can manage groups.

Manage Groups

Using manual creation

- Groups locally created in Control Hub
- Can be created even if this Webex ORG is using Entra ID Wizard or Directory Connector.



Create a group

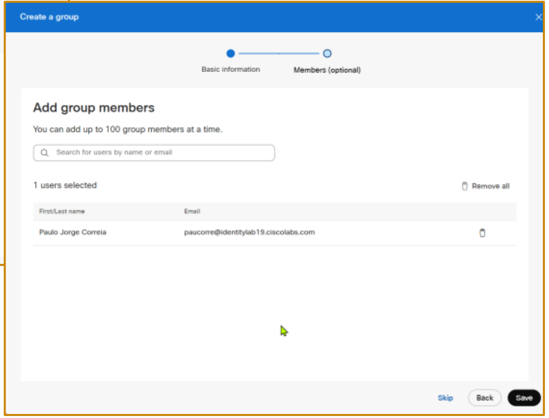
Add your group's basic information

Group name *

Local Group

Description

Local group in Webex



Create a group

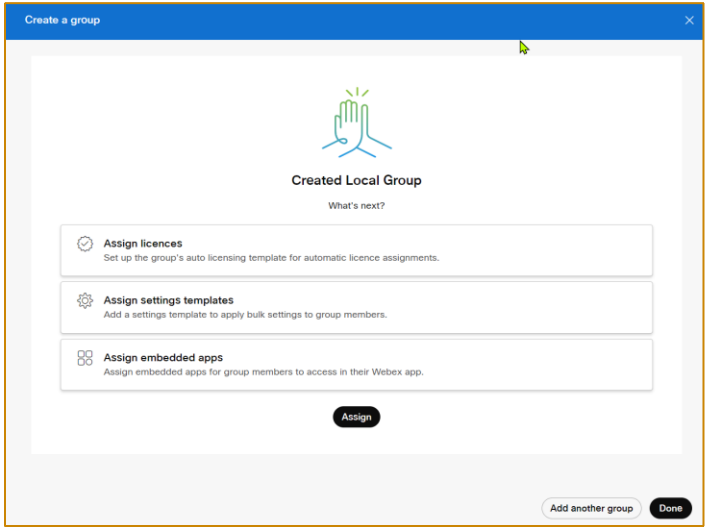
Add group members

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

Search for users by name or email

1 users selected Remove all

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



Create a group

Created Local Group

What's next?

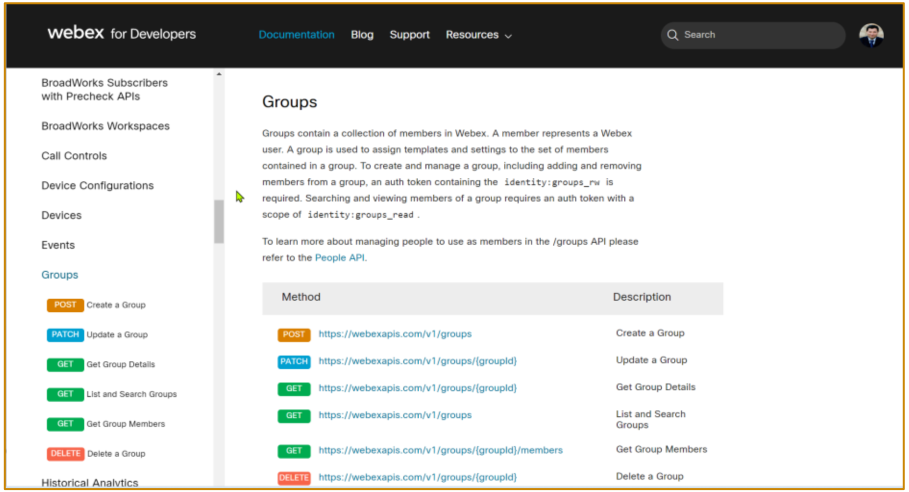
Assign licences
Set up the group's auto licensing template for automatic licence assignments.

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.

Manage Groups

Using APIs



Groups

Groups contain a collection of members in Webex. A member represents a Webex user. A group is used to assign templates and settings to the set of members contained in a group. To create and manage a group, including adding and removing members from a group, an auth token containing the `identity:groups_rw` is required. Searching and viewing members of a group requires an auth token with a scope of `identity:groups_read` .

To learn more about managing people to use as members in the /groups API please refer to the People API.

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.

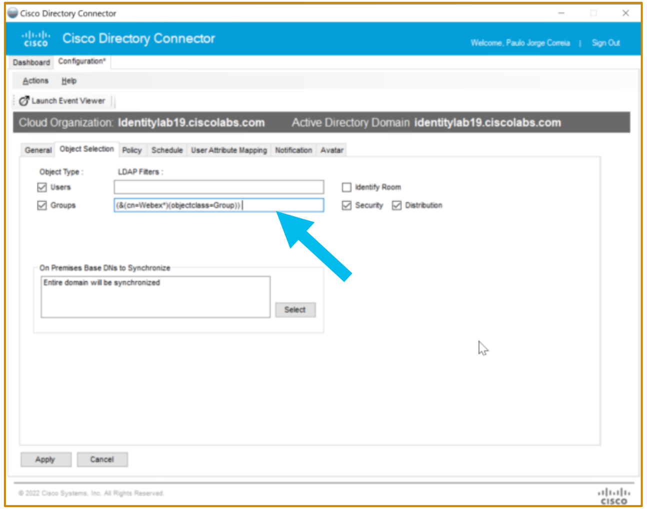
Key Capabilities

- 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 Directory Connector

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



Cloud Organization: **Identitylab19.ciscolabs.com** Active Directory Domain **identitylab19.ciscolabs.com**

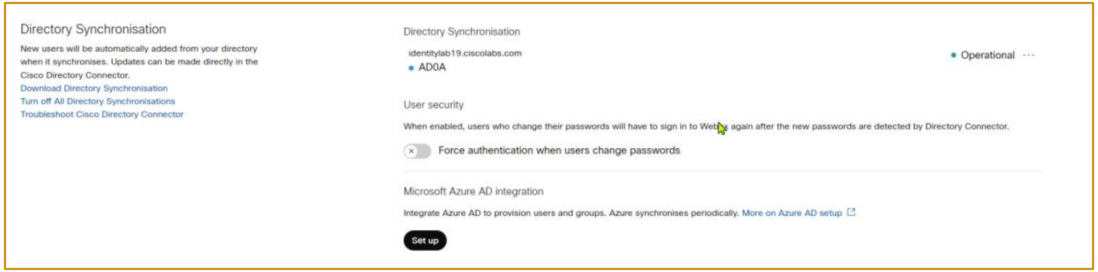
Object Type : LDAP Filters :

☑ Users ☐ Identify Room

☑ Groups (&(cn=Webex*)(objectclass=Group)) ☑ Security ☑ Distribution

On Premises Base DNs to Synchronize

Entire domain will be synchronized



Directory Synchronisation

New users will be automatically added from your directory when it synchronises. Updates can be made directly in the Cisco Directory Connector.

Download Directory Synchronisation

Turn off All Directory Synchronisations

Troubleshoot Cisco Directory Connector

Directory Synchronisation

identitylab19.ciscolabs.com

- AD0A

● Operational ···

User security

When enabled, users who change their passwords will have to sign in to Webex again after the new passwords are detected by Directory Connector.

☒ Force authentication when users change passwords

Microsoft Azure AD integration

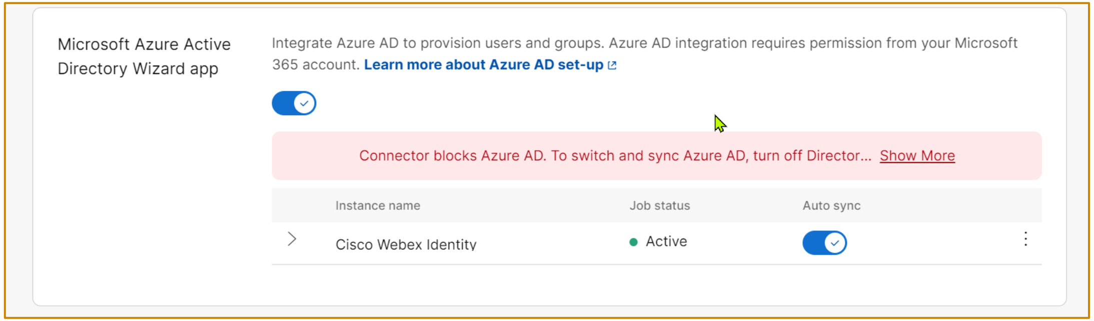
Integrate Azure AD to provision users and groups. Azure synchronises periodically. More on Azure AD setup

Manage Groups

Using Entra ID Wizard

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

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

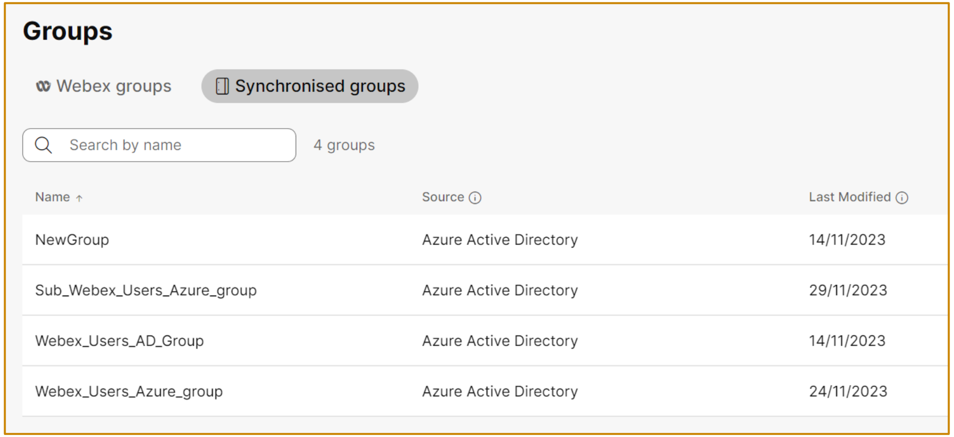


Microsoft Azure Active Directory Wizard app

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

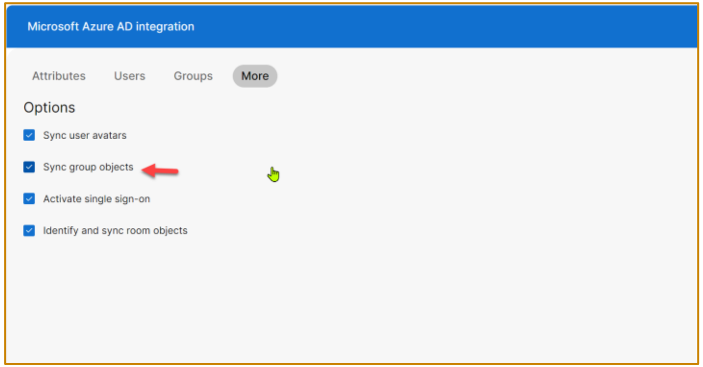
Instance name	Job status	Auto sync
Cisco Webex Identity	● Active	✓



Groups

Search by name — 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



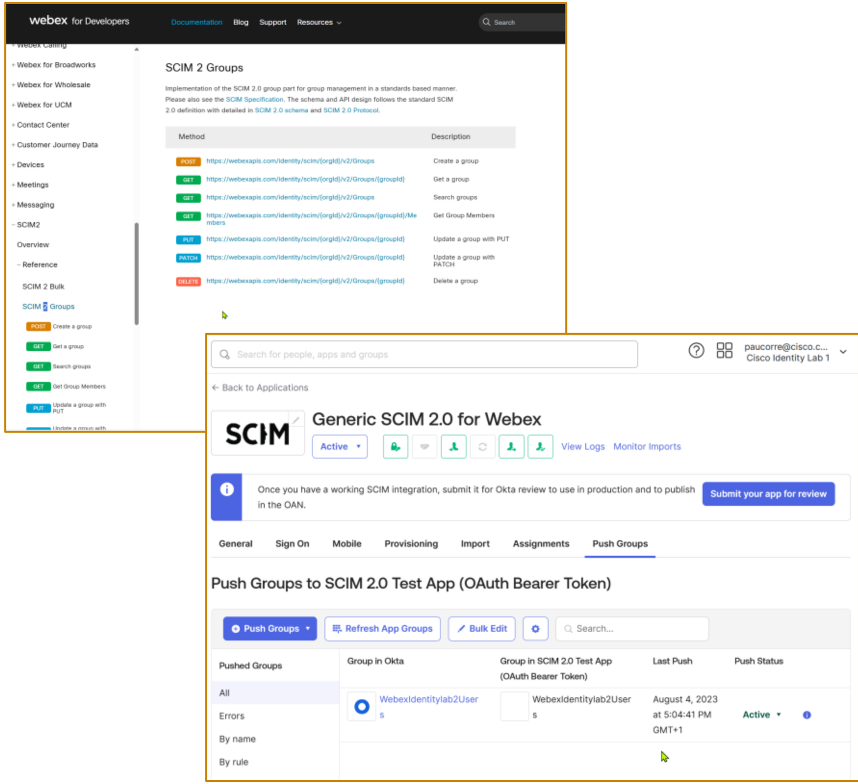
Microsoft Azure AD integration

Options

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

Groups synchronization using SCIM 2.0

- Allows for IDM’s to provide groups and its membership to Webex
- Allowing from the IDM to assign users to specific Licenses, Templates and Embedded Apps



SCIM 2 Groups

Implementation of the SCIM 2.0 group part for group management in a standards based manner. 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.

Method		Description
POST	https://webexapis.com/identity/scim/{orgId}/v2/Groups	Create a group
GET	https://webexapis.com/identity/scim/{orgId}/v2/Groups/{groupId}	Get a group
GET	https://webexapis.com/identity/scim/{orgId}/v2/Groups	Search groups
GET	https://webexapis.com/identity/scim/{orgId}/v2/Groups/{groupId}/Members	Get Group Members
PUT	https://webexapis.com/identity/scim/{orgId}/v2/Groups/{groupId}	Update a group with PUT
PATCH	https://webexapis.com/identity/scim/{orgId}/v2/Groups/{groupId}	Update a group with PATCH
DELETE	https://webexapis.com/identity/scim/{orgId}/v2/Groups/{groupId}	Delete a group

Generic SCIM 2.0 for Webex

Once you have a working SCIM integration, submit it for Okta review to use in production and to publish in the OAN.

Push Groups to SCIM 2.0 Test App (OAuth Bearer Token)

Group in Okta	Group in SCIM 2.0 Test App (OAuth Bearer Token)	Last Push	Push Status
WebexIdentitylab2Users	WebexIdentitylab2Users	August 4, 2023 at 5:04:41 PM GMT+1	Active

Webex Provision

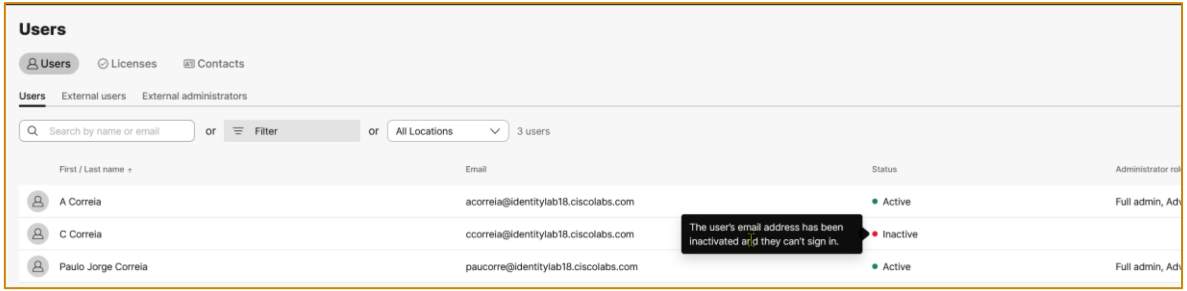
Other Provision Features

Delete inactive users

Inactive users by default are deleted after 30 days.

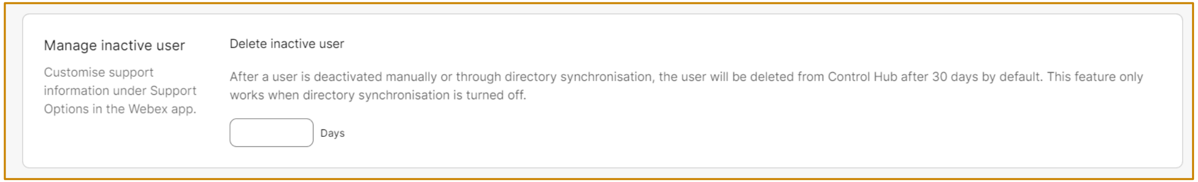
An inactive user can't login, and all his Access Tokens are not valid.

Default behavior can be changed



First / Last name	Email	Status	Administrator rol
A Correia	acorreia@identitylab18.ciscolabs.com	● Active	Full admin, Adv
C Correia	ccorreia@identitylab18.ciscolabs.com	● Inactive	
Paulo Jorge Correia	paucorre@identitylab18.ciscolabs.com	● Active	Full admin, Adv

The user's email address has been inactivated and they can't sign in.



Manage inactive user

Customise support information under Support Options in the Webex app.

Delete inactive user

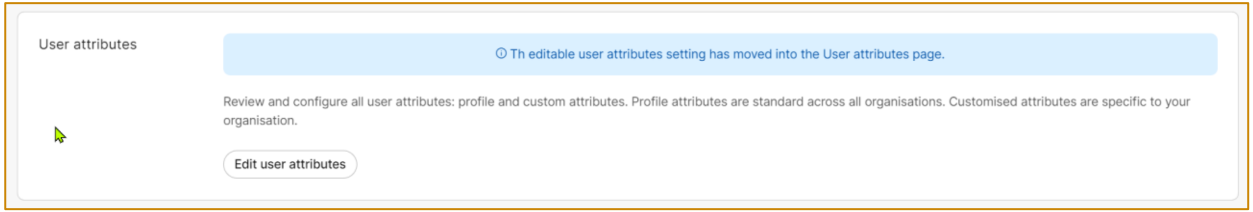
After a user is deactivated manually or through directory synchronisation, the user will be deleted from Control Hub after 30 days by default. This feature only works when directory synchronisation is turned off.

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.

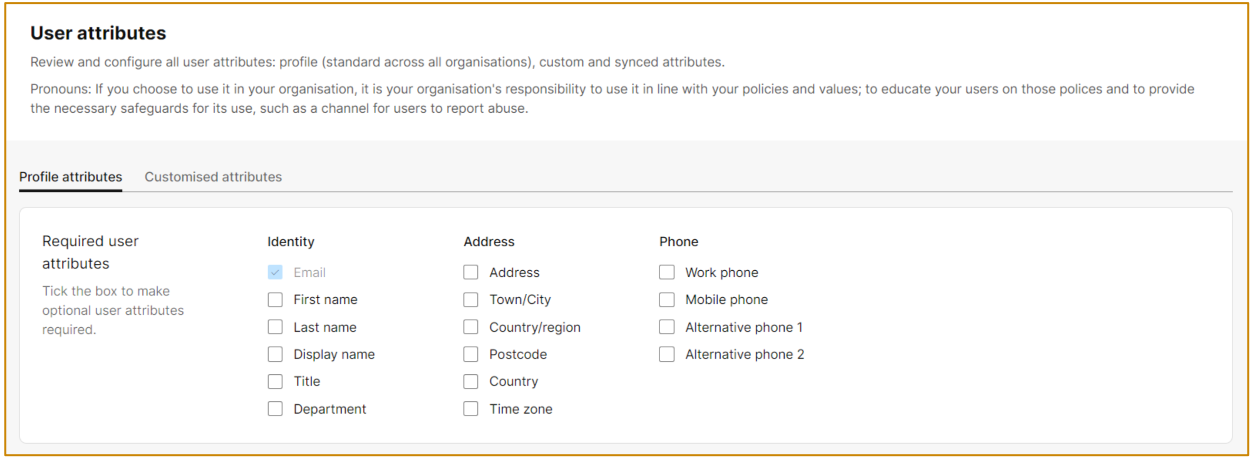


User attributes

ⓘ Th editable user attributes setting has moved into the User attributes page.

