TURN IT UP

cisco Live!

#CiscoLive

The bridge to possible

Collaboration Identity Provision

Paulo Jorge Correia
@paucorre

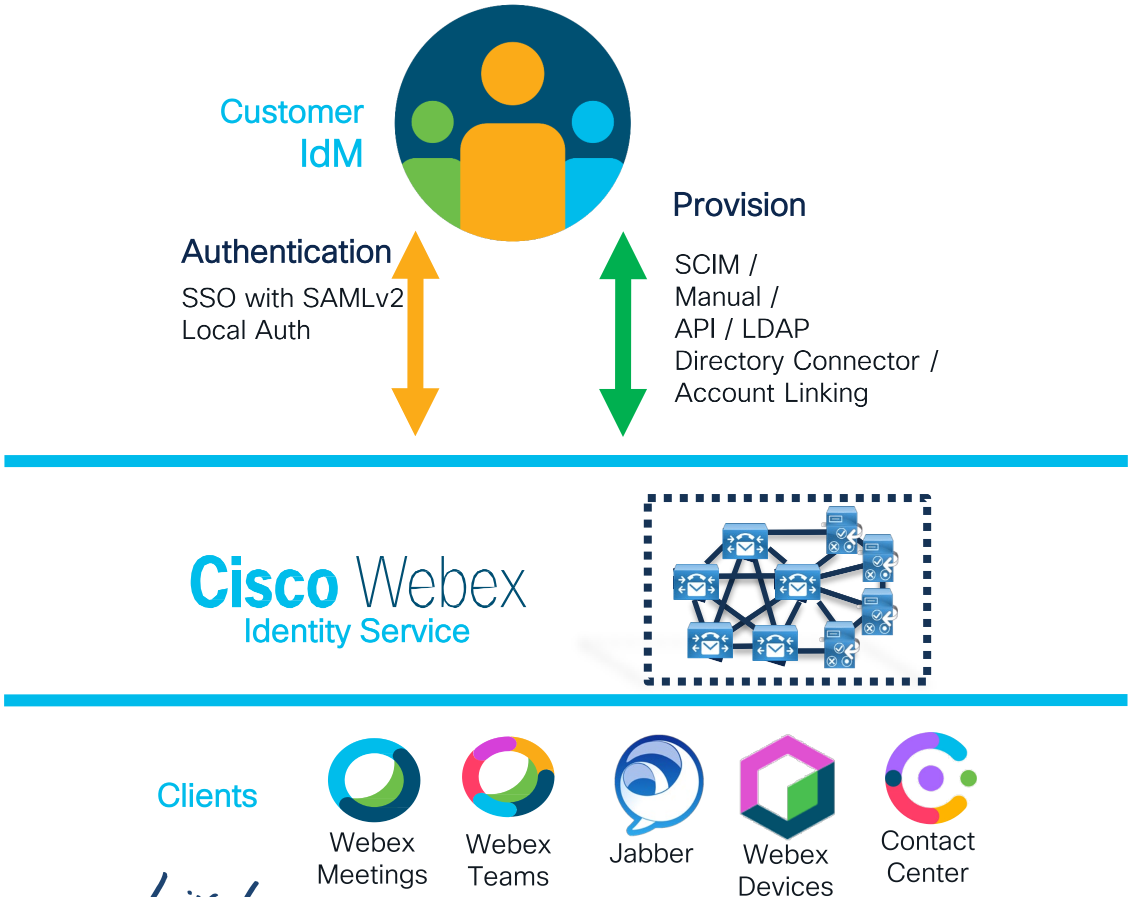
BRKCOL-2045

Agenda

- Cisco Collaboration Applications
- On-premise provision of users
- SCIM for Webex Identity
- Directory Connector
- Considerations on the Webex user provision
- Provision features and licenses using Groups

Cisco Collaboration Applications

Cisco Collaboration Applications



Customer IdM

Authentication

SSO with SAMLv2
Local Auth

Provision

SCIM /
Manual /
API / LDAP
Directory Connector /
Account Linking

Cisco Webex Identity Service

Clients

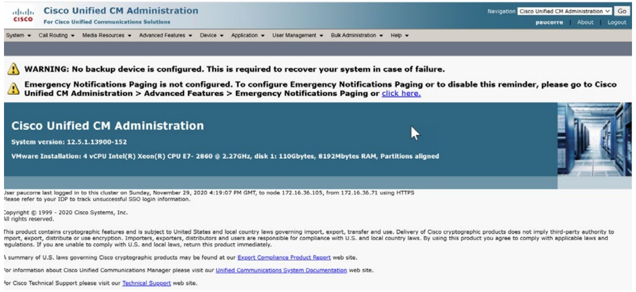
Webex Meetings

Webex Teams

Jabber

Webex Devices

Contact Center



WARNING: No backup device is configured. This is required to recover your system in case of failure.

Emergency Notifications Paging is not configured. To configure Emergency Notifications Paging or to disable this reminder, please go to Cisco Unified CM Administration > Advanced Features > Emergency Notifications Paging or click here.

Cisco Unified CM Administration

System version: 12.5.1.13900-152

VMware Installation: 4 vCPU Intel(R) Xeon(R) CPU E7- 2860 @ 2.27GHz, disk 1: 110Gbytes, 8192Mbytes RAM, Partitions aligned

Jser paucorre last logged in to this cluster on Sunday, November 29, 2020 4:19:07 PM GMT, to node 172.16.36.105, from 172.16.36.71 using HTTPS
Please refer to your IDP to track unsuccessful SSO login information.

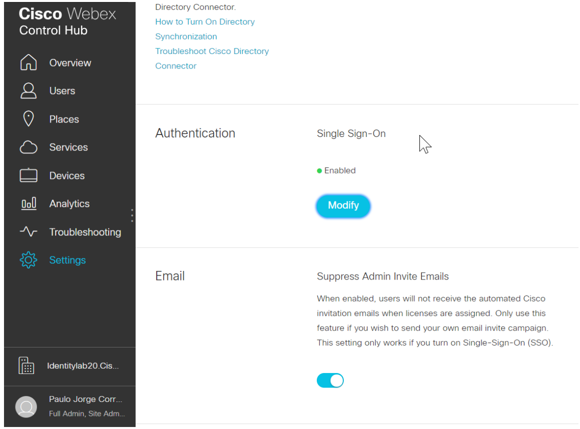
Copyright © 1999 - 2020 Cisco Systems, Inc.
All rights reserved.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to mport, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and egulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at our Export Compliance Product Report web site.

For information about Cisco Unified Communications Manager please visit our Unified Communications System Documentation web site.

For Cisco Technical Support please visit our Technical Support web site.



Directory Connector.
How to Turn On Directory Synchronization
Troubleshoot Cisco Directory Connector

Authentication

Single Sign-On

● Enabled

Modify

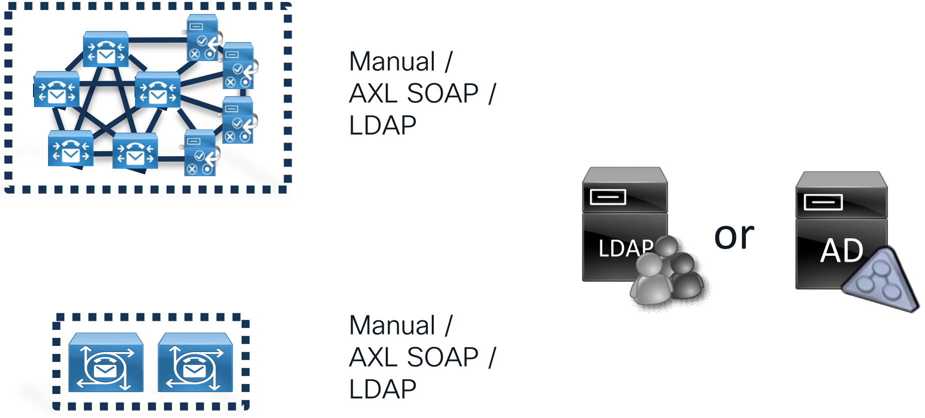
Email

Suppress Admin Invite Emails

When enabled, users will not receive the automated Cisco invitation emails when licenses are assigned. Only use this feature if you wish to send your own email invite campaign. This setting only works if you turn on Single-Sign-On (SSO).