Review and configure all user attributes: profile and custom attributes. Profile attributes are standard across all organisations. Customised attributes are specific to your organisation.

Edit user attributes



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 polices 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

Tick the box to make optional user attributes required.

Identity
- ☑ Email
- □ First name
- □ Last name
- □ Display name
- □ Title
- □ Department

Address
- □ Address
- □ Town/City
- □ Country/region
- □ Postcode
- □ Country
- □ Time zone

Phone
- □ Work phone
- □ Mobile phone
- □ Alternative phone 1
- □ Alternative phone 2

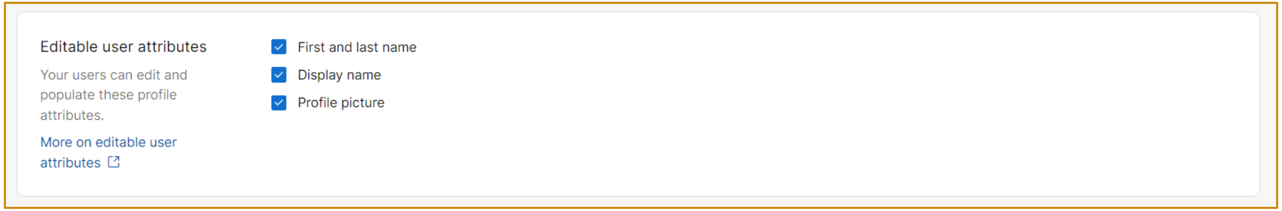
User Attributes

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

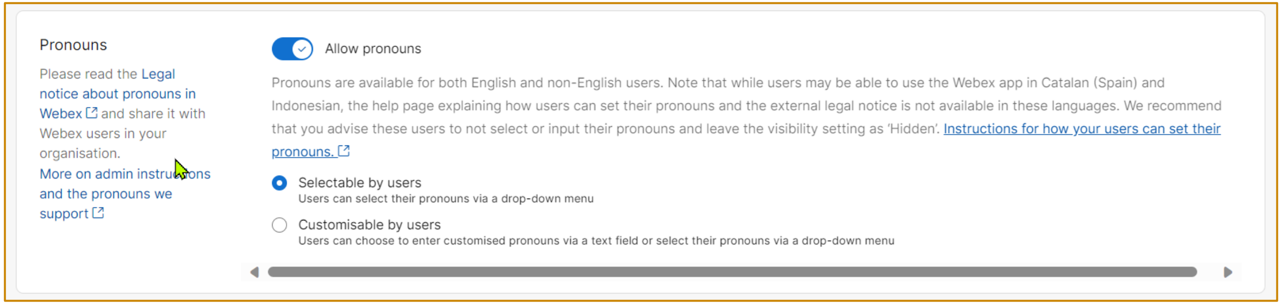
Your users can edit and populate these profile attributes.

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

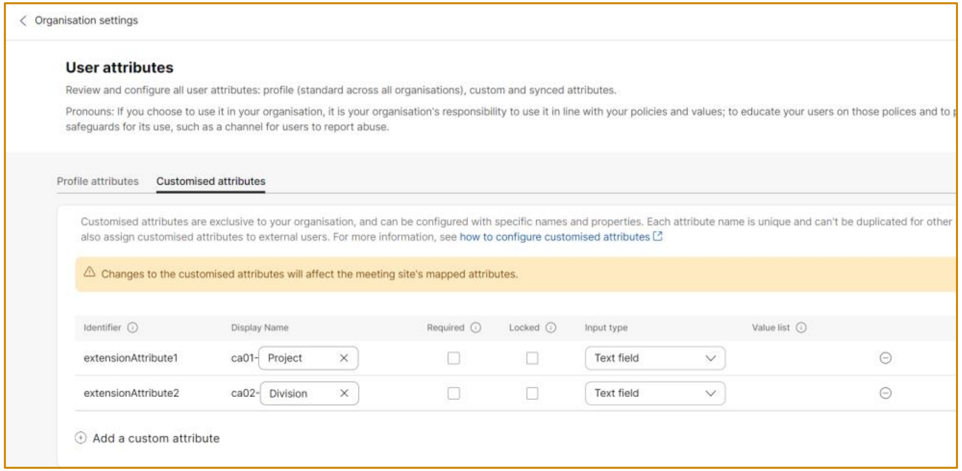
○ Customisable by users
Users can choose to enter customised pronouns via a text field or select their pronouns via a drop-down menu

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 polices and to p
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
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.

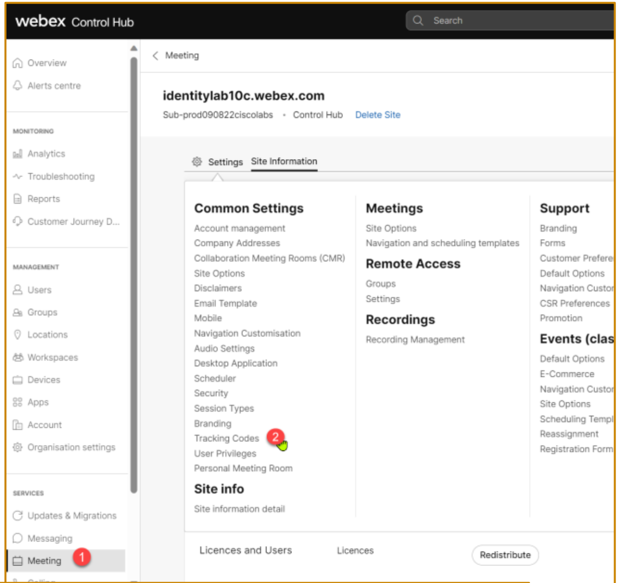
Identifier	Display Name	Required	Locked	Input type	Value list	
extensionAttribute1	ca01- Project	□	□	Text field		⊖
extensionAttribute2	ca02- Division	□	□	Text field		⊖

⊕ Add a custom attribute

User Attributes

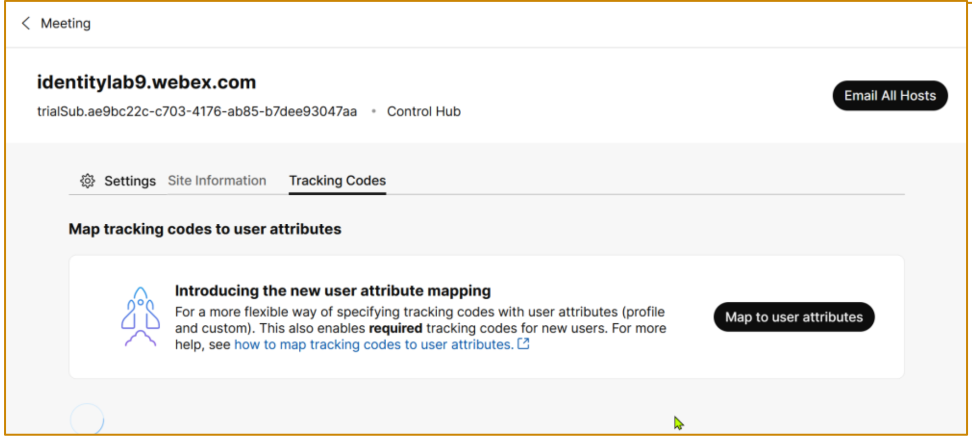
Custom Attributes mapping to tracking codes

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



identitylab10c.webex.com

Sub-prod090822ciscolabs • Control Hub Delete Site



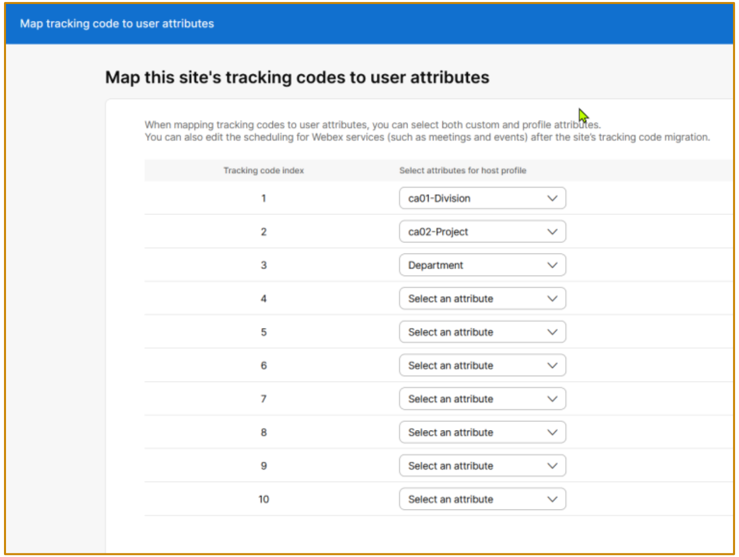
identitylab9.webex.com

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

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 this site's tracking codes to user attributes

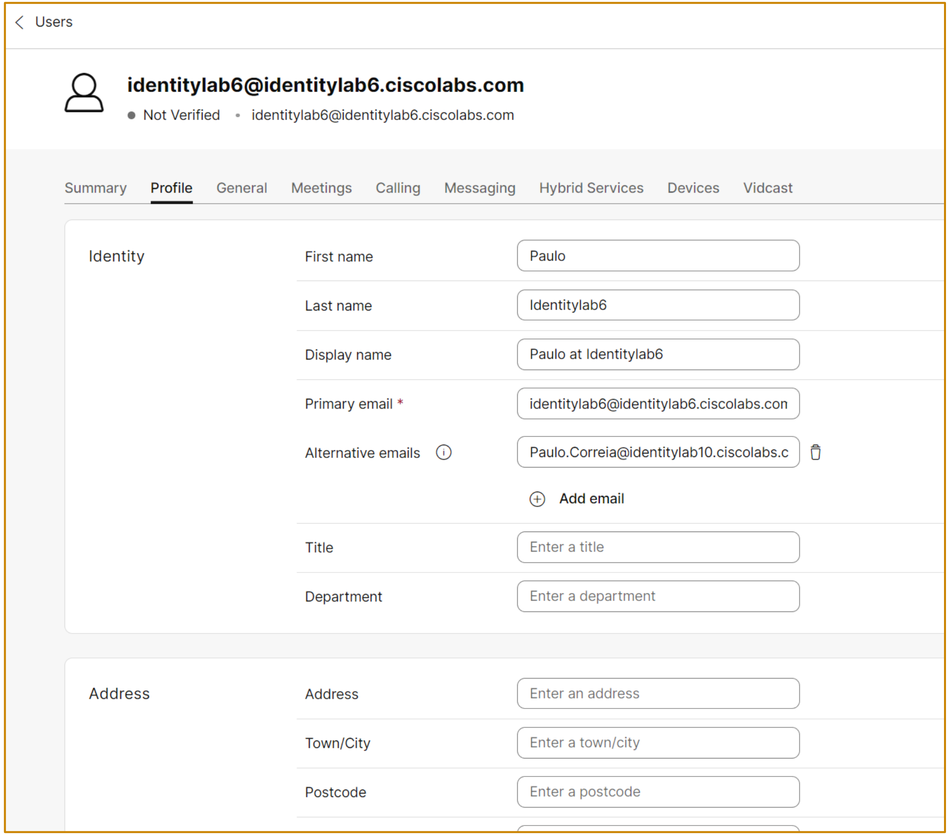
When mapping tracking codes to user attributes, you can select both custom and profile attributes.
You can also edit the scheduling for Webex services (such as meetings and events) after the site's tracking code migration.

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

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



< Users

identitylab6@identitylab6.ciscolabs.com

● Not Verified • identitylab6@identitylab6.ciscolabs.com

Identity

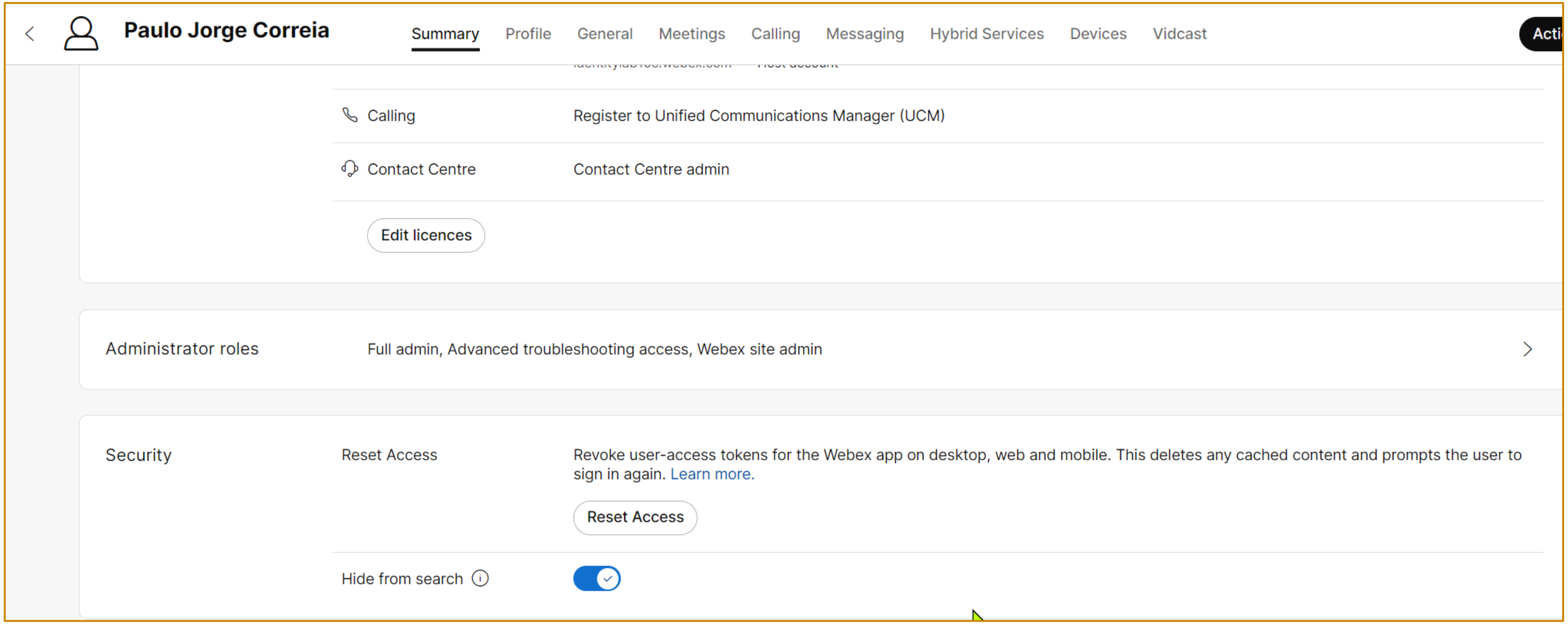
First name	Paulo
Last name	Identitylab6
Display name	Paulo at Identitylab6
Primary email *	identitylab6@identitylab6.ciscolabs.con
Alternative emails ⓘ	Paulo.Correia@identitylab10.ciscolabs.c
	⊕ Add email
Title	Enter a title
Department	Enter a department

Address

Address	Enter an address
Town/City	Enter a town/city
Postcode	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



Calling — Register to Unified Communications Manager (UCM)

Contact Centre — Contact Centre admin

Edit licences

Administrator roles — Full admin, Advanced troubleshooting access, Webex site admin

Security

Reset Access — 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.

Reset Access

Hide from search ⓘ ✓

Webex Provision

Entra ID Wizard

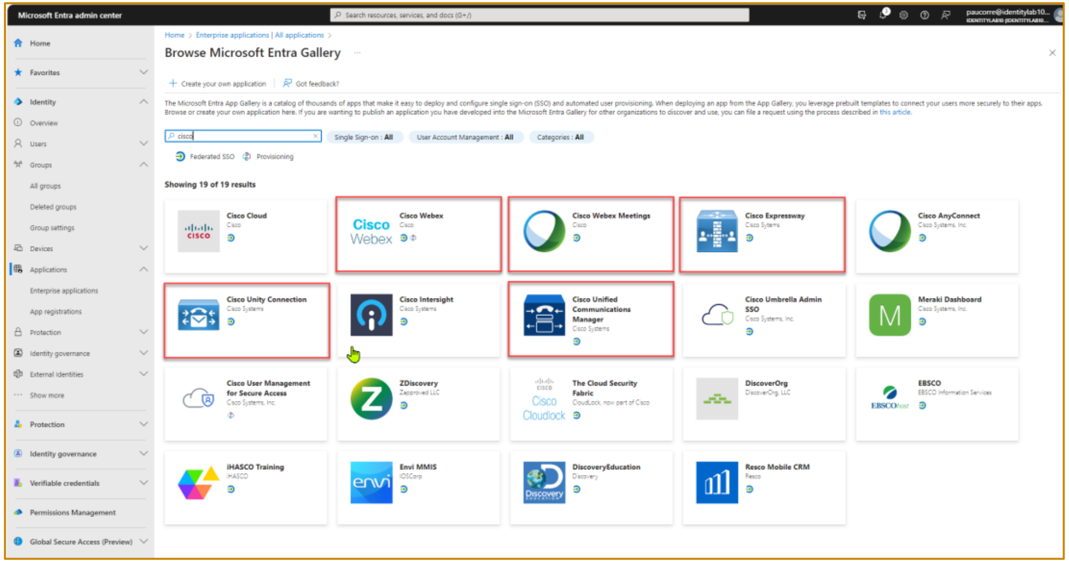
Microsoft Entra ID

Cisco Applications in Entra ID

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

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

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



Home > Enterprise applications | All applications >

Browse Microsoft Entra Gallery

+ Create your own application | Got feedback?

The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Gallery, you leverage prebuilt templates to connect your users more securely to their apps. Browse or create your own application here. If you are wanting to publish an application you have developed into the Microsoft Entra Gallery for other organizations to discover and use, you can file a request using the process described in this article.

cisco | Single Sign-on : All | User Account Management : All | Categories : All

Federated SSO | Provisioning

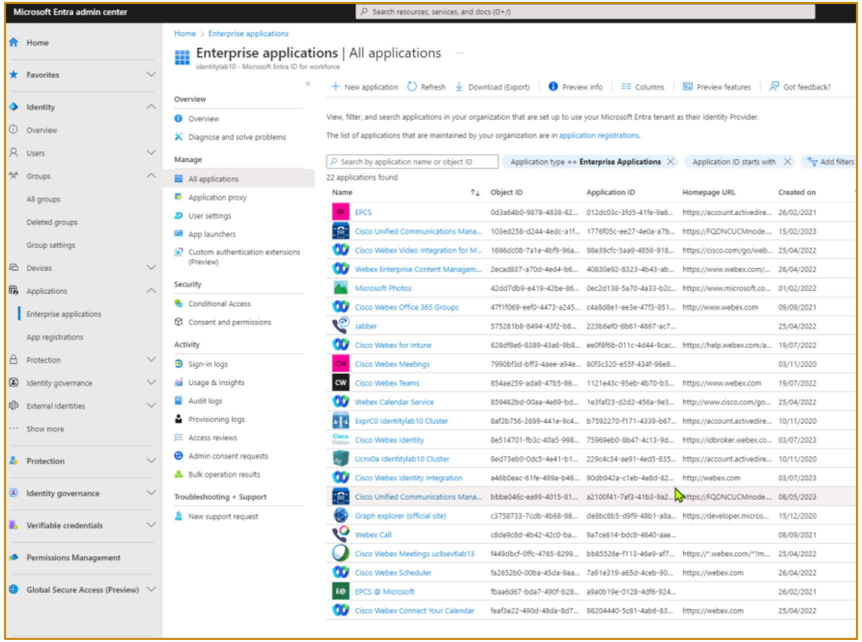
Showing 19 of 19 results

- Cisco Cloud – Cisco
- Cisco Webex – Cisco
- Cisco Webex Meetings – Cisco
- Cisco Expressway – Cisco Sytems
- Cisco AnyConnect – Cisco Systems, Inc.
- Cisco Unity Connection – Cisco Systems
- Cisco Intersight – Cisco Systems
- Cisco Unified Communications Manager – Cisco Systems
- Cisco Umbrella Admin SSO – Cisco Systems, Inc.
- Meraki Dashboard – Cisco Systems, Inc.
- Cisco User Management for Secure Access – Cisco Systems, Inc.
- ZDiscovery – Zapproved LLC
- The Cloud Security Fabric – CloudLock, now part of Cisco
- DiscoverOrg – DiscoverOrg, LLC
- EBSCO – EBSCO Information Services
- iHASCO Training – iHASCO
- Envi MMIS – IOSCorp
- DiscoveryEducation – Discovery
- Resco Mobile CRM – Resco

Microsoft Entra ID

Cisco Applications in Entra ID

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



Enterprise applications | All applications

identitylab10 - Microsoft Entra ID for workforce

View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.

The list of applications that are maintained by your organization are in application registrations.

22 applications found

Name	Object ID	Application ID	Homepage URL	Created on
EP EPCS	0d3a64b0-9878-4838-82...	012dc03c-3fd5-41fe-9a6...	https://account.activedire...	26/02/2021
Cisco Unified Communications Mana...	103ed258-d244-4edc-a1f...	1776f05c-ee27-4e0a-a7b...	https://FQDNCUCMnode....	15/02/2023
Cisco Webex Video Integration for M...	1696dc08-7a1e-4bf9-96a...	98e39cfc-3aa9-4856-918...	https://cisco.com/go/web...	25/04/2022
Webex Enterprise Content Managem...	2ecad837-a70d-4ed4-b6...	40830e92-8323-4b43-ab...	https://www.webex.com/...	26/04/2022
Microsoft Photos	42dd7db9-e419-42be-86...	0ec2d138-5a70-4a33-b2c...	https://www.microsoft.co...	01/02/2022
Cisco Webex Office 365 Groups	47f1f069-eef0-4473-a245...	c4a8d8e1-ee3e-47f3-851...	http://www.webex.com	09/09/2021
Jabber	575281b8-8494-43f2-b8...	223b6ef0-6b61-4867-ac7...		25/04/2022
Cisco Webex for Intune	628df8e6-8389-43a6-9b8...	ee0f8f6b-011c-4d44-9cac...	https://help.webex.com/a...	19/07/2022
CW Cisco Webex Meetings	7990bf3d-bff3-4aee-a94e...	80f3c320-e55f-434f-98e8...		03/11/2020
CW Cisco Webex Teams	854ae259-ada8-47b5-86...	1121e43c-95eb-4b70-b3...	https://www.webex.com	19/07/2022
Webex Calendar Service	859462bd-00aa-4e69-bd...	1e3faf23-d2d2-456a-9e3...	http://www.cisco.com/go...	25/04/2022
ExprC0 Identitylab10 Cluster	8af2b756-2699-441e-9c4...	b7592270-f171-4339-b67...	https://account.activedire...	10/11/2020
Cisco Webex Identity	8e514701-fb3c-40a5-998...	75969eb0-8b47-4c13-9d...	https://idbroker.webex.co...	03/07/2023
Ucnx0a Identitylab10 Cluster	8ed73eb0-0dc5-4e41-b1...	229c4c34-ae91-4ed5-835...	https://account.activedire...	10/11/2020
Cisco Webex Identity Integration	a46b0eac-61fe-499a-b46...	90db942a-c1eb-4e8d-82...	http://webex.com	03/07/2023
Cisco Unified Communications Mana...	bbbe046c-ea99-4015-81...	a2100f41-7af3-41b3-9a2...	https://FQDNCUCMnode....	08/05/2023
Graph explorer (official site)	c3758733-7cdb-4b68-86...	de8bc8b5-d9f9-48b1-a8a...	https://developer.micros...	15/12/2020
Webex Call	c8de9c8d-4b42-42c0-ba...	9a7ce614-bdc8-4640-aae...		08/09/2021
Cisco Webex Meetings uc8sevtlab13	f449dbcf-0ffc-4765-8299...	bb85526e-f113-46e9-af7...	https://*.webex.com/*?m...	25/04/2022
Cisco Webex Scheduler	fa2652b0-00ba-45da-9aa...	7a91e319-a65d-4ceb-90...	https://webex.com	26/04/2022
E@ EPCS @ Microsoft	fbaa6d67-bda7-490f-b28...	a9a0b19e-0128-4df6-924...		26/02/2021
Cisco Webex Connect Your Calendar	feaf3e22-490d-48da-8d7...	98204440-5c81-4ab6-83...	https://webex.com	25/04/2022

Microsoft Entra ID

Cisco Applications in Entra ID

Application created using MS Graph API

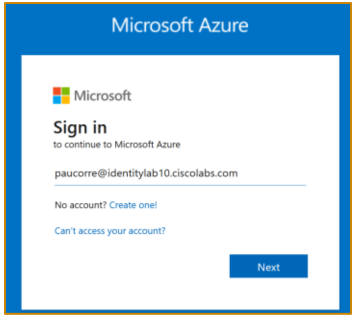
Entra ID Enterprise application	App ID
Webex Teams Enterprise Content Management	40830e92-8323-4b43-abd5-ca6b81d39b75
Cisco Webex Office 365 Groups	c4a8d8e1-ee3e-47f3-8514-2a4e6fea5b5c
Webex Calendar Service (Admin Consent)	1e3faf23-d2d2-456a-9e3e-55db63b869b0 189ea49b-75a4-4e53-a013-2aed74803405
Cisco 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 ID Wizard)	f6016c4c-c015-453c-8ea6-dfc146f7eb7f
Cisco Webex Identity Synchronization (CH Entra ID Wizard)	90db942a-c1eb-4e8d-82e4-eebf64a7e2ae
Cisco Webex Identity Integration for Migration (CH Entra ID 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 ID

Consent given by Administrators or Users

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

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



Microsoft Azure

Microsoft

Sign in

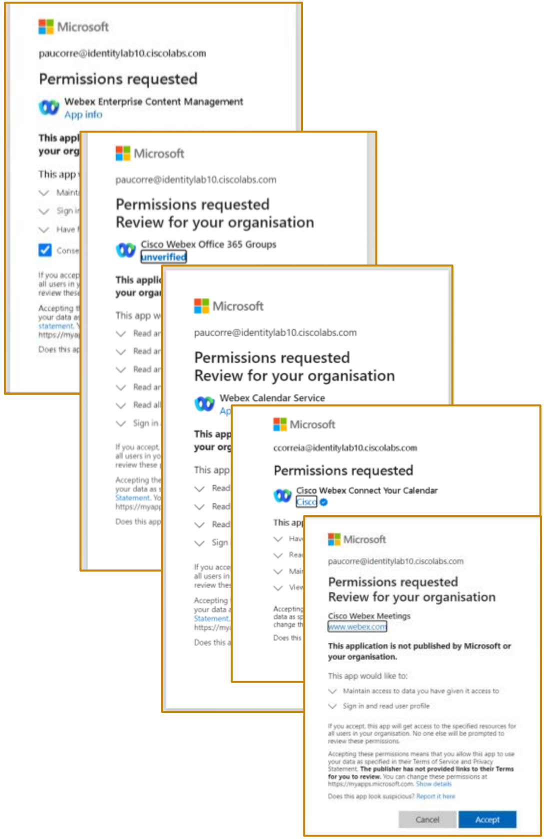
to continue to Microsoft Azure

paucorre@identitylab10.ciscolabs.com

No account? Create one!

Can't access your account?

Next



Microsoft

paucorre@identitylab10.ciscolabs.com

Permissions requested

Webex Enterprise Content Management

App info

Microsoft

paucorre@identitylab10.ciscolabs.com

Permissions requested
Review for your organisation

Cisco Webex Office 365 Groups

unverified

Microsoft

paucorre@identitylab10.ciscolabs.com

Permissions requested
Review for your organisation

Webex Calendar Service

Microsoft

ccorreia@identitylab10.ciscolabs.com

Permissions requested

Cisco Webex Connect Your Calendar

Cisco

Microsoft

paucorre@identitylab10.ciscolabs.com

Permissions requested
Review for your organisation

Cisco Webex Meetings

www.webex.com

This application is not published by Microsoft or your organisation.

This app would like to:

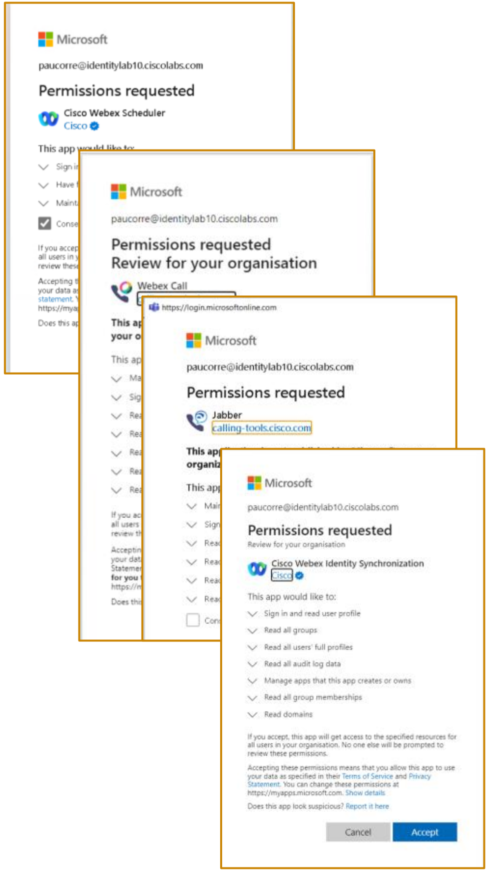
- Maintain access to data you have given it access to
- Sign in and read user profile

If you accept, this app will get access to the specified resources for all users in your organisation. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their Terms of Service and Privacy Statement. **The publisher has not provided links to their Terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

Cancel Accept



Microsoft

paucorre@identitylab10.ciscolabs.com

Permissions requested

Cisco Webex Scheduler

Cisco

Microsoft

paucorre@identitylab10.ciscolabs.com

Permissions requested
Review for your organisation

Webex Call

https://login.microsoftonline.com

Microsoft

paucorre@identitylab10.ciscolabs.com

Permissions requested

Jabber

calling-tools.cisco.com

Microsoft

paucorre@identitylab10.ciscolabs.com

Permissions requested

Review for your organisation

Cisco Webex Identity Synchronization

Cisco

This app would like to:

- Sign in and read user profile
- Read all groups
- Read all users' full profiles
- Read all audit log data
- Manage apps that this app creates or owns
- Read all group memberships
- Read domains

If you accept, this app will get access to the specified resources for all users in your organisation. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their Terms of Service and Privacy Statement. You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

Cancel Accept

Microsoft Entra ID

Consent given by Administrators or Users

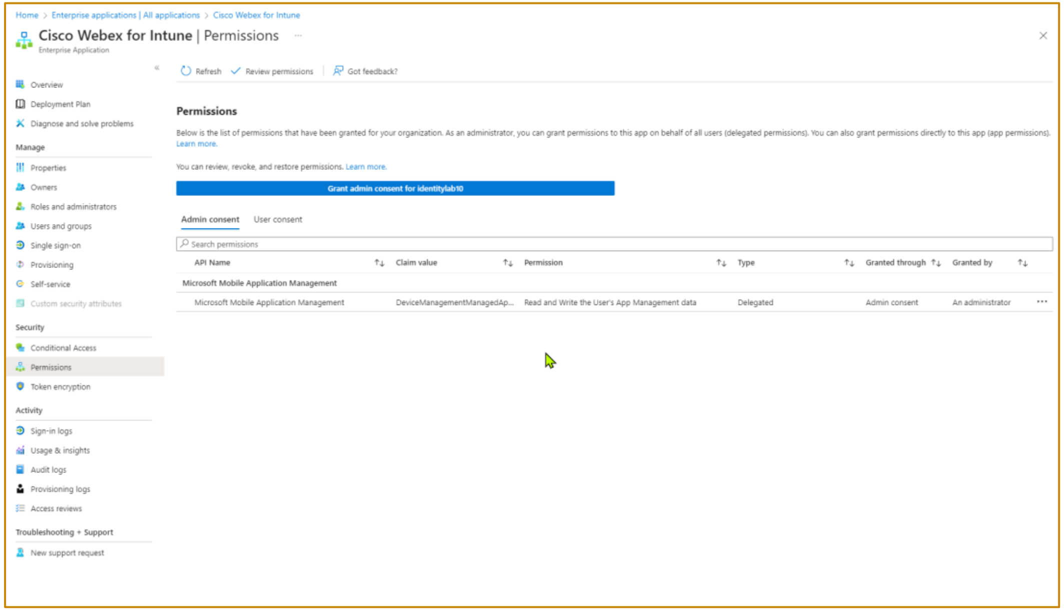
Sometimes the users in Webex doesn’t has permission to allow consent as an administrator in Entra ID.

It is possible in the desktop of the Entra ID 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



Permissions

Below is the list of permissions that have been granted for your organization. As an administrator, you can grant permissions to this app on behalf of all users (delegated permissions). You can also grant permissions directly to this app (app permissions). Learn more.

You can review, revoke, and restore permissions. Learn more.

API Name	Claim value	Permission	Type	Granted through	Granted by
Microsoft Mobile Application Management					
Microsoft Mobile Application Management	DeviceManagementManagedAp...	Read and Write the User's App Management data	Delegated	Admin consent	An administrator

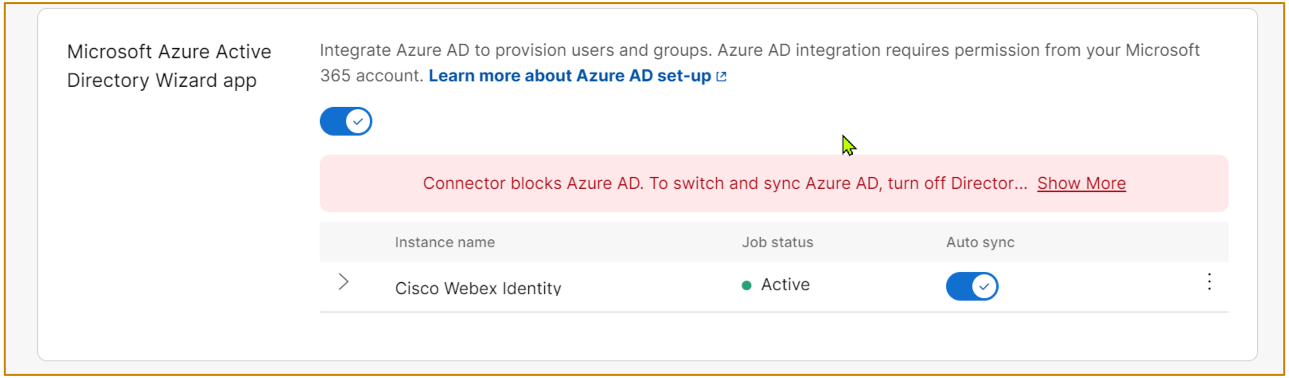
Microsoft Entra ID

Entra ID Wizard

Cisco Wizard from Control Hub that will configure the Webex Identity integration in Entra ID Portal.

Bring additional functionalities to what SCIM protocol can deliver.

Doesn't require any knowledge on Entra ID configuration, and providing a straightforward integration for Provision and Single Sign-On



Microsoft Azure Active Directory Wizard app

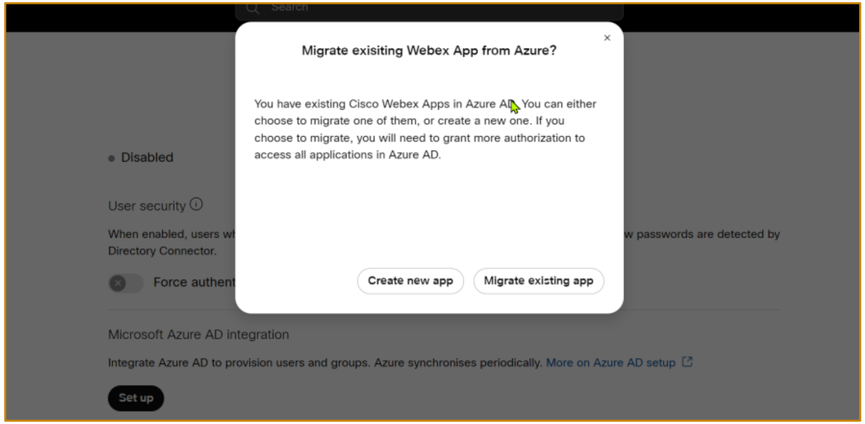
Integrate Azure AD to provision users and groups. Azure AD integration requires permission from your Microsoft 365 account. Learn more about Azure AD set-up

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 ID

Entra ID Wizard



Migrate exisiting Webex App from Azure?

You have existing Cisco Webex Apps in Azure AD. You can either choose to migrate one of them, or create a new one. If you choose to migrate, you will need to grant more authorization to access all applications in Azure AD.

Search
×
Create new app
Migrate existing app
Disabled
User security
When enabled, users w... w passwords are detected by Directory Connector.
Force authent...
Microsoft Azure AD integration
Integrate Azure AD to provision users and groups. Azure synchronises periodically. More on Azure AD setup
Set up

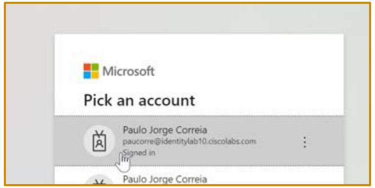
Entra ID Wizard allow us to migrate existent application that does User Provision using SCIM and SSO using SAML or create a new integration.

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 ID

Entra ID Wizard

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

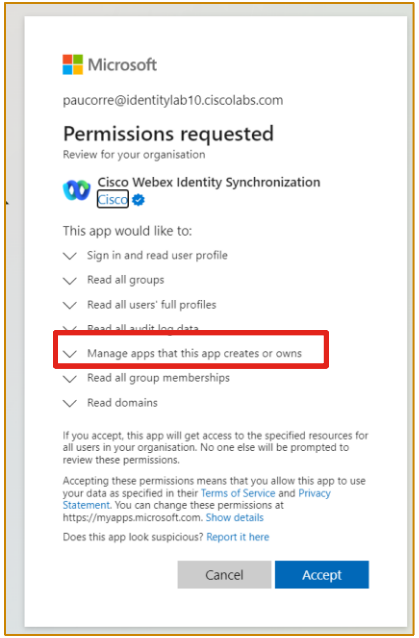


Microsoft

Pick an account

Paulo Jorge Correia
paucorre@identitylab10.ciscolabs.com
Signed in

Paulo Jorge Correia



Microsoft

paucorre@identitylab10.ciscolabs.com

Permissions requested

Review for your organisation

Cisco Webex Identity Synchronization
Cisco

This app would like to:

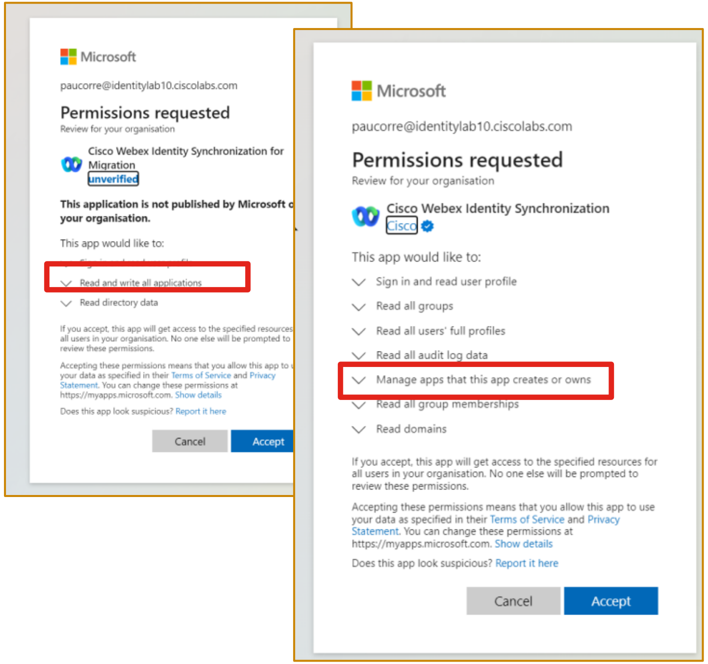
- Sign in and read user profile
- Read all groups
- Read all users' full profiles
- Read all audit log data
- Manage apps that this app creates or owns
- Read all group memberships
- Read domains

If you accept, this app will get access to the specified resources for all users in your organisation. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their Terms of Service and Privacy Statement. You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

Permission to create a **new application**



Microsoft

paucorre@identitylab10.ciscolabs.com

Permissions requested

Review for your organisation

Cisco Webex Identity Synchronization for Migration
unverified

This application is not published by Microsoft o your organisation.