On-premise provision of users

Users provision for CUCM and Connection



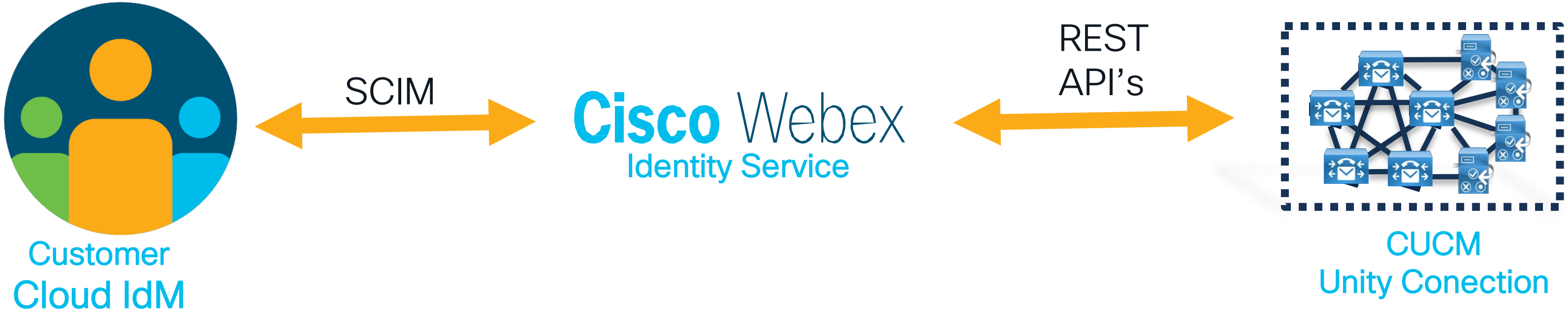
Manual /
AXL SOAP /
LDAP

Manual /
AXL SOAP /
LDAP

or

- This model serve us for many years, unfortunately today we have new challenges with IDM in the cloud (IDaaS)
- LDAP was never design as a protocol to be used on the internet.
- There aren’t any Firewall vendors that inspect LDAP at an application level

Our direction

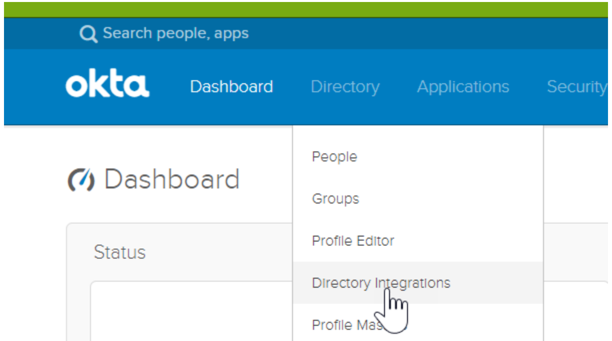


Cisco plan to use the identity engine in Webex to bring all user information from Customer Cloud IdM using standard protocols like SCIM and provide that user database to Cisco On-premise components.

This will allow us to have a common user database for cloud and on-premise products

What can we have today with the IDaaS ?

OKTA



Search people, apps

okta Dashboard Directory Applications Security

Dashboard

Status

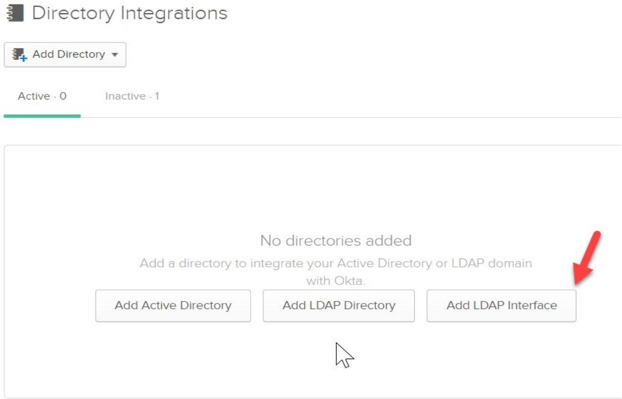
People

Groups

Profile Editor

Directory Integrations

Profile Mas



Directory Integrations

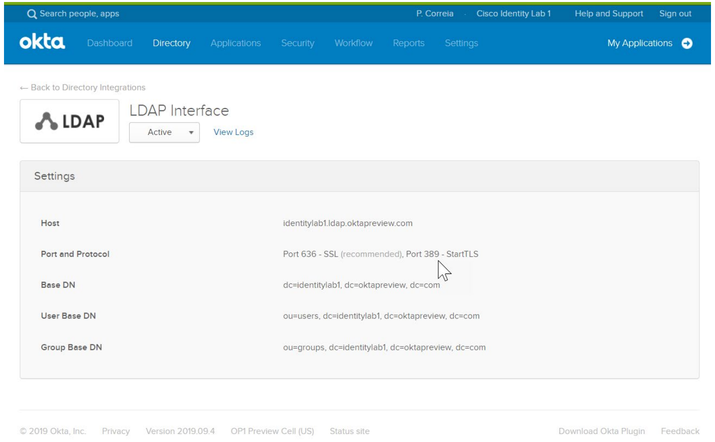
Add Directory ▾

Active · 0 Inactive · 1

No directories added

Add a directory to integrate your Active Directory or LDAP domain with Okta.

Add Active Directory | Add LDAP Directory | Add LDAP Interface



Search people, apps P. Correia · Cisco Identity Lab 1 Help and Support Sign out

okta Dashboard Directory Applications Security Workflow Reports Settings My Applications

← Back to Directory Integrations

LDAP Interface

Active ▾ View Logs

Settings

Host	identitylab1.ldap.oktapreview.com
Port and Protocol	Port 636 - SSL (recommended), Port 389 - StartTLS
Base DN	dc=identitylab1, dc=oktapreview, dc=com
User Base DN	ou=users, dc=identitylab1, dc=oktapreview, dc=com
Group Base DN	ou=groups, dc=identitylab1, dc=oktapreview, dc=com

© 2019 Okta, Inc. Privacy Version 2019.09.4 OP1 Preview Cell (US) Status site Download Okta Plugin Feedback

In OKTA we can create an LDAPS interface that can be reach by our on-premise Collaboration products

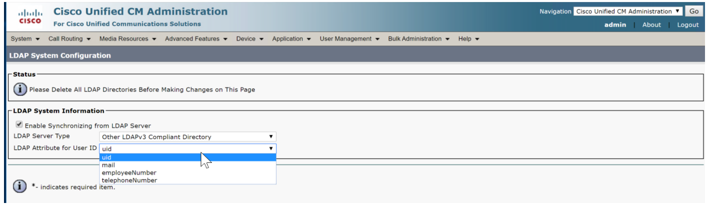
There will be a LDAPS synchronization from inside the customer network to the OKTA cloud, connection will be encrypted using TLS or SSL

What can we have today with the IDaaS ?

OKTA

In CUCM or Unity Connection we will need to upload the certificate used by the OKTA Services as tomcat trust.

You should configure the LDAP Server Type as Other LDAPv3 Compliant Directory, and the attribute for the user will be most likely uid, but you can choose also mail, employeeNumber or telephoneNumber.



LDAP System Configuration

Status

Please Delete All LDAP Directories Before Making Changes on This Page

LDAP System Information

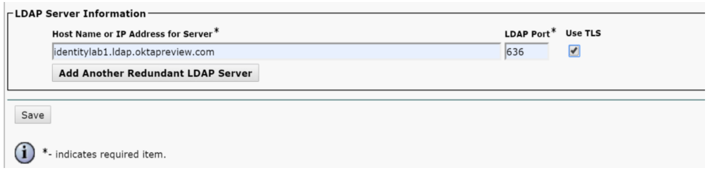
☑ Enable Synchronizing from LDAP Server

LDAP Server Type: Other LDAPv3 Compliant Directory

LDAP Attribute for User ID: uid

- uid
- mail
- employeeNumber
- telephoneNumber

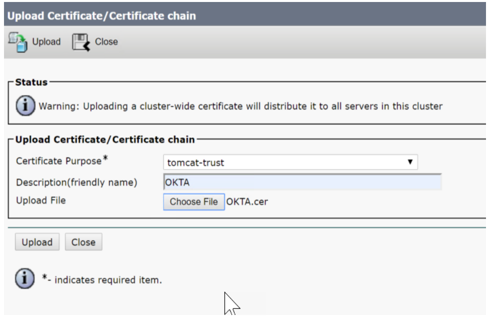
*- indicates required item.



LDAP Server Information

Host Name or IP Address for Server*	LDAP Port*	Use TLS
identitylab1.ldap.oktapreview.com	636	☑

*- indicates required item.



Upload Certificate/Certificate chain

Status

Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

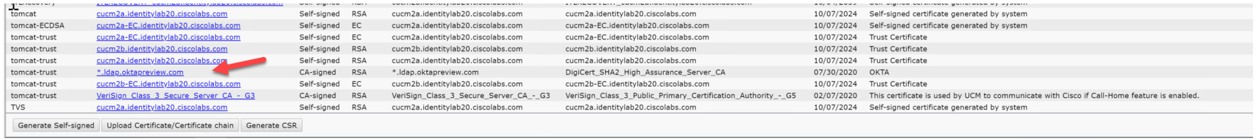
Upload Certificate/Certificate chain

Certificate Purpose*: tomcat-trust

Description(friendly name): OKTA

Upload File: Choose File OKTA.cer

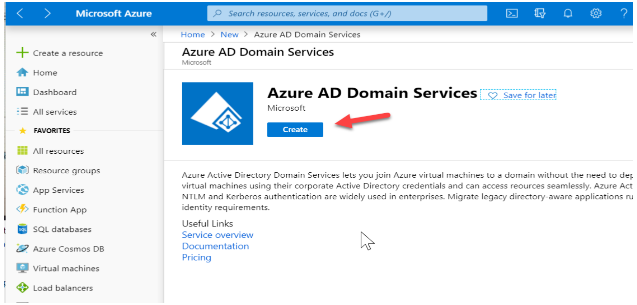
*- indicates required item.



tomcat	cucm2a.identitylab20.ciscolabs.com	Self-signed	RSA	cucm2a.identitylab20.ciscolabs.com	cucm2a.identitylab20.ciscolabs.com	10/07/2024	Self-signed certificate generated by system
tomcat-ECDSA	cucm2a-EC.identitylab20.ciscolabs.com	Self-signed	EC	cucm2a.identitylab20.ciscolabs.com	cucm2a-EC.identitylab20.ciscolabs.com	10/07/2024	Self-signed certificate generated by system
tomcat-trust	cucm2a-EC.identitylab20.ciscolabs.com	Self-signed	EC	cucm2a.identitylab20.ciscolabs.com	cucm2a-EC.identitylab20.ciscolabs.com	10/07/2024	Trust Certificate
tomcat-trust	cucm2b.identitylab20.ciscolabs.com	Self-signed	RSA	cucm2b.identitylab20.ciscolabs.com	cucm2b.identitylab20.ciscolabs.com	10/07/2024	Trust Certificate
tomcat-trust	cucm2a.identitylab20.ciscolabs.com	Self-signed	RSA	cucm2a.identitylab20.ciscolabs.com	cucm2a.identitylab20.ciscolabs.com	10/07/2024	Trust Certificate
tomcat-trust	*.ldap.oktapreview.com	CA-signed	RSA	*.ldap.oktapreview.com	DigiCert_SHA2_High_Assurance_Server_CA	07/30/2020	OKTA
tomcat-trust	cucm2b-EC.identitylab20.ciscolabs.com	Self-signed	EC	cucm2b.identitylab20.ciscolabs.com	cucm2b-EC.identitylab20.ciscolabs.com	10/07/2024	Trust Certificate
tomcat-trust	VeriSign_Class_3_Secure_Server_CA_-_G3	CA-signed	RSA	VeriSign_Class_3_Secure_Server_CA_-_G3	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5	02/07/2020	This certificate is used by UCM to communicate with Cisco if Call-Home feature is enabled.
TVS	cucm2a.identitylab20.ciscolabs.com	Self-signed	RSA	cucm2a.identitylab20.ciscolabs.com	cucm2a.identitylab20.ciscolabs.com	10/07/2024	Self-signed certificate generated by system

What can we have today with the IDaaS ?

Azure AD



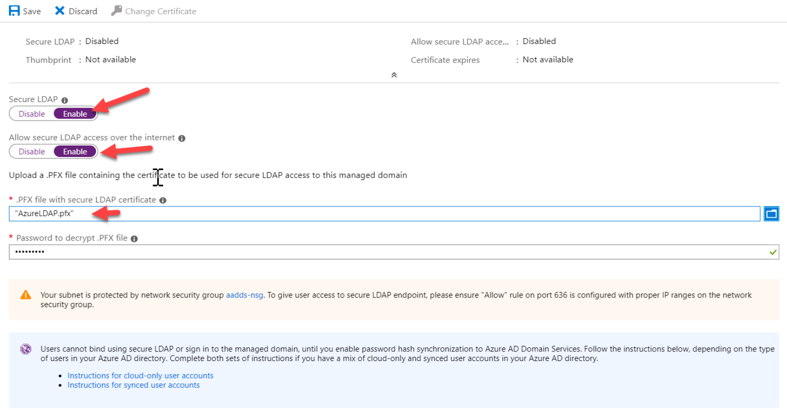
Azure AD Domain Services
Microsoft

Azure AD Domain Services
Microsoft

Azure Active Directory Domain Services lets you join Azure virtual machines to a domain without the need to dep
virtual machines using their corporate Active Directory credentials and can access reources seamlessly. Azure Act
NTLM and Kerberos authentication are widely used in enterprises. Migrate legacy directory-aware applications ru
identity requirements.

Useful Links
Service overview
Documentation
Pricing

With Azure AD IDaaS we can deploy a AD Domain controller in the cloud, it will be a VM running in the Azure Cloud, the VM is called Azure AD Domain Services.



Secure LDAP : Disabled
Thumbprint : Not available
Allow secure LDAP acce... : Disabled
Certificate expires : Not available

Secure LDAP
○ Disable ● Enable

Allow secure LDAP access over the internet
○ Disable ● Enable

Upload a .PFX file containing the certificate to be used for secure LDAP access to this managed domain

* .PFX file with secure LDAP certificate
"AzureLDAP.pfx"

* Password to decrypt .PFX file
•••••••••

Your subnet is protected by network security group aadds-nsg. To give user access to secure LDAP endpoint, please ensure "Allow" rule on port 636 is configured with proper IP ranges on the network security group.