This app would like to:

- Read and write all applications
- Read directory data

If you accept, this app will get access to the specified resources all users in your organisation. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to your data as specified in their Terms of Service and Privacy Statement. You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

Microsoft

paucorre@identitylab10.ciscolabs.com

Permissions requested

Review for your organisation

Cisco Webex Identity Synchronization
Cisco

This app would like to:

- Sign in and read user profile
- Read all groups
- Read all users' full profiles
- Read all audit log data
- Manage apps that this app creates or owns
- Read all group memberships
- Read domains

If you accept, this app will get access to the specified resources for all users in your organisation. No one else will be prompted to review these permissions.

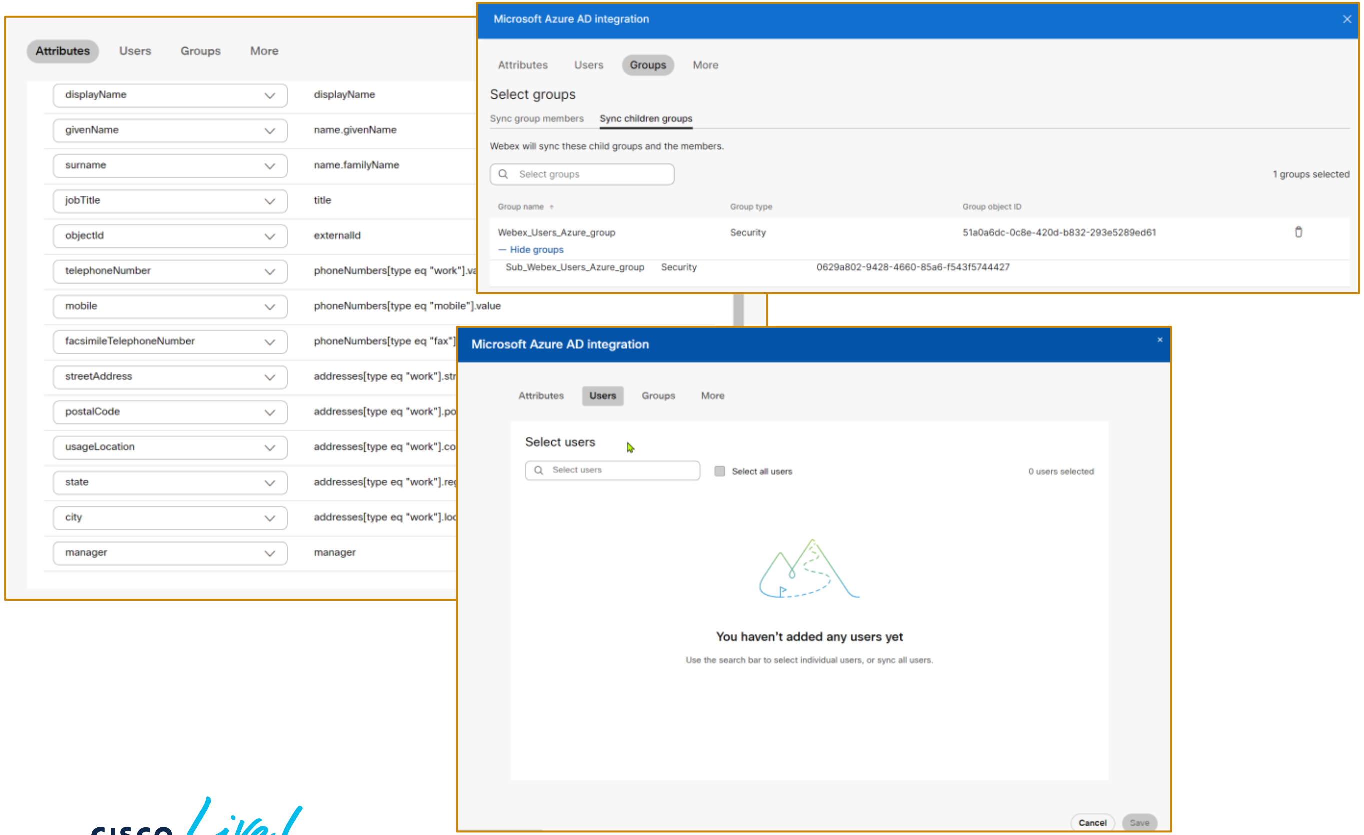
Accepting these permissions means that you allow this app to use your data as specified in their Terms of Service and Privacy Statement. You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

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

Microsoft Entra ID

Entra ID Wizard



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

Microsoft Azure AD integration

Select groups

Webex will sync these child groups and the members.

1 groups selected

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

Microsoft Azure AD integration

Select users

0 users selected

You haven't added any users yet

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

Allow us to map attributes.

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

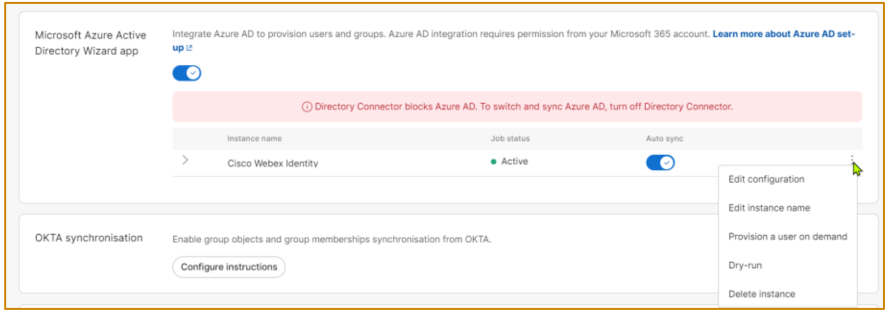
Manager attribute is possible now

Microsoft Entra ID

Entra ID 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 Azure Active Directory Wizard app

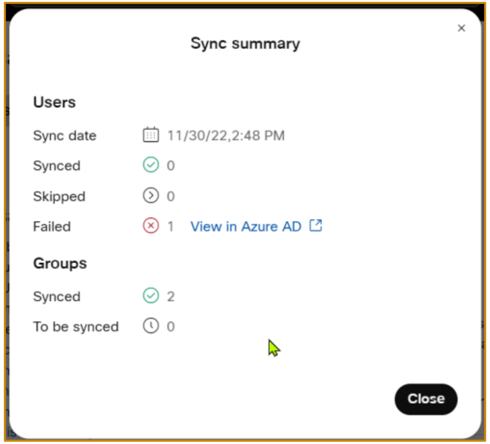
Integrate Azure AD to provision users and groups. Azure AD integration requires permission from your Microsoft 365 account. **Learn more about Azure AD set-up**

Directory Connector blocks Azure AD. To switch and sync Azure AD, turn off Directory Connector.

Instance name	Job status	Auto sync
Cisco Webex Identity	● Active	

OKTA synchronisation

Enable group objects and group memberships synchronisation from OKTA.



Sync summary

Users

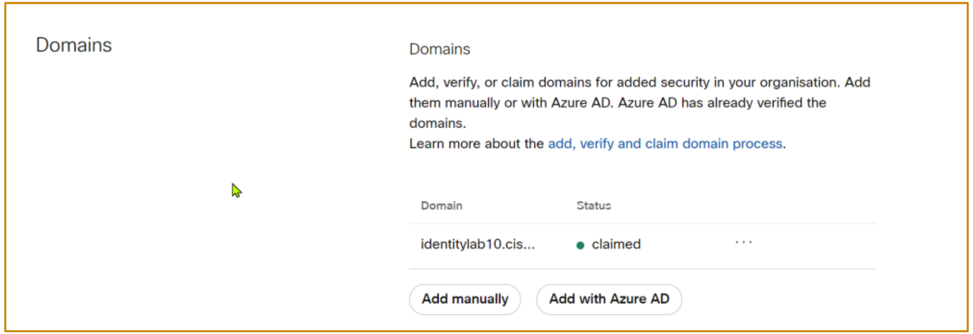
Sync date	11/30/22,2:48 PM
Synced	✓ 0
Skipped	0
Failed	✕ 1 View in Azure AD

Groups

Synced	✓ 2
To be synced	0

Microsoft Entra ID

Entra ID Wizard



Domains

Domains

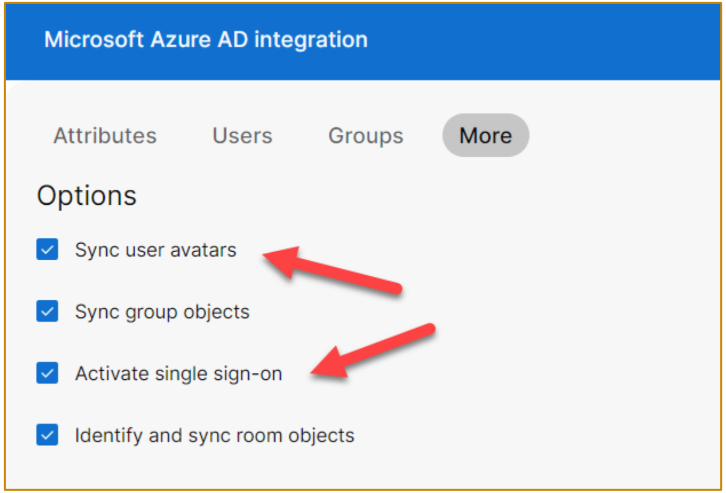
Add, verify, or claim domains for added security in your organisation. Add them manually or with Azure AD. Azure AD has already verified the domains.
Learn more about the add, verify and claim domain process.

Domain	Status
identitylab10.cis...	● claimed

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

Microsoft Entra ID

Entra ID Wizard



Microsoft Azure AD integration

Options

☑ Sync user avatars

☑ Sync group objects

☑ Activate single sign-on

☑ Identify and sync room objects

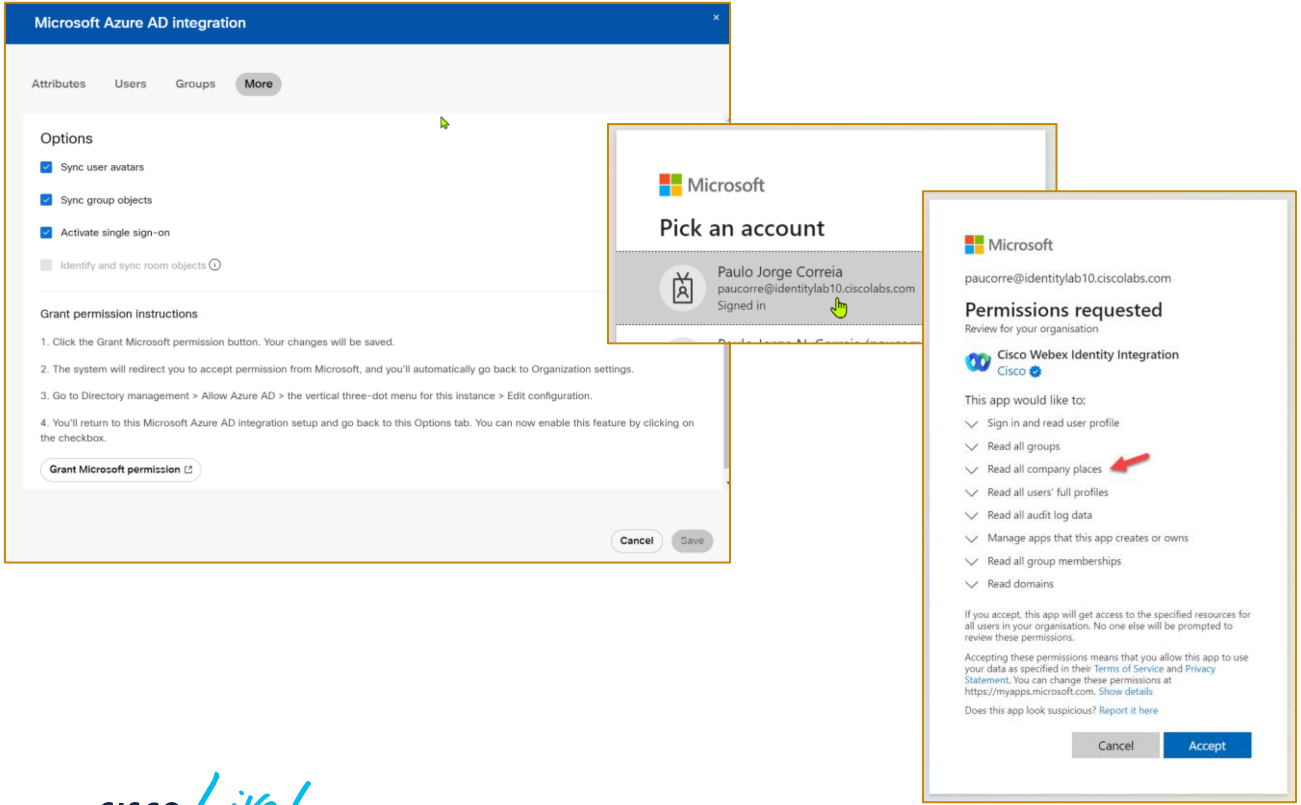
Allow us to sync Avatars.

Can also configure the SSO integration with Entra ID 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 ID

Entra ID Wizard



Microsoft Azure AD integration

Options

☑ Sync user avatars

☑ Sync group objects

☑ Activate single sign-on

☐ Identify and sync room objects

Grant permission instructions

1. Click the Grant Microsoft permission button. Your changes will be saved.
2. The system will redirect you to accept permission from Microsoft, and you'll automatically go back to Organization settings.
3. Go to Directory management > Allow Azure AD > the vertical three-dot menu for this instance > Edit configuration.
4. You'll return to this Microsoft Azure AD integration setup and go back to this Options tab. You can now enable this feature by clicking on the checkbox.

Microsoft

Pick an account

Paulo Jorge Correia
paucorre@identitylab10.ciscolabs.com
Signed in

Microsoft

paucorre@identitylab10.ciscolabs.com

Permissions requested

Review for your organisation

Cisco Webex Identity Integration
Cisco

This app would like to:

- Sign in and read user profile
- Read all groups
- Read all company places
- Read all users' full profiles
- Read all audit log data
- Manage apps that this app creates or owns
- Read all group memberships
- Read domains

If you accept, this app will get access to the specified resources for all users in your organisation. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their Terms of Service and Privacy Statement. You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

To allow for rooms objects to be imported from Entra ID an extension of permission will be needed to accept to Company places in Entra ID

Microsoft Entra ID

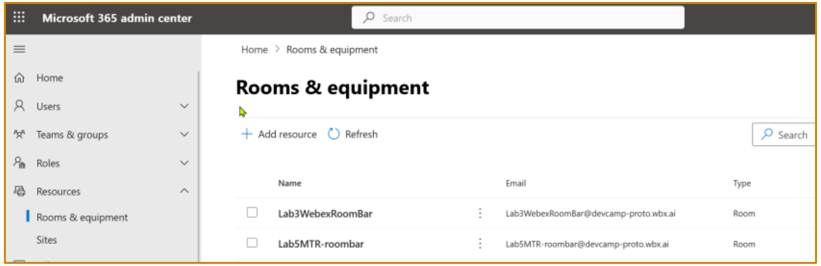
Creating Workspaces from IDM’s

Workspace can be automatically synchronized from IDM’s.

Supported sources:

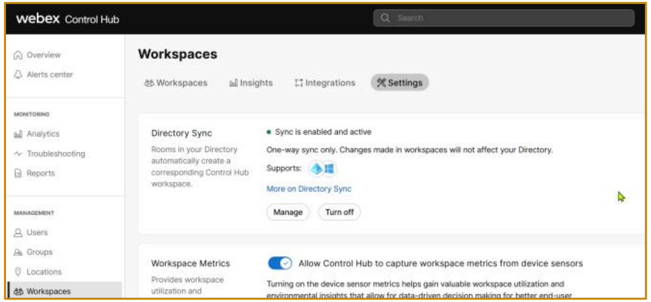
Active Directory (https://help.webex.com/en-us/article/np2gdab/Directory-sync-from-Workspaces-in-Control-Hub)

- Microsoft 365 Room Resource



Rooms & equipment

	Name	Email	Type
□	Lab3WebexRoomBar	Lab3WebexRoomBar@devcamp-proto.wbx.ai	Room
□	Lab5MTR-roombar	Lab5MTR-roombar@devcamp-proto.wbx.ai	Room



Workspaces

Directory Sync

Rooms in your Directory automatically create a corresponding Control Hub workspace.

● Sync is enabled and active

One-way sync only. Changes made in workspaces will not affect your Directory.

Supports:

More on Directory Sync

Workspace Metrics

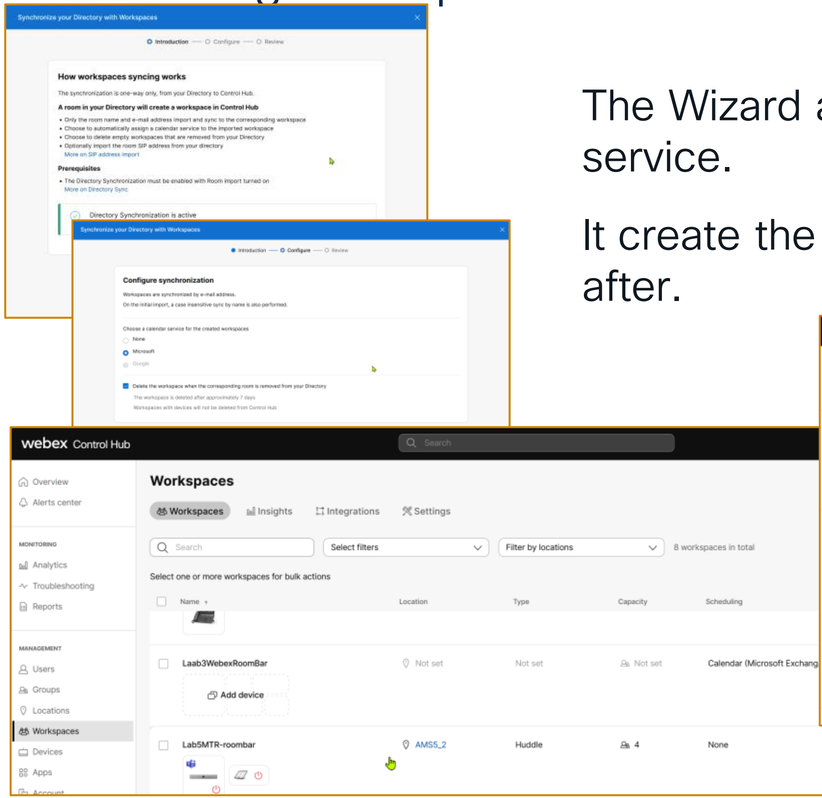
Provides workspace utilization and

Allow Control Hub to capture workspace metrics from device sensors

Turning on the device sensor metrics helps gain valuable workspace utilization and environmental insights that allow for data-driven decision making for better end-user

Microsoft Entra ID

Creating Workspaces from Directories



Synchronize your Directory with Workspaces

○ Introduction — ○ Configure — ○ Review

How workspaces syncing works

The synchronization is one-way only, from your Directory to Control Hub.