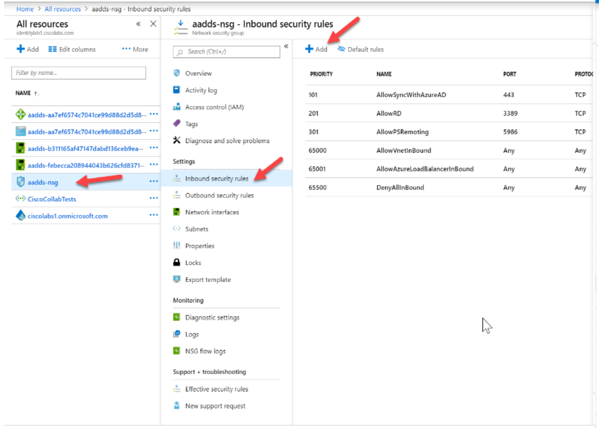
Users cannot bind using secure LDAP or sign in to the managed domain, until you enable password hash synchronization to Azure AD Domain Services. Follow the instructions below, depending on the type of users in your Azure AD directory. Complete both sets of instructions if you have a mix of cloud-only and synced user accounts in your Azure AD directory.

- Instructions for cloud-only user accounts
- Instructions for synced user accounts

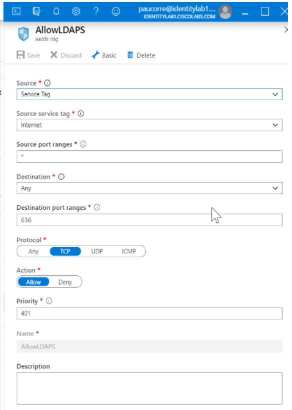
You should/must enable the LDAPS interface and for that you will need to provide a certificate (a PFX with private/public key)

What can we have today with the IDaaS ?

Azure AD



PRIORITY	NAME	PORT	PROTOC
101	AllowSyncWithAzureAD	443	TCP
201	AllowRD	3389	TCP
301	AllowPSRemoting	5986	TCP
65000	AllowVnetInBound	Any	Any
65001	AllowAzureLoadBalancerInBound	Any	Any
65500	DenyAllInBound	Any	Any



Source * Service Tag

Source service tag * Internet

Source port ranges * *

Destination * Any

Destination port ranges * 636

Protocol * Any [✓ TCP] UDP ICMP

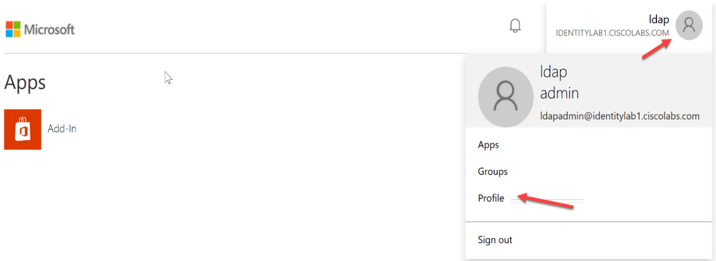
Action * [✓ Allow] Deny

Priority * 401

Name * AllowLDAPS

Description

You will need to change the VM firewall rules, so that it allows LDAPS connection from outside Azure cloud, it should allow connections from the public IP address of the customer network.

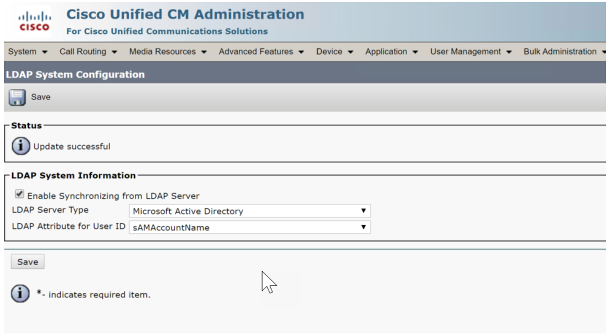

Microsoft
Apps
Add-In
ldap
IDENTITYLAB1.CISCOLABS.COM
ldap
admin
ldapadmin@identitylab1.ciscolabs.com
Apps
Groups
Profile
Sign out

You need to have a user for the LDAP authentication, and the password isn't synchronizing yet between Azure AD and the Azure DS, so you will need to change the password.

In fact any user associate with Azure DS will need to reset their password, for the sync between Azure AD and Azure DS to happen.

What can we have today with the IDaaS ?

Azure AD



LDAP System Configuration

Status

Update successful

LDAP System Information

☑ Enable Synchronizing from LDAP Server

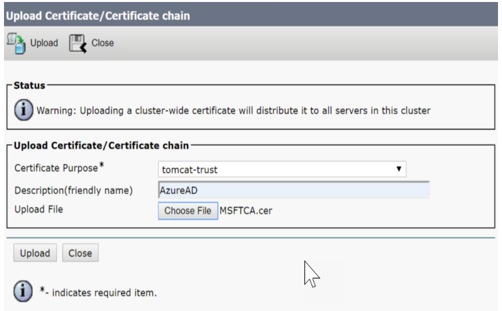
LDAP Server Type: Microsoft Active Directory

LDAP Attribute for User ID: sAMAccountName

*- indicates required item.

In CUCM or Unity Connection we will need to upload the certificate used by the Azure DS Services as tomcat trust.

You should configure the LDAP Server Type as Microsoft Active Directory, and the attribute for the user will be most likely sAMAccountName, but you can choose also mail, employeeNumber or telephoneNumber.



Upload Certificate/Certificate chain

Status

Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

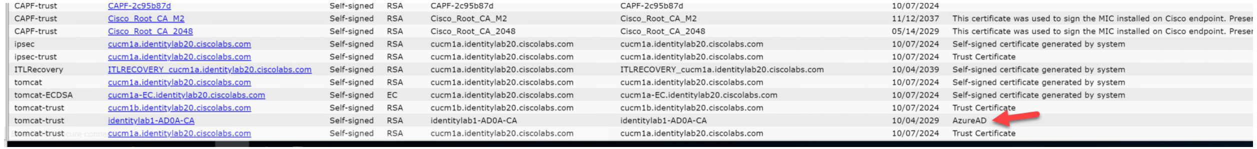
Upload Certificate/Certificate chain

Certificate Purpose*: tomcat-trust

Description(friendly name): AzureAD

Upload File: MSFTCA.cer

*- indicates required item.



CAPF-trust	CAPF-2c95b87d	Self-signed	RSA	CAPF-2c95b87d	CAPF-2c95b87d	10/07/2024	
CAPF-trust	Cisco_Root_CA_M2	Self-signed	RSA	Cisco_Root_CA_M2	Cisco_Root_CA_M2	11/12/2037	This certificate was used to sign the MIC installed on Cisco endpoint. Preser
CAPF-trust	Cisco_Root_CA_2048	Self-signed	RSA	Cisco_Root_CA_2048	Cisco_Root_CA_2048	05/14/2029	This certificate was used to sign the MIC installed on Cisco endpoint. Preser
ipsec	cucm1a.identitylab20.ciscolabs.com	Self-signed	RSA	cucm1a.identitylab20.ciscolabs.com	cucm1a.identitylab20.ciscolabs.com	10/07/2024	Self-signed certificate generated by system
ipsec-trust	cucm1a.identitylab20.ciscolabs.com	Self-signed	RSA	cucm1a.identitylab20.ciscolabs.com	cucm1a.identitylab20.ciscolabs.com	10/07/2024	Trust Certificate
ITLRecovery	ITLRECOVERY_cucm1a.identitylab20.ciscolabs.com	Self-signed	RSA	cucm1a.identitylab20.ciscolabs.com	ITLRECOVERY_cucm1a.identitylab20.ciscolabs.com	10/04/2039	Self-signed certificate generated by system
tomcat	cucm1a.identitylab20.ciscolabs.com	Self-signed	RSA	cucm1a.identitylab20.ciscolabs.com	cucm1a.identitylab20.ciscolabs.com	10/07/2024	Self-signed certificate generated by system
tomcat-ECDSA	cucm1a-EC.identitylab20.ciscolabs.com	Self-signed	EC	cucm1a.identitylab20.ciscolabs.com	cucm1a-EC.identitylab20.ciscolabs.com	10/07/2024	Self-signed certificate generated by system
tomcat-trust	cucm1b.identitylab20.ciscolabs.com	Self-signed	RSA	cucm1b.identitylab20.ciscolabs.com	cucm1b.identitylab20.ciscolabs.com	10/07/2024	Trust Certificate
tomcat-trust	identitylab1-AD0A-CA	Self-signed	RSA	identitylab1-AD0A-CA	identitylab1-AD0A-CA	10/04/2029	AzureAD
tomcat-trust	cucm1a.identitylab20.ciscolabs.com	Self-signed	RSA	cucm1a.identitylab20.ciscolabs.com	cucm1a.identitylab20.ciscolabs.com	10/07/2024	Trust Certificate

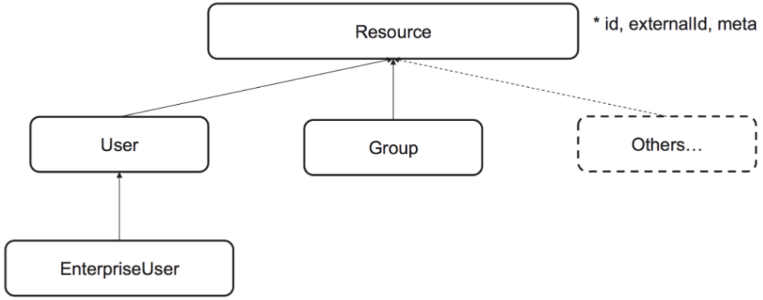
SCIM for Webex Identity

What is SCIM ?

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

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

Normally we will see a Model like :

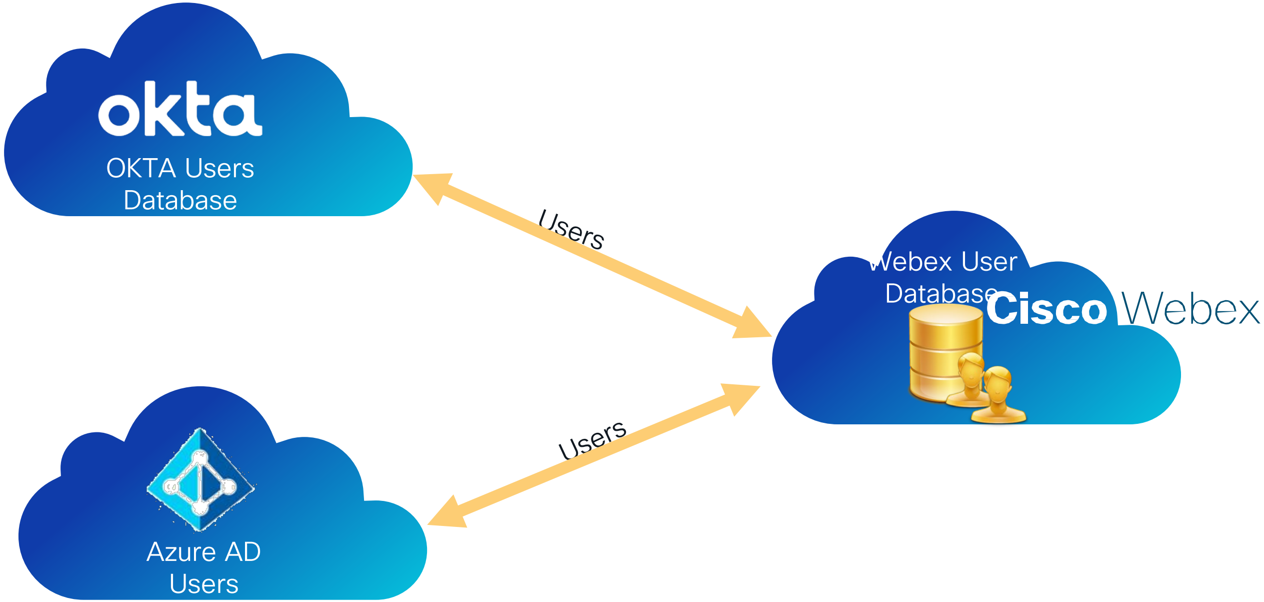


http://www.simplecloud.info/

Example of a user object passed by the IdM to Cisco Webex as we support it today

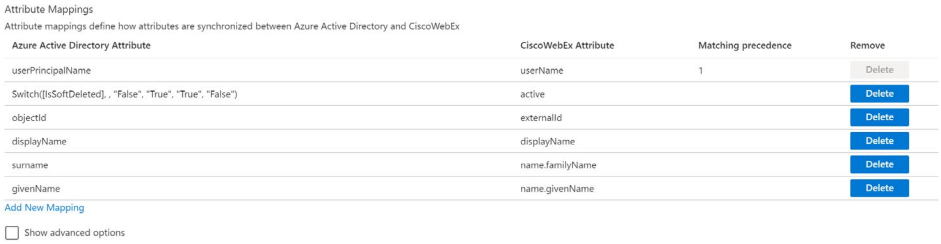
```
{
  "schemas":["urn:scim:schemas:core:1.0"],
  “externalId”:”a54028dd-f9ab-4c02-9526-a27bc158b04d”,
  "userName": “paucorre@cisco.com",
  "name":{
    "givenName":“Paulo Jorge",
    "familyName":“Correia"
  },
  "displayName": “Paulo Jorge Correia",
  "phoneNumbers":[
   {
     "value": "+351253123456",
     "type": "work"
   },
   {
     "value": "+351911234567",
     "type": "mobile"
   }
   {
     "value": "+351253234567",
     "type": “fax"
   }
  ],
  "addresses": [
   {
     "type": "work",
     "streetAddress": “Av. 31 Janeiro, 111",
     "locality": “Braga",
     "region": “Minho",
     "postalCode": “4710-452",
     "country": “PT"
   }
  ],
  "title": “Technical Solutions Architect",
  “active": True,
}
```

SCIM integrations



Azure AD SCIM integration

By default, attributes defined in the application



Attribute Mappings

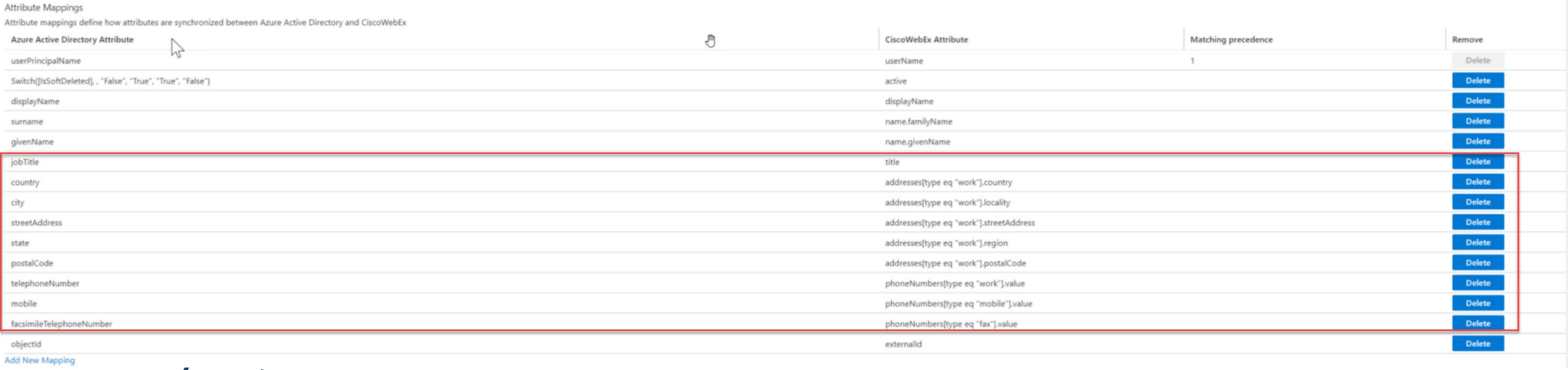
Attribute mappings define how attributes are synchronized between Azure Active Directory and CiscoWebEx