A room in your Directory will create a workspace in Control Hub

- Only the room name and e-mail address import and sync to the corresponding workspace
- Choose to automatically assign a calendar service to the imported workspace
- Choose to delete empty workspaces that are removed from your Directory
- Optionally import the room SIP address from your directory
  More on SIP address import

Prerequisites

- The Directory Synchronization must be enabled with Room import turned on
  More on Directory Sync

Directory Synchronization is active

Synchronize your Directory with Workspaces

● Introduction — ○ Configure — ○ Review

Configure synchronization

Workspaces are synchronized by e-mail address.
On the initial import, a case insensitive sync by name is also performed.

Choose a calendar service for the created workspaces

○ None
● Microsoft
○ Google

☑ Delete the workspace when the corresponding room is removed from your Directory
The workspace is deleted after approximately 7 days
Workspaces with devices will not be deleted from Control Hub

webex Control Hub

Workspaces

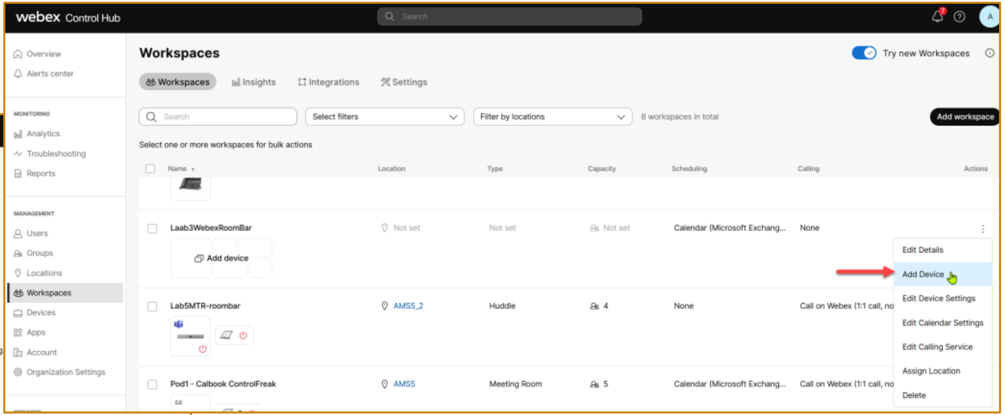
Select one or more workspaces for bulk actions

8 workspaces in total

Name	Location	Type	Capacity	Scheduling	Calling
Laab3WebexRoomBar	Not set	Not set	Not set	Calendar (Microsoft Exchang	
Lab5MTR-roombar	AMS5_2	Huddle	4	None	Call on Webex (1:1 call, non-...

The Wizard allow us to link the workspace with the calendar service.

It create the workspace itself allowing the device association after.



webex Control Hub

Workspaces

Select one or more workspaces for bulk actions

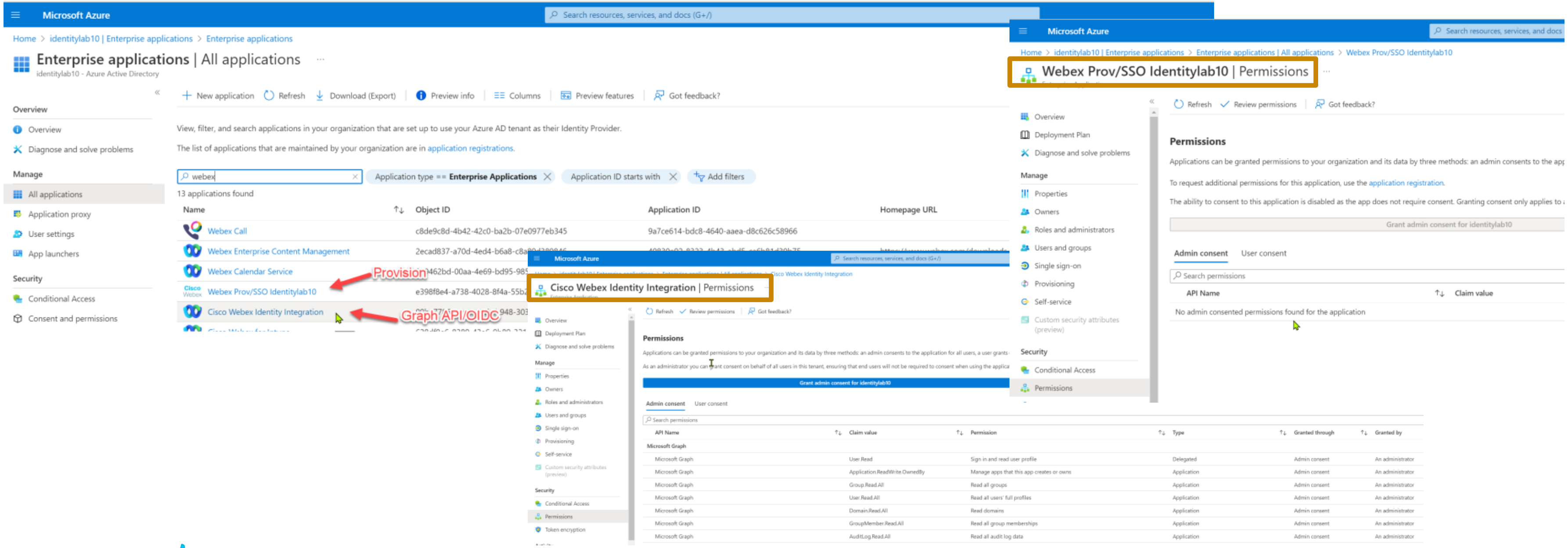
8 workspaces in total

Name	Location	Type	Capacity	Scheduling	Calling	Actions
Laab3WebexRoomBar	Not set	Not set	Not set	Calendar (Microsoft Exchang...	None	
Lab5MTR-roombar	AMS5_2	Huddle	4	None	Call on Webex (1:1 call, no	
Pod1 - Calbook ControlFreak	AMS5	Meeting Room	5	Calendar (Microsoft Exchang...	Call on Webex (1:1 call, no	

Microsoft Entra ID

Entra ID Wizard

What to expect in Entra ID Enterprise Applications created by Webex Entra ID Wizard



Microsoft Azure
Search resources, services, and docs (G+/)
Home > identitylab10 | Enterprise applications > Enterprise applications

Enterprise applications | All applications

identitylab10 - Azure Active Directory

View, filter, and search applications in your organization that are set up to use your Azure AD tenant as their Identity Provider.

The list of applications that are maintained by your organization are in application registrations.

webex | Application type == **Enterprise Applications** | Application ID starts with | Add filters

13 applications found

Name	Object ID	Application ID	Homepage URL
Webex Call	c8de9c8d-4b42-42c0-ba2b-07e0977eb345	9a7ce614-bdc8-4640-aaea-d8c626c58966	
Webex Enterprise Content Management	2ecad837-a70d-4ed4-b6a8-c8a		
Webex Calendar Service	462bd-00aa-4e69-bd95-985		
Webex Prov/SSO Identitylab10	e398f8e4-a738-4028-8f4a-55b2		
Cisco Webex Identity Integration	948-303		

Provision

Graph API/OIDC

Microsoft Azure
Search resources, services, and docs (G+/)
Cisco Webex Identity Integration

Cisco Webex Identity Integration | Permissions

Permissions

Applications can be granted permissions to your organization and its data by three methods: an admin consents to the application for all users, a user grants

As an administrator you can grant consent on behalf of all users in this tenant, ensuring that end users will not be required to consent when using the applica

Grant admin consent for identitylab10

Admin consent | User consent

Search permissions

API Name	Claim value	Permission	Type	Granted through	Granted by
Microsoft Graph					
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

Microsoft Azure
Search resources, services, and docs
Home > identitylab10 | Enterprise applications > Enterprise applications | All applications > Webex Prov/SSO Identitylab10

Webex Prov/SSO Identitylab10 | Permissions

Permissions

Applications can be granted permissions to your organization and its data by three methods: an admin consents to the app

To request additional permissions for this application, use the application registration.

The ability to consent to this application is disabled as the app does not require consent. Granting consent only applies to

Grant admin consent for identitylab10

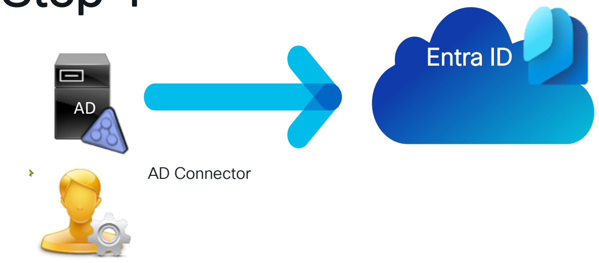
Admin consent | User consent

Search permissions

API Name	Claim value
No admin consented permissions found for the application	

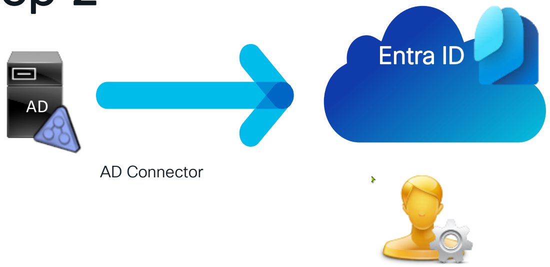
Identity Management migration from AD to Entra ID from Microsoft perspective?

Step 1



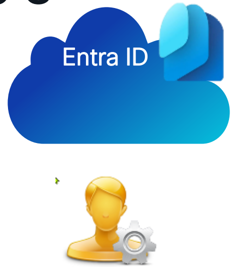
Initially all the Create, Read, Update and Delete Operations (CRUD) will be done in AD.

Step 2



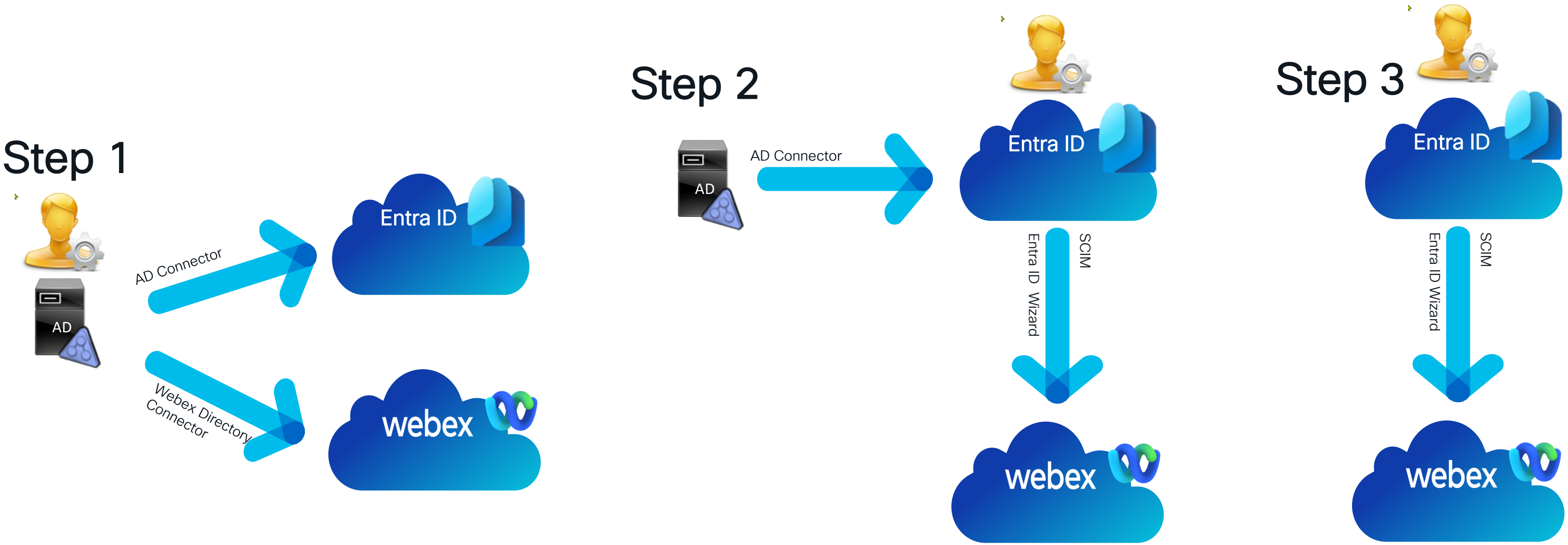
At some point they will migrate the CRUD operation to Entra ID and at that point AD is only for Legacy applications, and there will be users in the cloud that no longer exist on-premise

Step 3



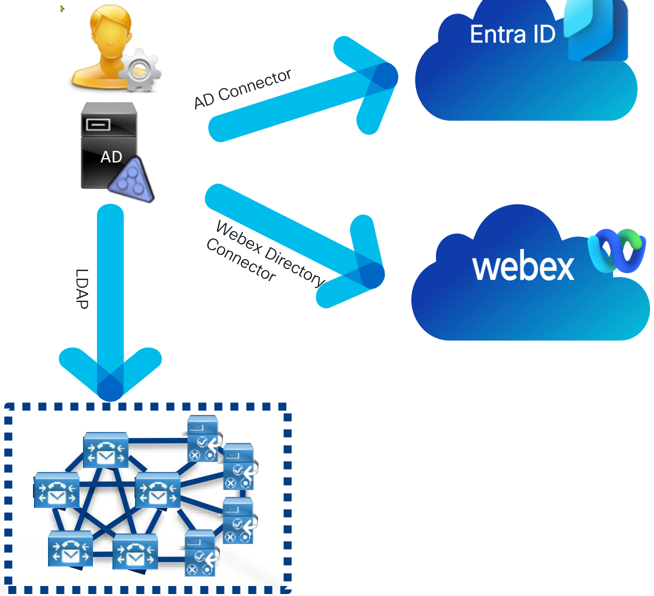
There isn't any longer an AD on-premise

Webex Integration for each step recommendation

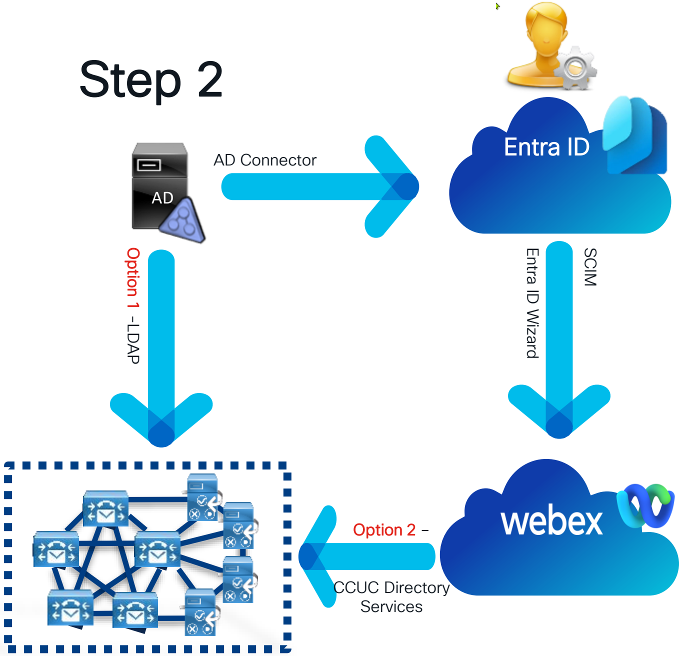


And if the customer still has CUCM and other on-premise services?

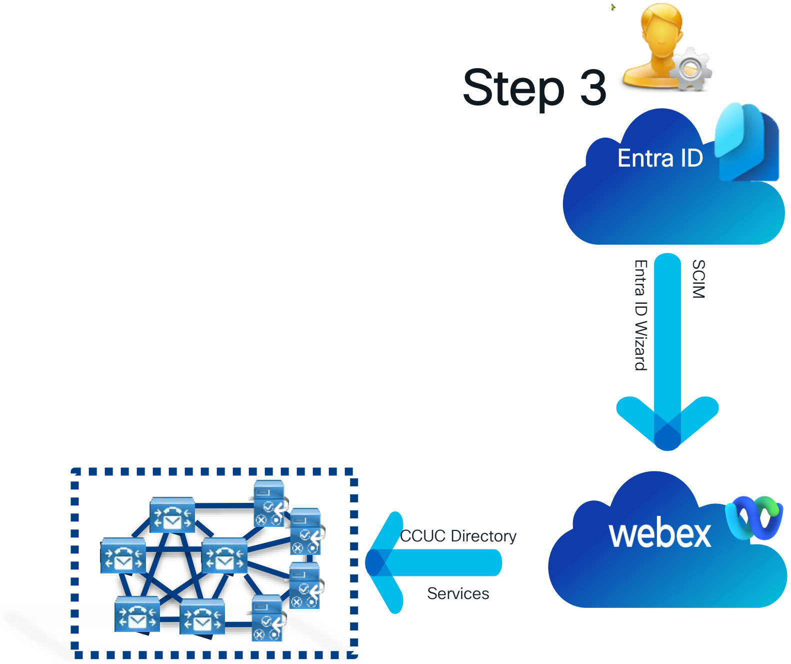
Step 1



Step 2



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

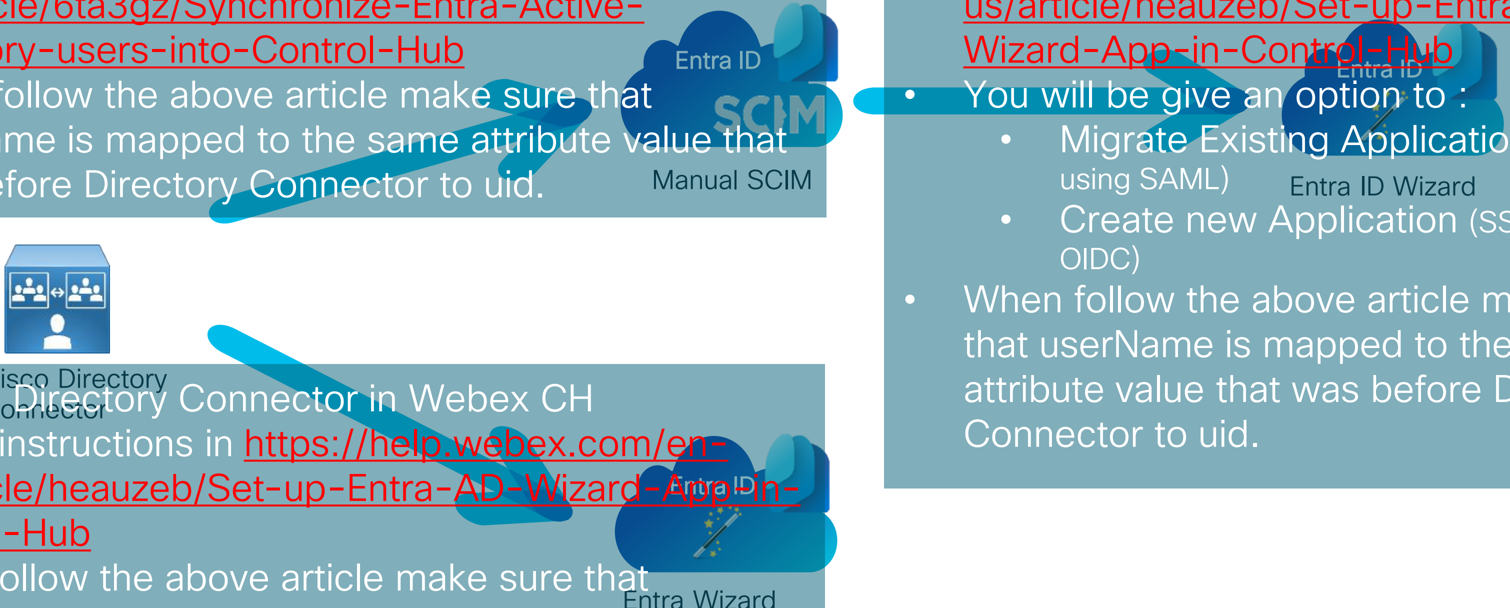


How do we Migrate from one to the other ?

- 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.

- Follow instructions in https://help.webex.com/en-us/article/heauzeb/Set-up-Entra-AD-Wizard-App-in-Control-Hub
- You will be give an option to :
  - Migrate Existing Application (SSO using SAML)
  - 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.

- Disable Directory Connector in Webex CH
- Follow instructions in https://help.webex.com/en-us/article/heauzeb/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.



Comparing SCIM, Entra ID Wizard & Directory Connector

	SCIM 1.1	SCIM 2.0	Entra ID 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	❌	❌	❌	✅

* Near Future

OpenID Connect

how does it work?

What is OpenID Connect ?

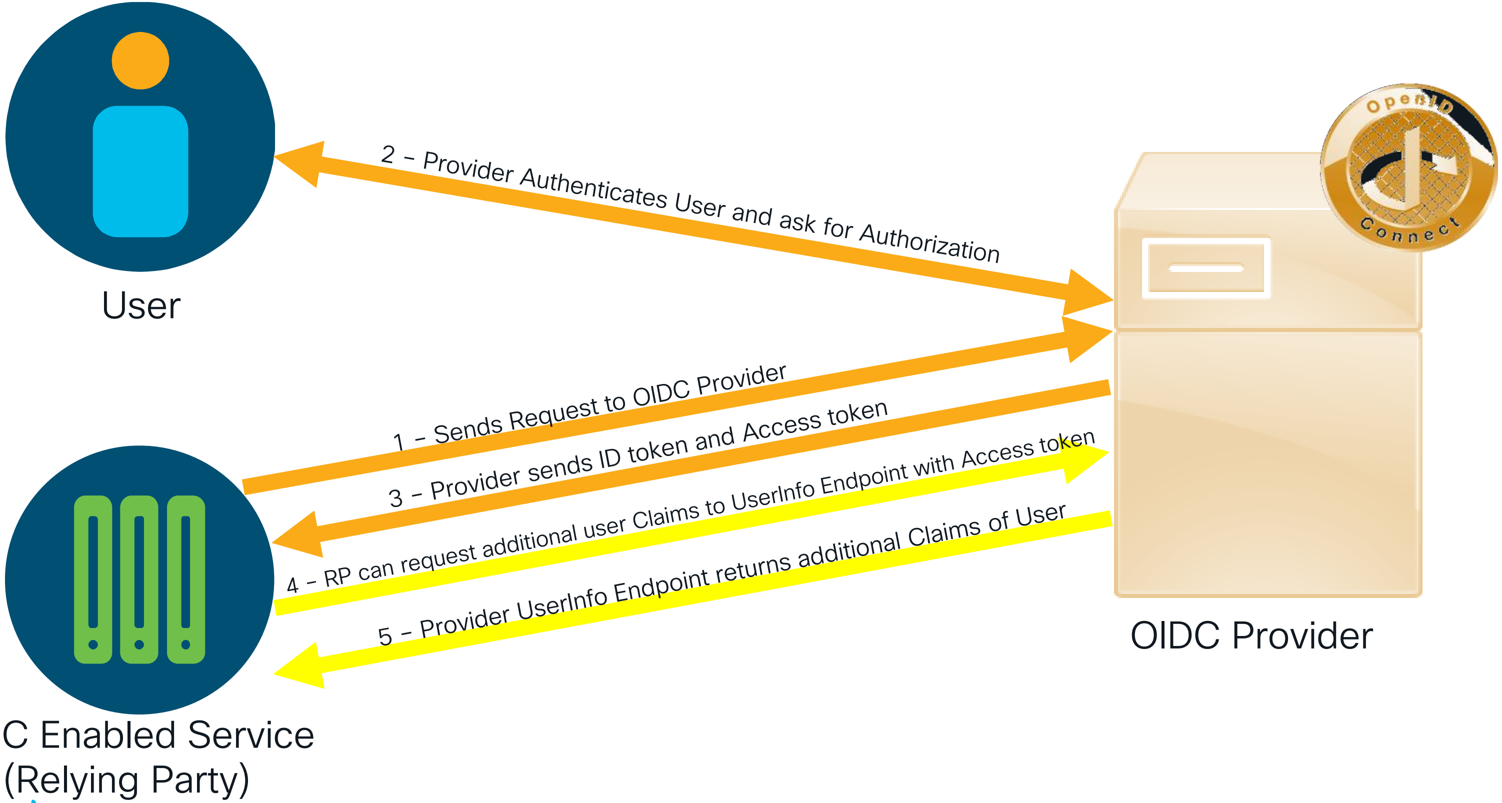
OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol.

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



User

2 – Provider Authenticates User and ask for Authorization

1 – Sends Request to OIDC Provider

3 – Provider sends ID token and Access token

4 – RP can request additional user Claims to UserInfo Endpoint with Access token

5 – Provider UserInfo Endpoint returns additional Claims of User

OIDC Provider

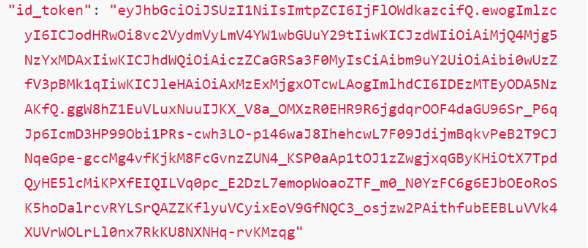
OIDC Enabled Service (Relying Party)

ID Token

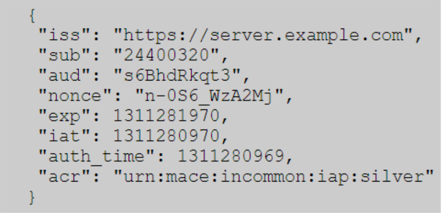
The ID Token is a security token that contains Claims about the Authentication of an End-User by an Authorization Server when using a Client, and potentially other requested Claims.

The ID Token is represented as a JSON Web Token (JWT)

More information in https://openid.net/specs/openid-connect-core-1_0.html#IDToken



```
"id_token": "eyJhbGciOiJSUzI1NiIsImtpZCI6IjFlOWdkazcifQ.ewogImlzc
  yI6ICJodHRwOi8vc2VydmVyLmV4YW1wbGUuY29tIiwKICJzdWIiOiAiMjQ4Mjg5
  NzYxMDAxIiwKICJhdWQiOiAiczZCaGRSa3F0MyIsCiAibm9uY2UiOiAibi0wUzZ
  fV3pBMk1qIiwKICJleHAiOiAxMzExMjgxOTcwLAogImlhdCI6IDEzMTEyODA5Nz
  AKfQ.ggW8hZ1EuVLuxNuuIJKX_V8a_OMXzR0EHR9R6jgdqrOOF4daGU96Sr_P6q
  Jp6IcmD3HP99Obi1PRs-cwh3LO-p146waJ8IhehcwL7F09JdijmBqkvPeB2T9CJ
  NqeGpe-gccMg4vfKjkM8FcGvnzZUN4_KSP0aAp1tOJ1zZwgjxqGByKHiOtX7Tpd
  QyHE5lcMiKPXfEIQILVq0pc_E2DzL7emopWoaoZTF_m0_N0YzFC6g6EJbOEoRoS
  K5hoDalrcvRYLSrQAZZKflyuVCyixEoV9GfNQC3_osjzw2PAithfubEEBLuVVk4
  XUVrWOLrLl0nx7RkKU8NXNHq-rvKMzqg"
```



```
{
 "iss": "https://server.example.com",
 "sub": "24400320",
 "aud": "s6BhdRkqt3",
 "nonce": "n-0S6_WzA2Mj",
 "exp": 1311281970,
 "iat": 1311280970,
 "auth_time": 1311280969,
 "acr": "urn:mace:incommon:iap:silver"
}
```

https://jwt.io/

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.

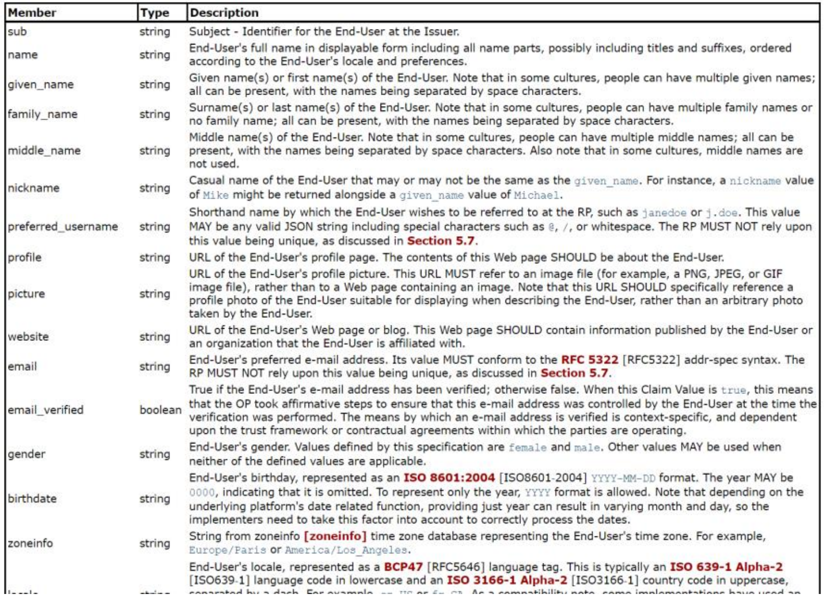
More information in https://openid.net/specs/openid-connect-core-1_0.html#Claims

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"
}
```

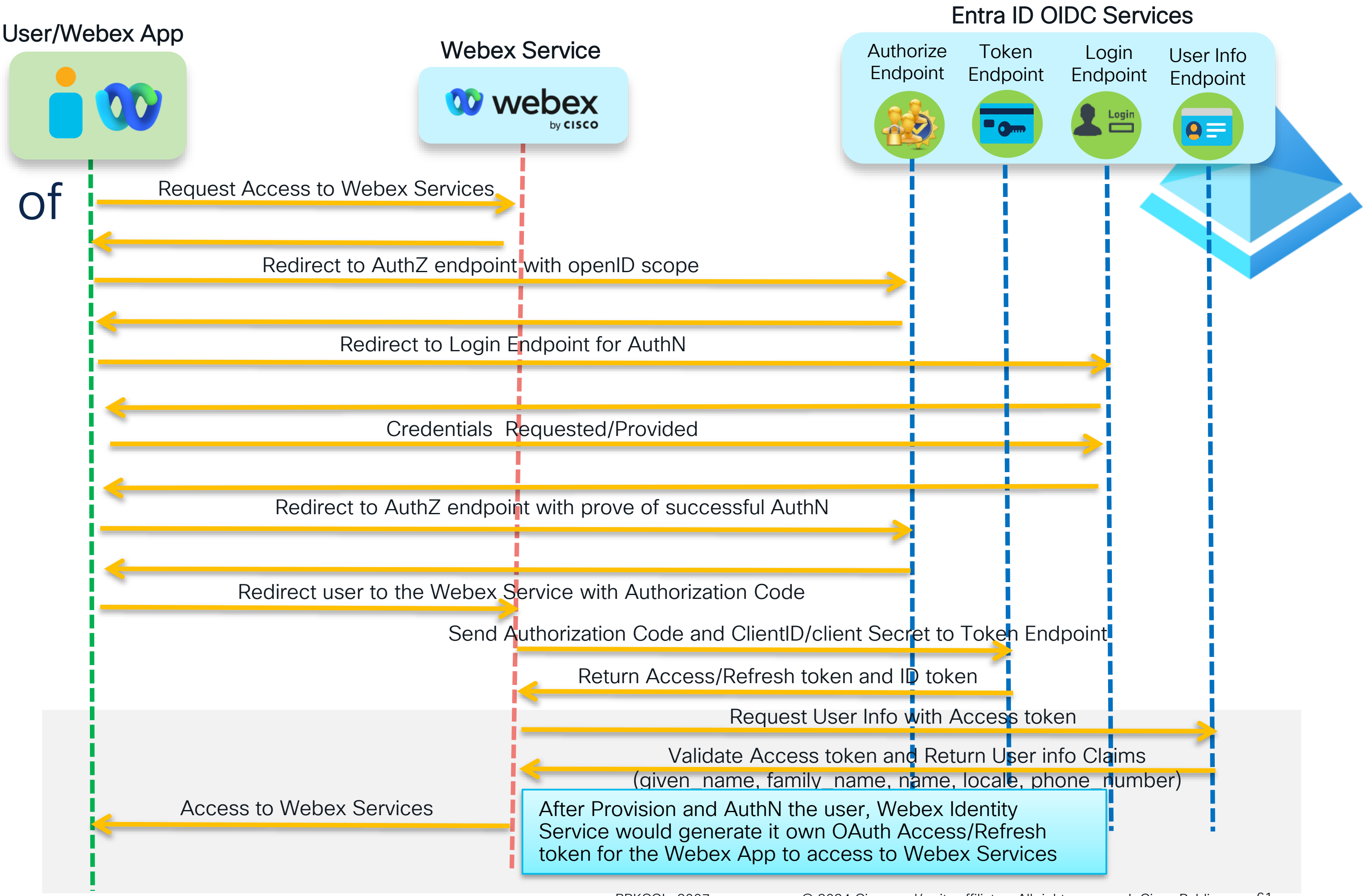
Standard Claims



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.
locale	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-CA. As a compatibility note, some implementations have used an

Example of OpenID Connect flow for Webex Entra ID

(AuthN & Provision)



User/Webex App

Webex Service

Entra ID OIDC Services

Authorize Endpoint

Token Endpoint

Login Endpoint

User Info Endpoint

Request Access to Webex Services

Redirect to AuthZ endpoint with openID scope

Redirect to Login Endpoint for AuthN

Credentials Requested/Provided

Redirect to AuthZ endpoint with prove of successful AuthN

Redirect user to the Webex Service with Authorization Code

Send Authorization Code and ClientID/client Secret to Token Endpoint

Return Access/Refresh token and ID token

Request User Info with Access token

Validate Access token and Return User info Claims (given_name, family_name, name, locale, phone_number)

Access to Webex Services

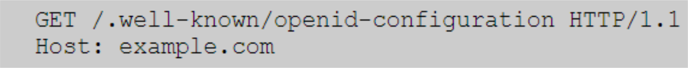
After Provision and AuthN the user, Webex Identity Service would generate it own OAuth Access/Refresh token for the Webex App to access to Webex Services

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.)

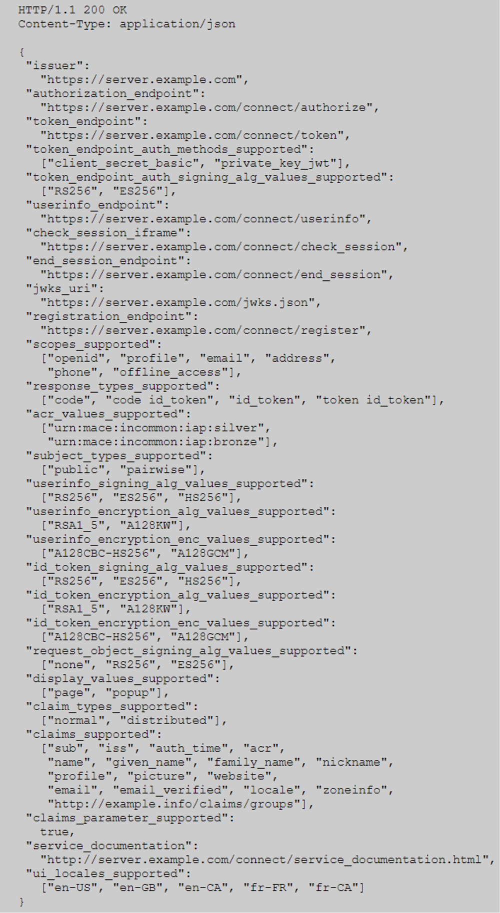
So the configuration can be request according to Discovery extensions https://openid.net/specs/openid-connect-discovery-1_0.html, in the end we just need to know the hostname for the service.

OpenID Provider Configuration Request



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

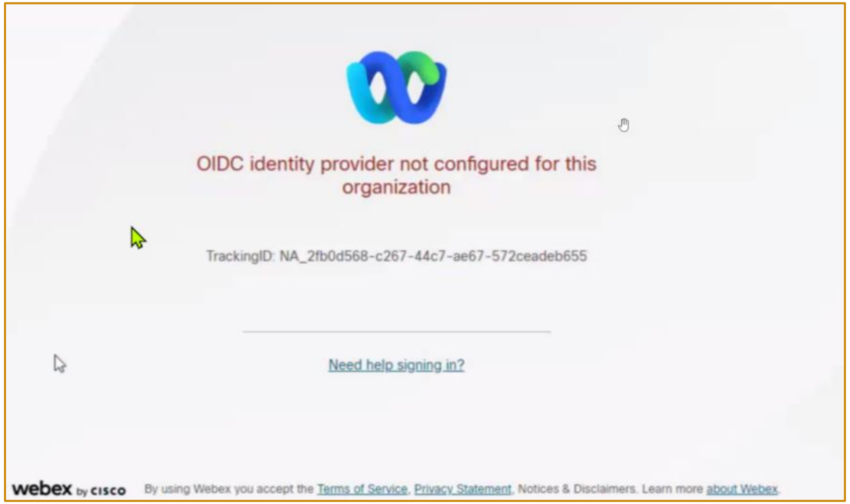
OpenID Provider Configuration Response