Azure Active Directory Attribute	CiscoWebEx Attribute	Matching precedence	Remove
userPrincipalName	userName	1	Delete
Switch([IsSoftDeleted], , "False", "True", "True", "False")	active		Delete
objectId	externalId		Delete
displayName	displayName		Delete
surname	name.familyName		Delete
givenName	name.givenName		Delete

Add New Mapping

□ Show advanced options

But you can expand the attributes to be pass to Webex



Attribute Mappings

Attribute mappings define how attributes are synchronized between Azure Active Directory and CiscoWebEx

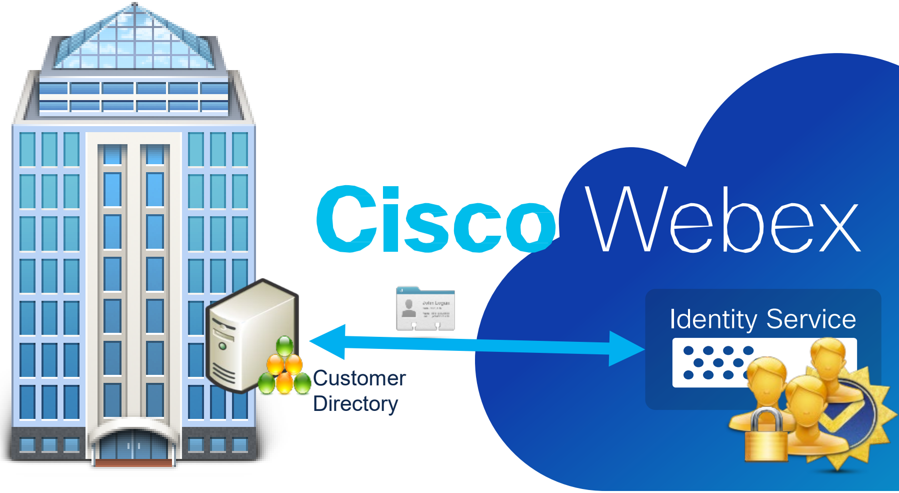
Azure Active Directory Attribute	CiscoWebEx Attribute	Matching precedence	Remove
userPrincipalName	userName	1	Delete
Switch([IsSoftDeleted], , "False", "True", "True", "False")	active		Delete
displayName	displayName		Delete
surname	name.familyName		Delete
givenName	name.givenName		Delete
jobTitle	title		Delete
country	addresses[type eq "work"].country		Delete
city	addresses[type eq "work"].locality		Delete
streetAddress	addresses[type eq "work"].streetAddress		Delete
state	addresses[type eq "work"].region		Delete
postalCode	addresses[type eq "work"].postalCode		Delete
telephoneNumber	phoneNumbers[type eq "work"].value		Delete
mobile	phoneNumbers[type eq "mobile"].value		Delete
facsimileTelephoneNumber	phoneNumbers[type eq "fax"].value		Delete
objectId	externalId		Delete

Add New Mapping

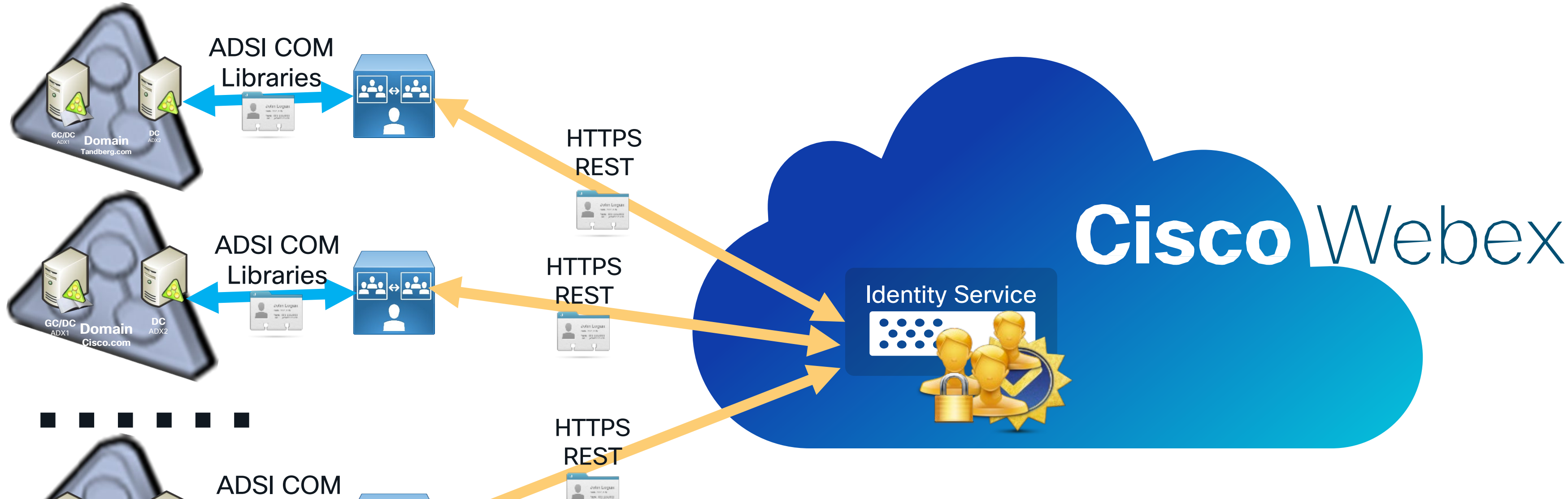
Directory Connector

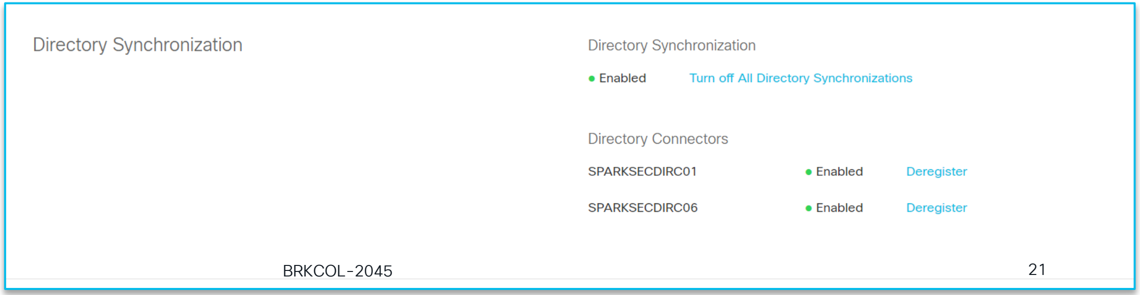
Directory Connector

- 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)



Directory Connector





Directory Synchronization

Directory Synchronization

● Enabled Turn off All Directory Synchronizations

Directory Connectors

SPARKSECDIRC01	● Enabled	Deregister
SPARKSECDIRC06	● Enabled	Deregister

Considerations on the Webex user provision

Webex User Account Management Options

Options	Description
Manual or CSV updates through Org Admin	Admin can use Webex Control Hub to manage user accounts
User Invite	User Self-Enroll or invite another user to use Webex Teams
Directory Connector	Automatic method for creating, updating and deactivating user accounts and groups. Account information will be synchronized from Customer Active Directory Domain Controllers
SCIM protocol	Automatic method for creating, updating and deactivating user accounts from IdM's that are SCIM enabled (Azure AD and OKTA supported today)
People API	Create, Delete, Update and List users by using API's
Account Linking	Customer with Webex meetings under Site admin, users will be provision automatically in Webex Control Hub

🟦 Enterprise grade provision mechanisms

Which provision mechanisms can be used together?

	Manual and/or CSV	Account Linking	People API's	SCIM	Directory Connector
Manual and/or CSV	✅	✅	✅	✅	❌
Account Linking	✅	✅	✅	☑	☑
People API's	✅	✅	✅	✅	❌
SCIM	✅	☑	✅	✅	❌
Directory Connector	❌	☑	❌	❌	✅

Comparing Directory Connector to SCIM provision

	SCIM	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	✗	✓

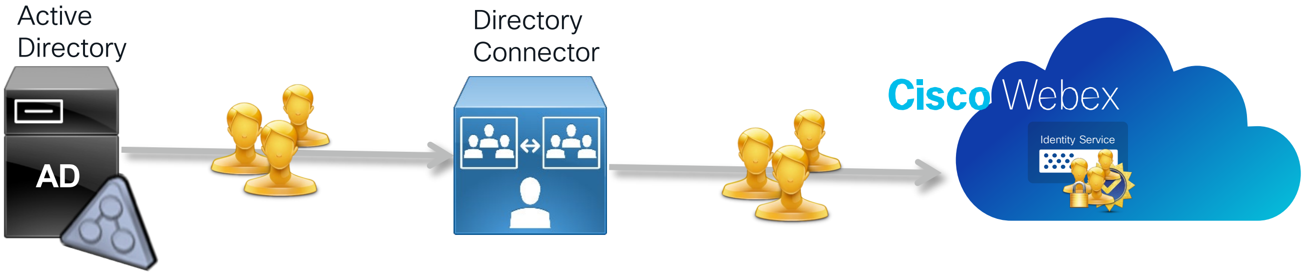
Provision features and licenses using Groups

Why do we need AD Groups?

- **Reuse/Simplification** by grouping users. On **onboarding users, Licenses** should be easily assigned based on AD Groups. This way administrators can create user “personas” and assign proper licensing to those groups of users
- Improve usage of auto license templates

  https://help.webex.com/en-us/ndl247o/Set-Up-Your-Automatic-License-Assignment-Template

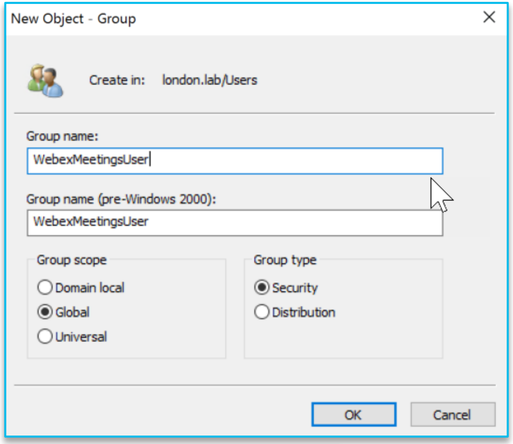
- **Opens the door** to other features that would allow for better customization for “personas” profiles



How to configure and best practice

In AD created Global Security groups that describe the license features that you want to provide to that group of users.

Make sure that you give to the **group a meaningful name,** so that you can filter the groups that should be imported to Webex (E.g. Webex.....)



New Object - Group

Create in: london.lab/Users

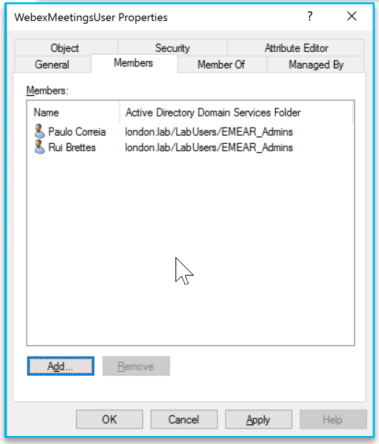
Group name:
WebexMeetingsUser

Group name (pre-Windows 2000):
WebexMeetingsUser

Group scope
○ Domain local
● Global
○ Universal

Group type
● Security
○ Distribution

Assign the users that will be entitled to that kind of licenses to that group.



WebexMeetingsUser Properties

Members:

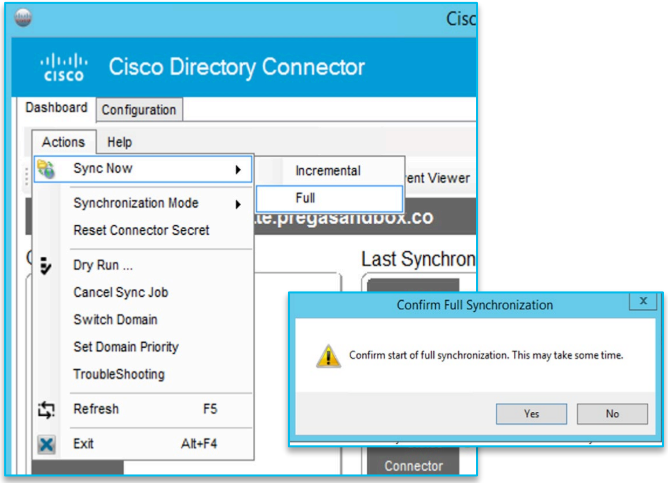
Name	Active Directory Domain Services Folder
Paulo Correia	london.lab/LabUsers/EMEAR_Admins
Rui Brettes	london.lab/LabUsers/EMEAR_Admins

How to configure and best practice (part2)

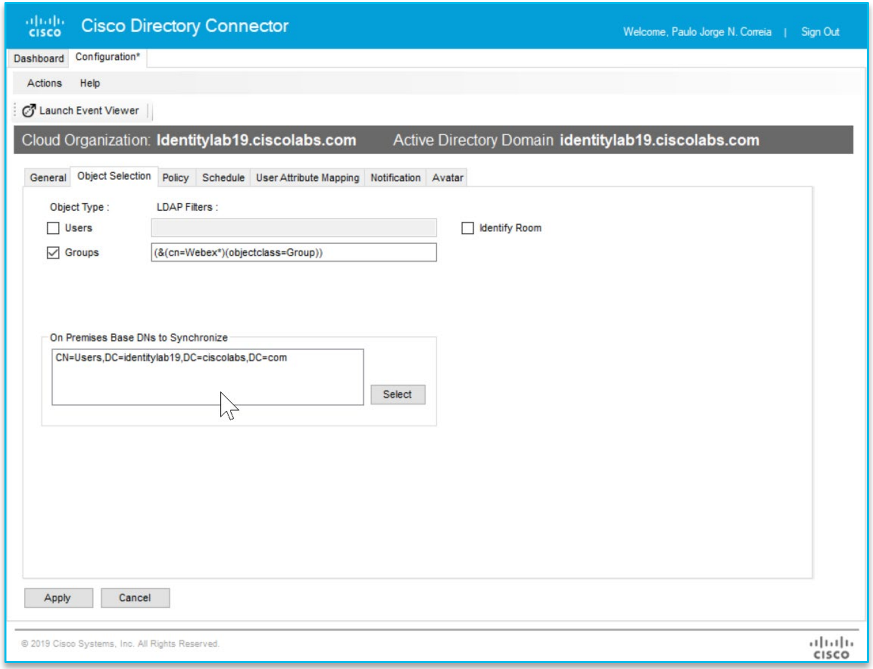
Create a filter so you only import the groups that you created for the Webex roles (E.g. Webex.....)