```
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"]
}
```

OIDC troubleshooting



OIDC identity provider not configured for this organization

TrackingID: NA_2fb0d568-c267-44c7-ae67-572ceadeb655

Need help signing in?

webex by cisco By using Webex you accept the Terms of Service, Privacy Statement, Notices & Disclaimers. Learn more about Webex.

invalid_entity_config OIDC identity provider configured incorrectly for this organization

fail_to_get_id_token Failed to get id token from identity provider

fail_to_parse_id_token Failed to parse id token from identity provider

no_email_in_id_token No email found in id token from identity provider

OriEmailNotPresent Original email is not present

linkingError Failed to link the account

Webex AuthN/AuthZ improvements

Token Management and which kind of OS to allow to connect to Webex

How long refresh token lasts.

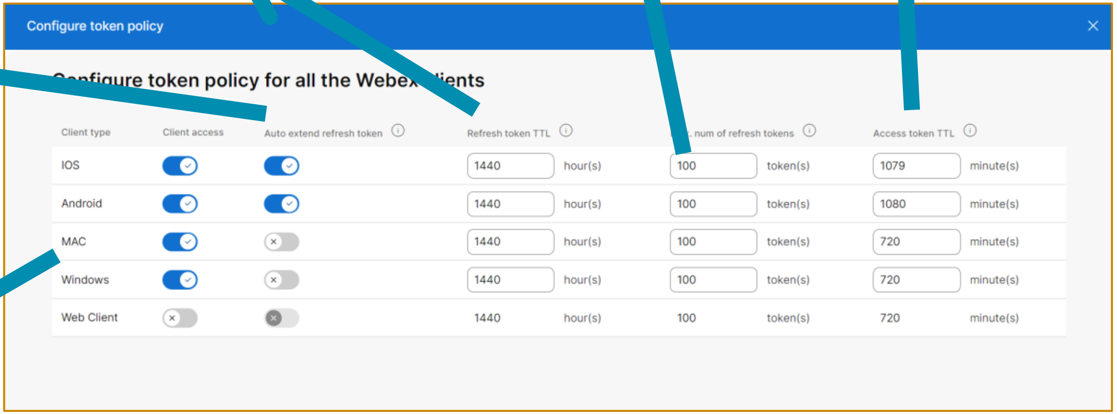
- If Auto Extend on – is the maximum duration that the client can be disconnected, before AuthN again, but might never need auth AuthN again.
- If Auto Extend Off – is when the Client need to AuthN again.

Maximum number of Clients that the User can have under their account

How long before getting another OAuth Access token

Would the refresh token be auto renew or not ?

Type of clients and which ones are enabled



Configure token policy

Configure token policy for all the Webex clients

Client type	Client access	Auto extend refresh token	Refresh token TTL		Max. num of refresh tokens		Access token TTL	
IOS	✓	✓	1440	hour(s)	100	token(s)	1079	minute(s)
Android	✓	✓	1440	hour(s)	100	token(s)	1080	minute(s)
MAC	✓	✕	1440	hour(s)	100	token(s)	720	minute(s)
Windows	✓	✕	1440	hour(s)	100	token(s)	720	minute(s)
Web Client	✕	✕	1440	hour(s)	100	token(s)	720	minute(s)

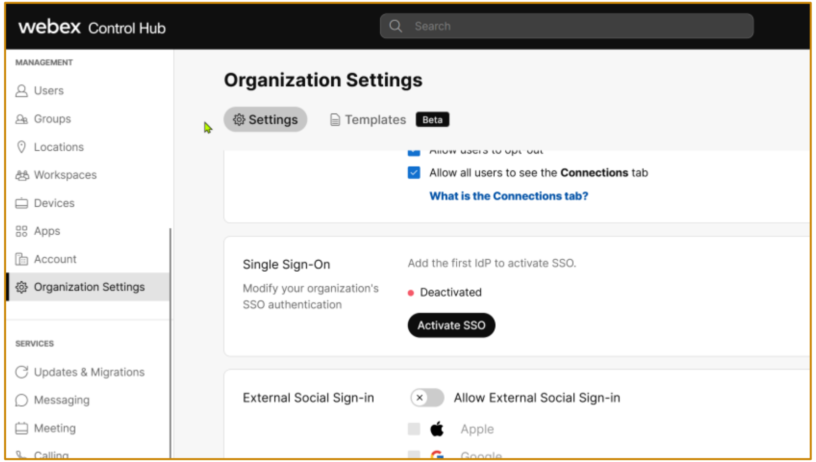
Authentication

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.



Organization Settings

☑ Allow users to opt-out

☑ Allow all users to see the **Connections** tab

What is the Connections tab?

Single Sign-On

Modify your organization's SSO authentication

Add the first IdP to activate SSO.

● Deactivated

Activate SSO

External Social Sign-in

☒ Allow External Social Sign-in

□ Apple

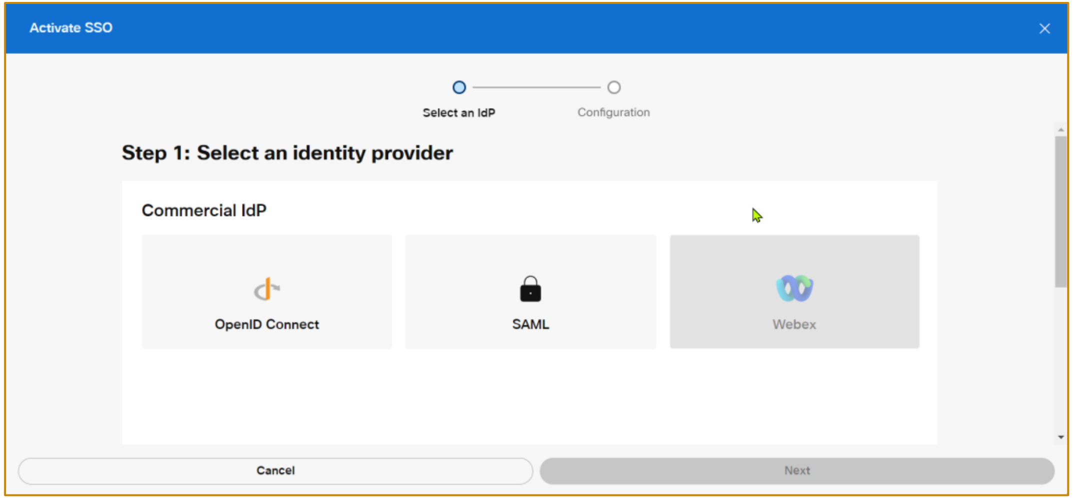
□ Google

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.



Activate SSO

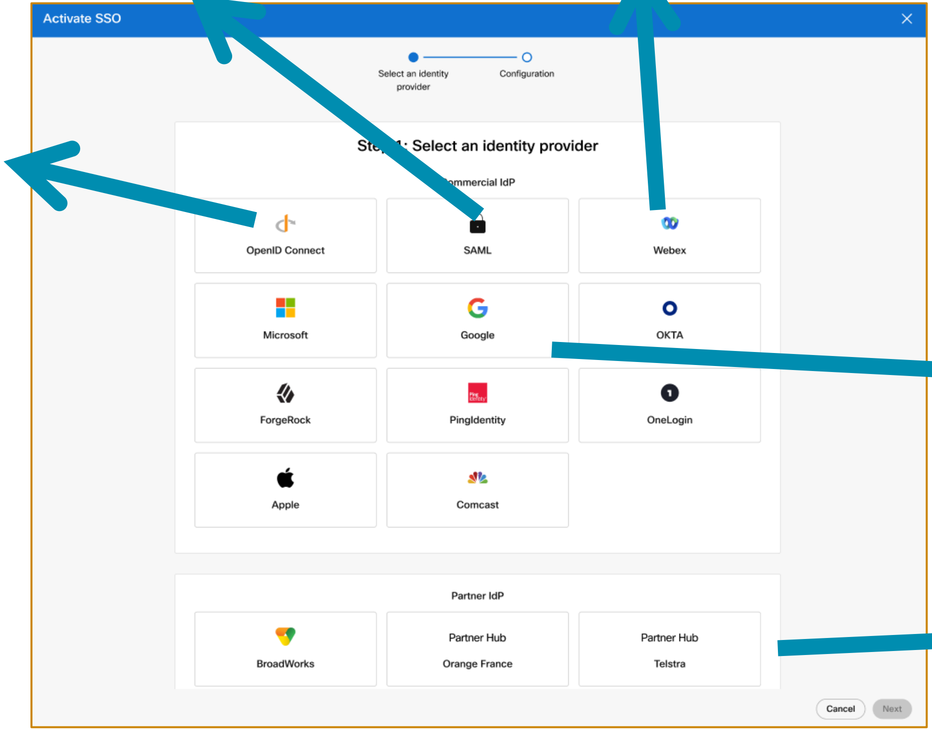
Step 1: Select an identity provider

Commercial IdP

Future

Single Sign-On

Other options in the future



Activate SSO

Select an identity provider — Configuration

Step 1: Select an identity provider

Commercial IdP

- OpenID Connect
- SAML
- Webex
- Microsoft
- Google
- OKTA
- ForgeRock
- PingIdentity
- OneLogin
- Apple
- Comcast

Partner IdP

- BroadWorks
- Partner Hub Orange France
- Partner Hub Telstra

Configure a SAML IdP

User Webex Credentials

Configure an OIDC IdP

Social Login or Cloud IdMs

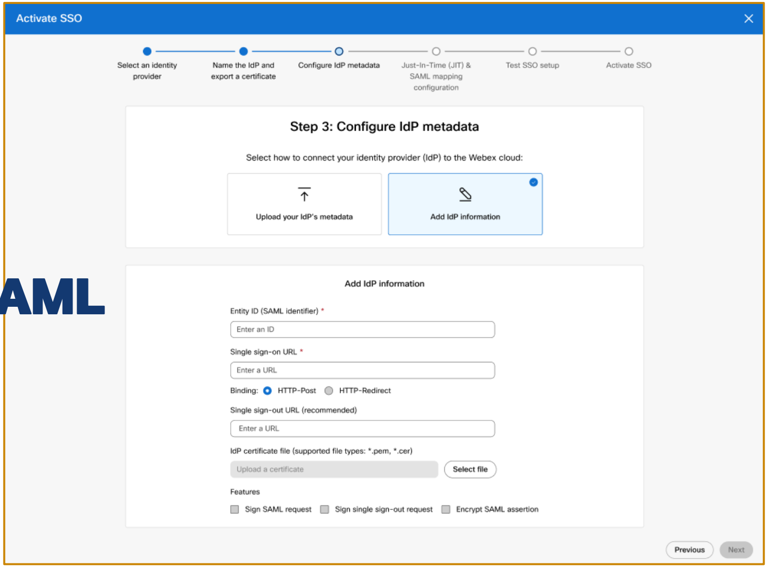
Partners IdMs

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


Activate SSO
Select an identity provider
Name the IdP and export a certificate
Configure IdP metadata
Just-In-Time (JIT) & SAML mapping configuration
Test SSO setup
Activate SSO
Upload your IdP's metadata
Add IdP information
Select file
Previous
Next

Step 3: Configure IdP metadata

Select how to connect your identity provider (IdP) to the Webex cloud:

Add IdP information

Entity ID (SAML identifier) *: Enter an ID

Single sign-on URL *: Enter a URL

Binding: ● HTTP-Post ○ HTTP-Redirect

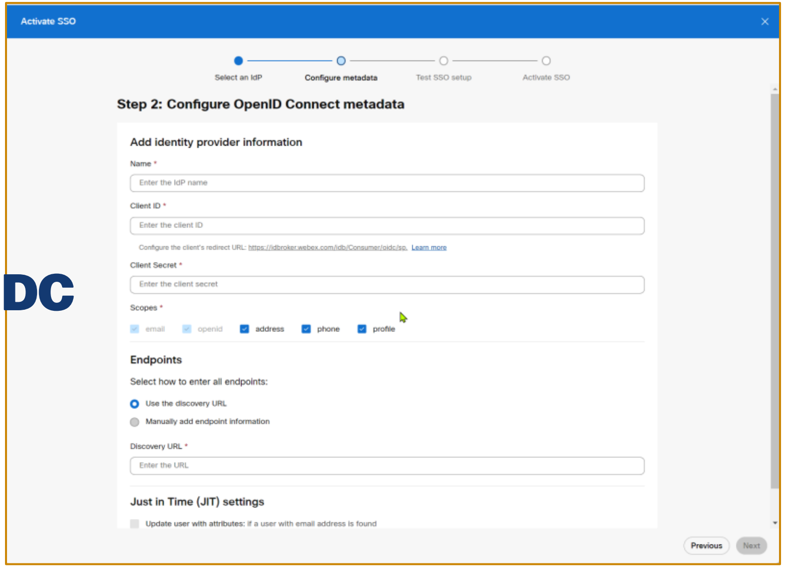
Single sign-out URL (recommended): Enter a URL

IdP certificate file (supported file types: *.pem, *.cer): Upload a certificate

Features

□ Sign SAML request □ Sign single sign-out request □ Encrypt SAML assertion

OIDC



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/idb/Consumer/oidc/sp. 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

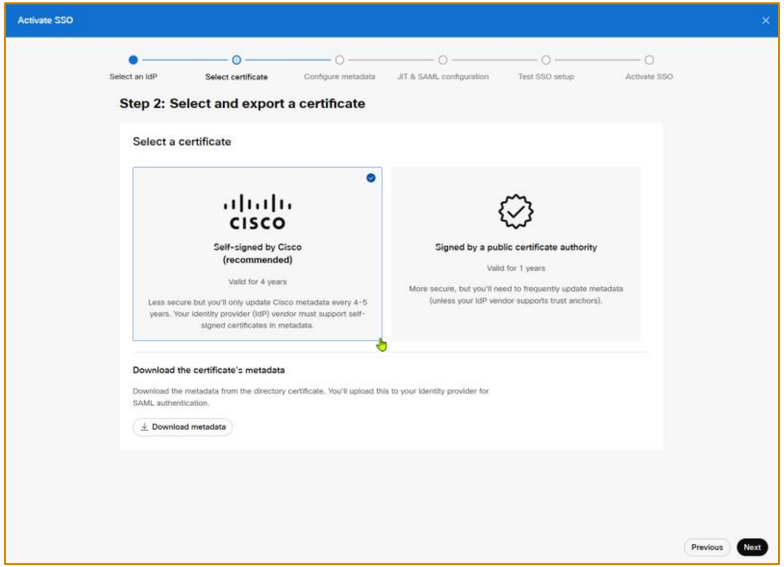
□ Update user with attributes: if a user with email address is found

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, …….)



Step 2: Select and export a certificate

Select a certificate

● 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.

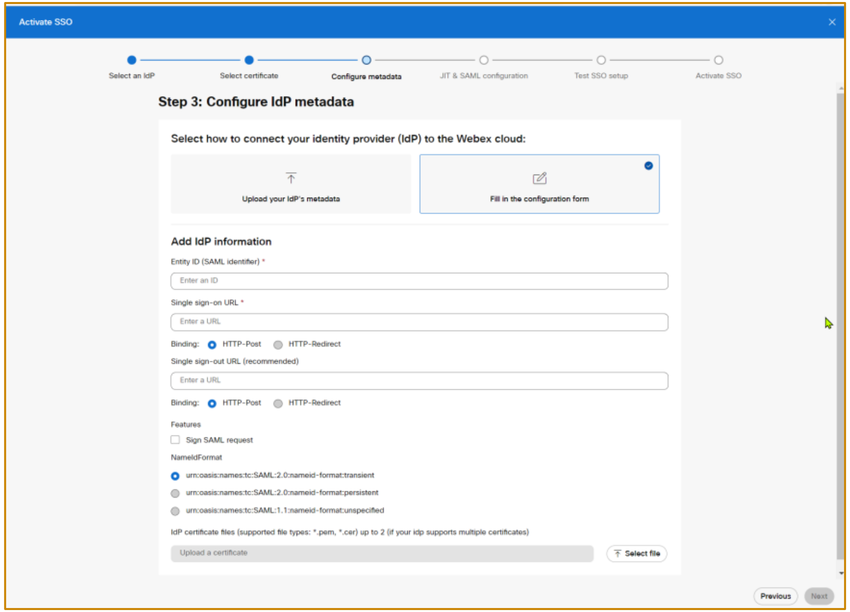
Signed by a public certificate authority

Valid for 1 years

More secure, but you'll need to frequently update metadata (unless your IdP vendor supports trust anchors).

Download the certificate's metadata

Download the metadata from the directory certificate. You'll upload this to your identity provider for SAML authentication.



Step 3: Configure IdP metadata

Select how to connect your identity provider (IdP) to the Webex cloud:

Upload your IdP's metadata

● Fill in the configuration form

Add IdP information

Entity ID (SAML identifier) *

Enter an ID

Single sign-on URL *

Enter a URL

Binding: ● HTTP-Post ○ HTTP-Redirect

Single sign-out URL (recommended)

Enter a URL

Binding: ● HTTP-Post ○ HTTP-Redirect

Features

☐ Sign SAML request

NameIdFormat

● urn:oasis:names:tc:SAML:2.0:nameid-format:transient

○ urn:oasis:names:tc:SAML:2.0:nameid-format:persistent

○ urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

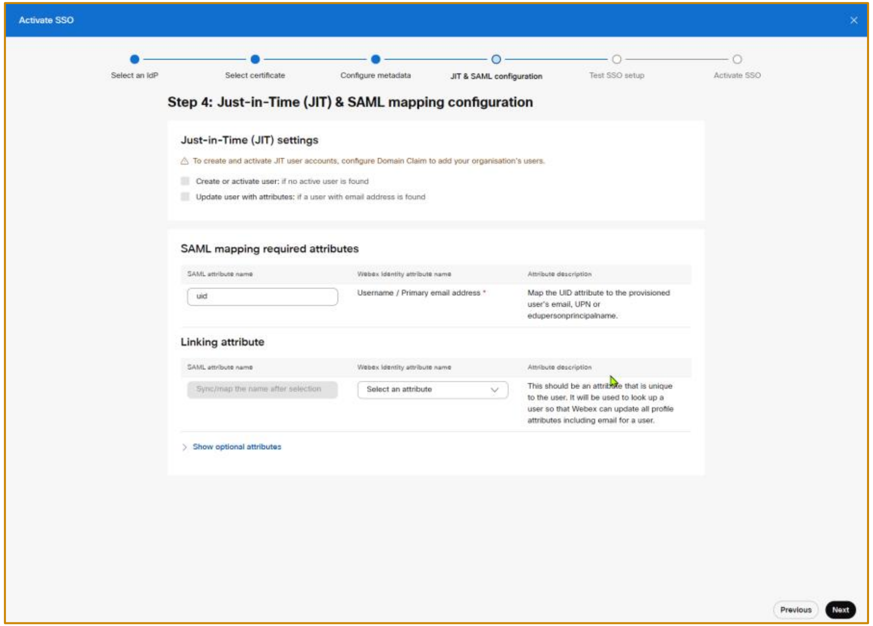
IdP certificate files (supported file types: *.pem, *.cer) up to 2 (if your idp supports multiple certificates)

Upload a certificate

Single Sign-On

SAML IdPs

Step 4 – SAML mappings and JIT



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

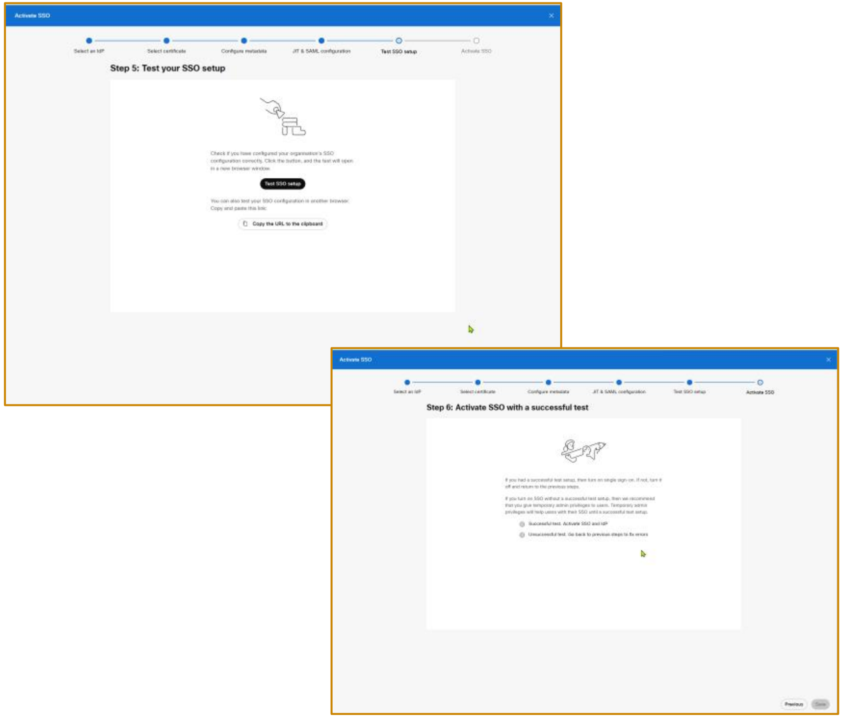
SAML attribute name	Webex Identity attribute name	Attribute description
uid	Username / Primary email address *	Map the UID attribute to the provisioned user's email, UPN or edupersonprincipalname.

Linking attribute