(&(cn=Webex)(objectclass=Group))*

Perform a full sync just on groups



Confirm start of full synchronization. This may take some time.



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

Object Type : LDAP Filters :

☐ Users

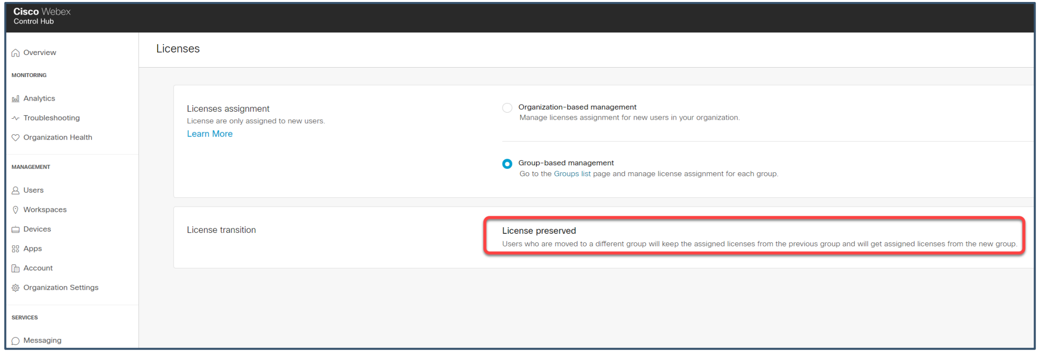
☑ Groups (&(cn=Webex*)(objectclass=Group))

☐ Identify Room

On Premises Base DNs to Synchronize

CN=Users,DC=identitylab19,DC=ciscolabs,DC=com

What to configure in Control Hub



Licenses

Licenses assignment
License are only assigned to new users.
Learn More

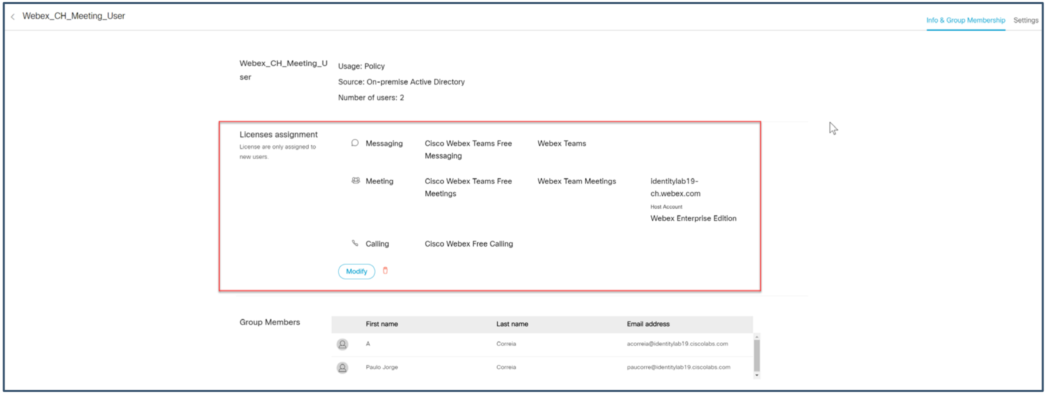
○ Organization-based management
Manage licenses assignment for new users in your organization.

● Group-based management
Go to the Groups list page and manage license assignment for each group.

License transition

License preserved
Users who are moved to a different group will keep the assigned licenses from the previous group and will get assigned licenses from the new group.

When users change groups membership, they acquire new licenses, but keep licenses from the old group



Webex_CH_Meeting_User

Usage: Policy
Source: On-premise Active Directory
Number of users: 2

Licenses assignment
License are only assigned to new users.

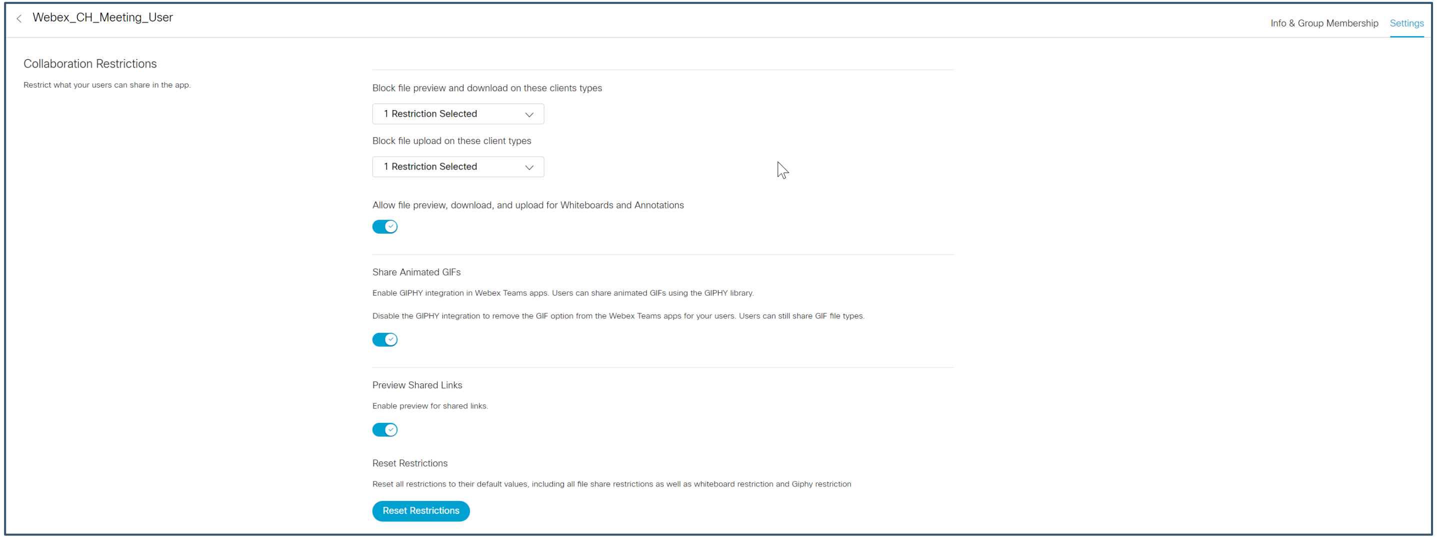
Messaging	Cisco Webex Teams Free Messaging	Webex Teams	
Meeting	Cisco Webex Teams Free Meetings	Webex Team Meetings	identitylab19-ch.webex.com Host Account Webex Enterprise Edition
Calling	Cisco Webex Free Calling		

Group Members

First name	Last name	Email address
A	Correia	acorreia@identitylab19.ciscolabs.com
Paulo Jorge	Correia	paucorre@identitylab19.ciscolabs.com

Each AD group can have a license template, and you can see the group members, defined in AD

What to configure in Control Hub



Webex_CH_Meeting_User

Collaboration Restrictions

Restrict what your users can share in the app.

Block file preview and download on these clients types

1 Restriction Selected

Block file upload on these client types

1 Restriction Selected

Allow file preview, download, and upload for Whiteboards and Annotations

Share Animated GIFs

Enable GIPHY integration in Webex Teams apps. Users can share animated GIFs using the GIPHY library.

Disable the GIPHY integration to remove the GIF option from the Webex Teams apps for your users. Users can still share GIF file types.

Preview Shared Links

Enable preview for shared links.

Reset Restrictions

Reset all restrictions to their default values, including all file share restrictions as well as whiteboard restriction and Giphy restriction

Today you can only define the collaboration restrictions for sharing in file, but you can expect many more global features in CH to apply at a group level.

The bridge to possible

Thank you

cisco Live!

#CiscoLive