SAML attribute name	Webex Identity attribute name	Attribute description
Sync/map the name after selection	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.

Step 5 – Test Configuration

Step 6 – Enable or Disable SSO



Step 5: Test your SSO setup

Check if you have configured your organisation's SSO configuration correctly. Click the button, and the test will open in a new browser window.

You can also test your SSO configuration in another browser. Copy and paste this link:

Step 6: Activate SSO with a successful test

If you had a successful test setup, then turn on single sign-on. If not, turn it off and return to the previous steps.

If you turn on SSO without a successful test setup, then we recommend that you give temporary admin privileges to users. Temporary admin privileges will help users with their SSO until a successful test setup.

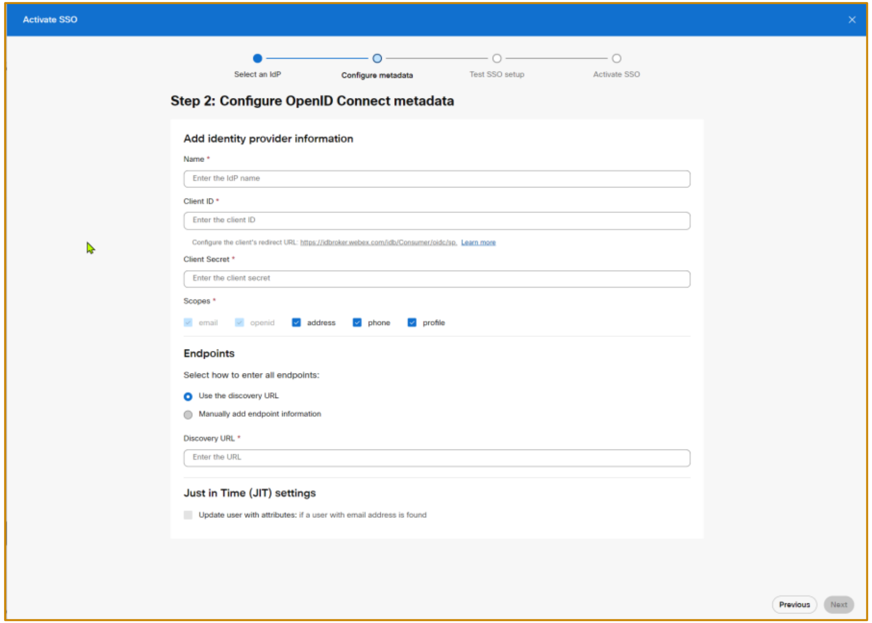
○ Successful test. Activate SSO and IdP

○ 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



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/idb/Consumer/oidc/sp. 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

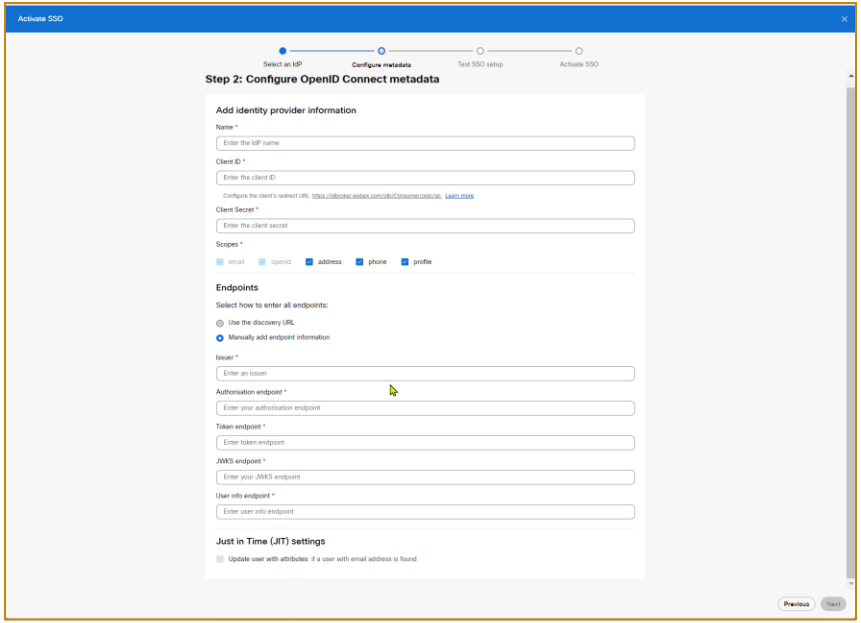
○ Manually add endpoint information

Discovery URL *

Enter the URL

Just in Time (JIT) settings

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



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/idb/Consumer/oidc/sp. 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

Authorisation 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

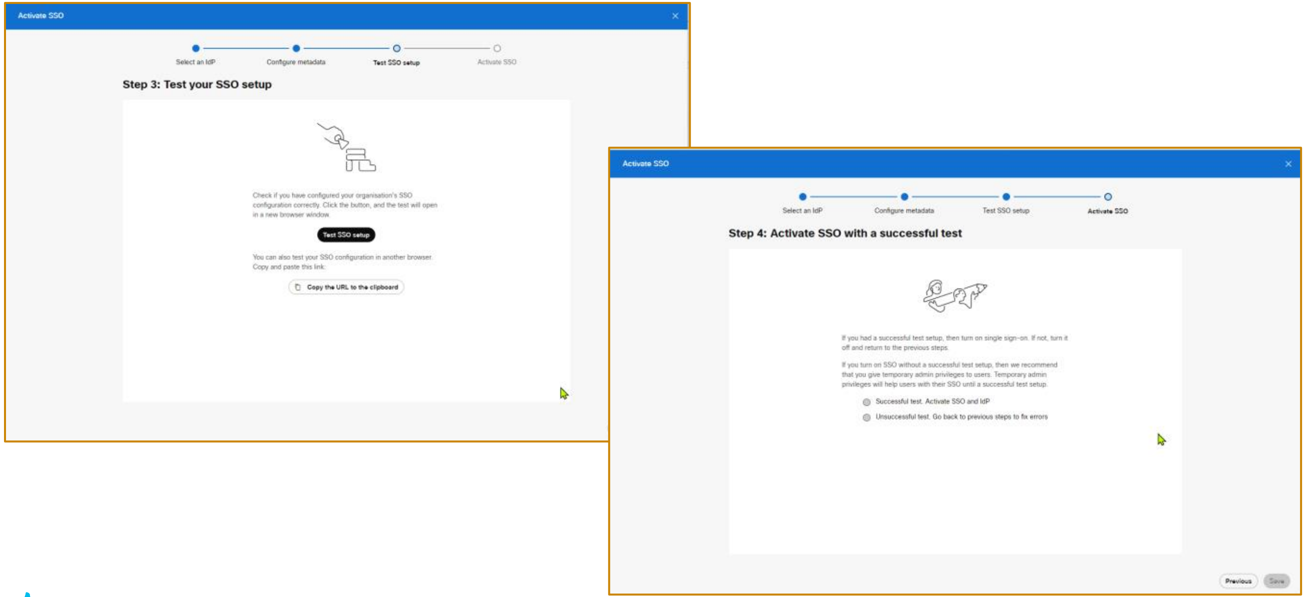
□ Update user with attributes: if a user with email address is found

Single Sign-On

OIDC IdPs

Step 3 – Test SSO

Step 4 – Activate or deactivate SSO



Activate SSO

Step 3: Test your SSO setup

Check if you have configured your organisation's SSO configuration correctly. Click the button, and the test will open in a new browser window.

You can also test your SSO configuration in another browser. Copy and paste this link:

Activate SSO

Step 4: Activate SSO with a successful test

If you had a successful test setup, then turn on single sign-on. If not, turn it off and return to the previous steps.

If you turn on SSO without a successful test setup, then we recommend that you give temporary admin privileges to users. Temporary admin privileges will help users with their SSO until a successful test setup.

○ Successful test. Activate SSO and IdP

○ Unsuccessful test. Go back to previous steps to fix errors

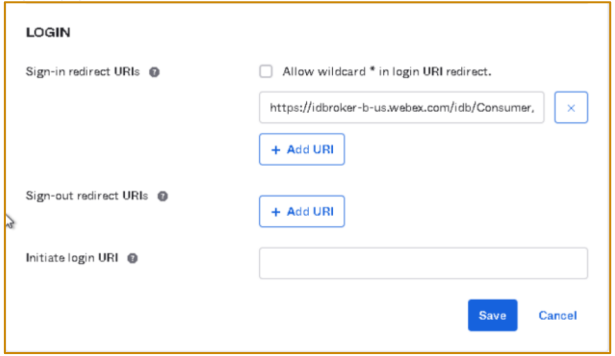
Cloud OIDC IdP

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,

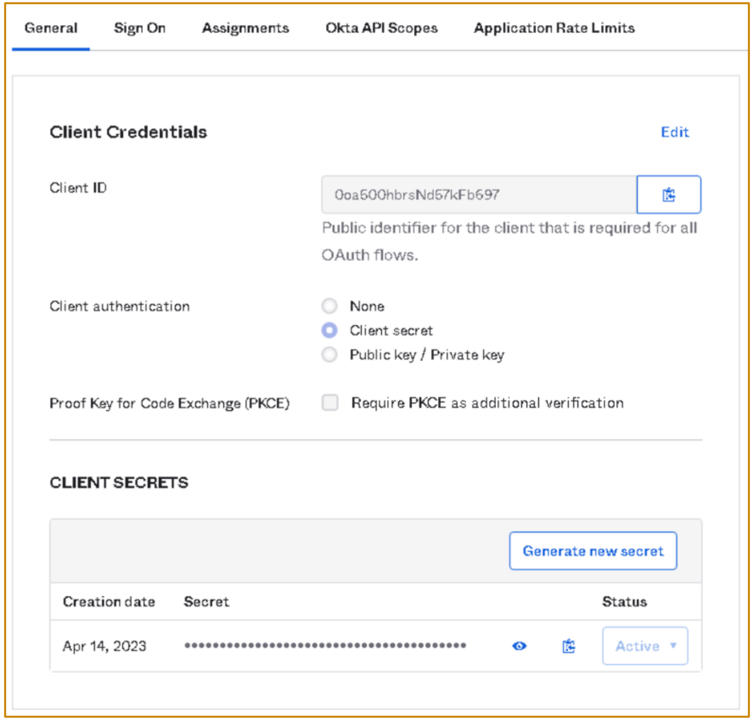
Sign-out redirect URIs

Initiate login URI

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



Client Credentials

Client ID: 0oa500hbrsNd57kFb697

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

Creation date	Secret	Status
Apr 14, 2023	••	Active

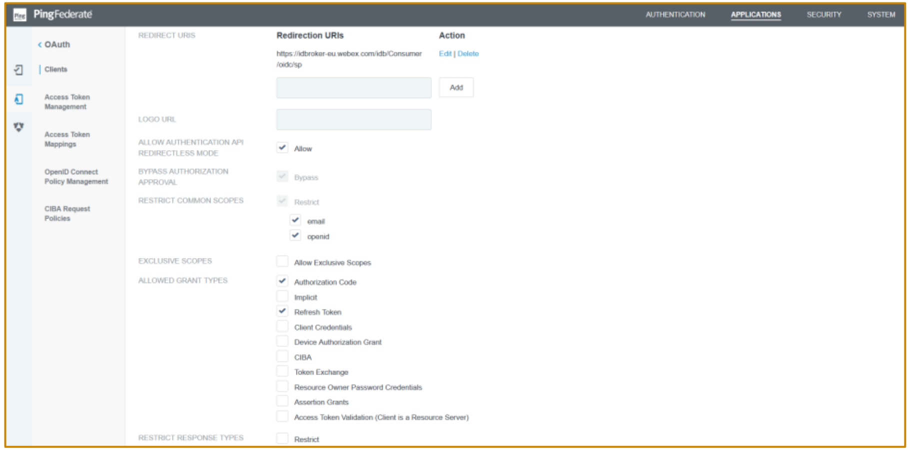
On-Premise OIDC IdP

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.



REDIRECT URIS

Redirection URIs	Action
https://idbroker-eu.webex.com/idb/Consumer/oidc/sp	Edit | Delete

LOGO URL

ALLOW AUTHENTICATION API REDIRECTLESS MODE ☑ Allow

BYPASS AUTHORIZATION APPROVAL ☑ Bypass

RESTRICT COMMON SCOPES ☑ Restrict
- ☑ email
- ☑ openid

EXCLUSIVE SCOPES □ Allow Exclusive Scopes

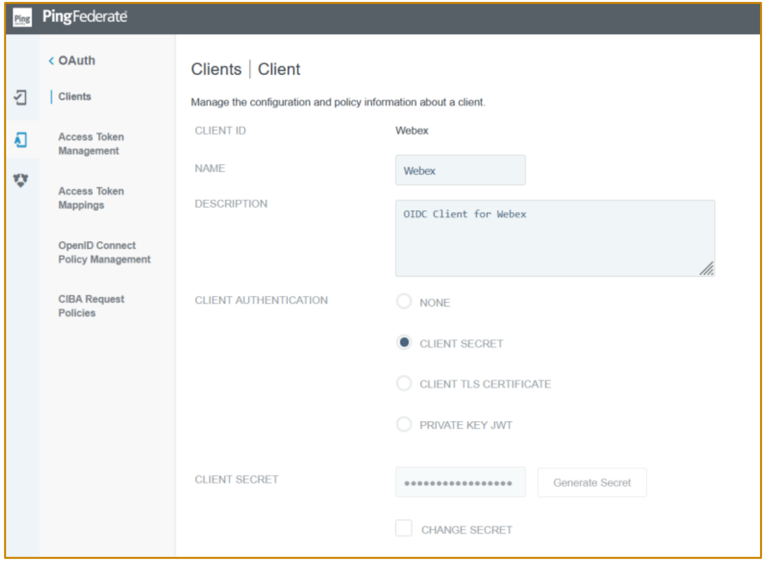
ALLOWED GRANT TYPES
- ☑ Authorization Code
- □ Implicit
- ☑ Refresh Token
- □ Client Credentials
- □ Device Authorization Grant
- □ CIBA
- □ Token Exchange
- □ Resource Owner Password Credentials
- □ Assertion Grants
- □ Access Token Validation (Client is a Resource Server)

RESTRICT RESPONSE TYPES □ Restrict

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



Clients | Client

Manage the configuration and policy information about a client.

CLIENT ID Webex

NAME Webex

DESCRIPTION OIDC Client for Webex

CLIENT AUTHENTICATION
- ○ NONE
- ● CLIENT SECRET
- ○ CLIENT TLS CERTIFICATE
- ○ PRIVATE KEY JWT

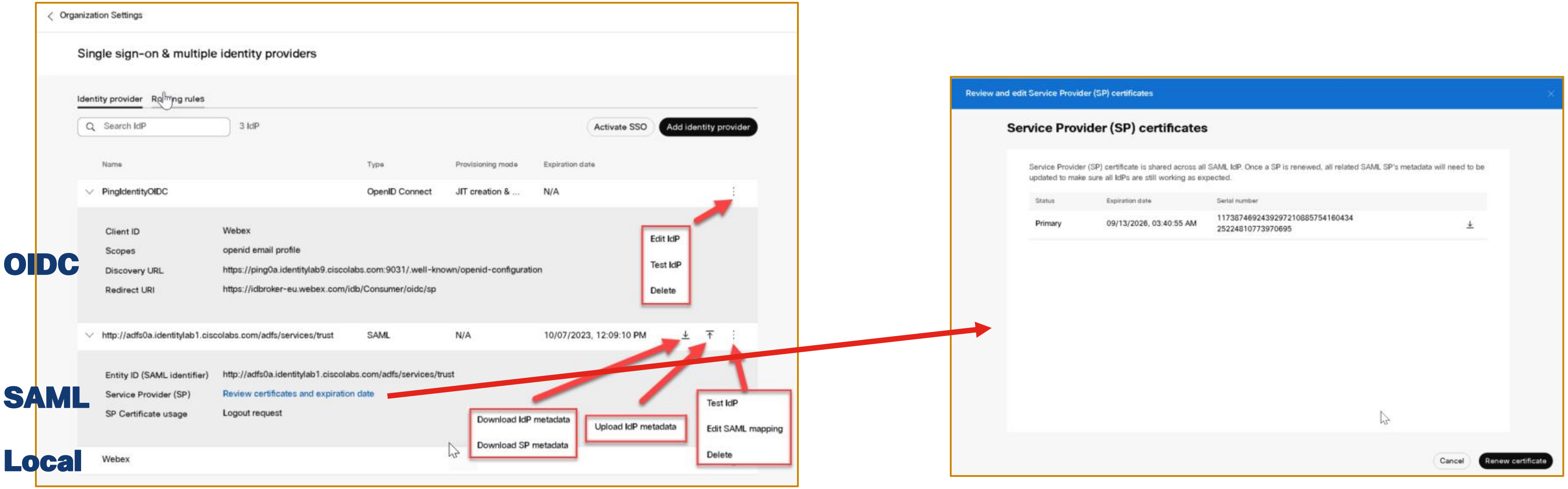
CLIENT SECRET ••••••••••••••••

□ CHANGE SECRET

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



‹ Organization Settings

Single sign-on & multiple identity providers

Identity provider | Routing rules

Search IdP | 3 IdP | Activate SSO | Add identity provider

Name	Type	Provisioning mode	Expiration date
PingIdentityOIDC	OpenID Connect	JIT creation & ...	N/A

OIDC

Client ID	Webex
Scopes	openid email profile
Discovery URL	https://ping0a.identitylab9.ciscolabs.com:9031/.well-known/openid-configuration
Redirect URI	https://idbroker-eu.webex.com/idb/Consumer/oidc/sp

Name	Type	Provisioning mode	Expiration date
http://adfs0a.identitylab1.ciscolabs.com/adfs/services/trust	SAML	N/A	10/07/2023, 12:09:10 PM

SAML

Entity ID (SAML identifier)	http://adfs0a.identitylab1.ciscolabs.com/adfs/services/trust
Service Provider (SP)	Review certificates and expiration date
SP Certificate usage	Logout request

Local Webex

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	117387469243929721088575416043425224810773970695

Multiple IdP Single Sign-On

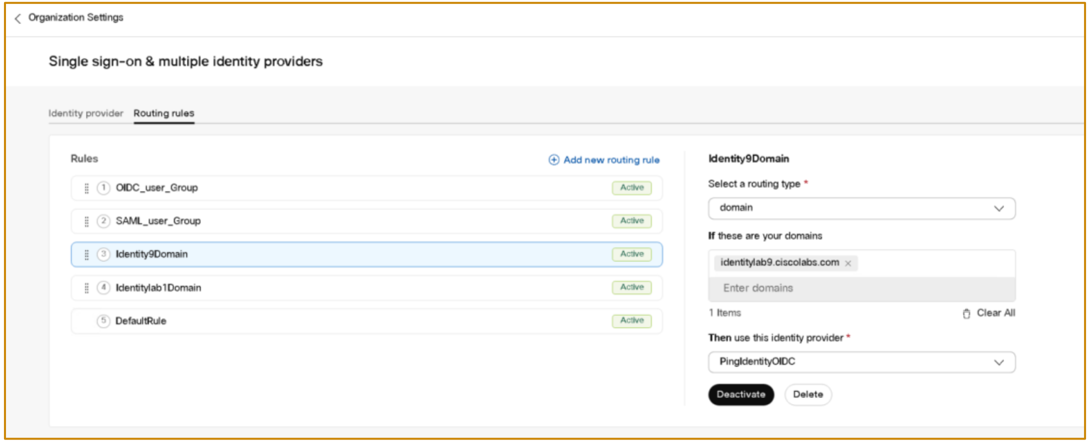
How to associate each user to a different IdP

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.



< Organization Settings

Single sign-on & multiple identity providers

Identity provider | Routing rules

Rules — ⊕ Add new routing rule

1. OIDC_user_Group — Active
2. SAML_user_Group — Active
3. Identity9Domain — Active
4. Identitylab1Domain — Active
5. DefaultRule — Active

Identity9Domain

Select a routing type *: domain

If these are your domains: identitylab9.ciscolabs.com ×

Enter domains

1 Items — Clear All

Then use this identity provider *: PingIdentityOIDC

Deactivate | Delete

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

Let’s go